РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА
УНИВЕРЗИТЕТ „СВ.КИРИЛ И МЕТОДИЈ“ - СКОПЈЕ
ПРАВЕН ФАКУЛТЕТ „ЈУСТИНИЈАН ПРВИ“ - СКОПЈЕ

# ПРИВАТНОСТ И ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ДИГИТАЛНАТА ЕРА

***- Докторска дисертација -***

Кандидат:

м-р Нора Османи

Ментор:

Проф. д-р Владо Бучковски

Скопје, 2020

# СОДРЖИНА

# Вовед

Технолошкиот развој и достапноста на различни информации на Интернет доведе до комерцијализација на човековите вредности. Во денешно време информациите можат полесно да се соберат, да се зачуваат, да се разменат и да се процесираат. Онлајн продавниците, рекламите и сите други можности за пристап до онлајн услуги оставаат траги за секој корисник на Интернет. Многу корисници не се свесни за трагите и нивните податоци што ги оставаат во секоја Интернет комуникација, како на пример: давање на е-пошта, домашна адреса или податоци за кредитни картички, со што сè повеќе и повеќе веб страниците во онлајн светот добиваат слика за корисниците и нивните интереси.

Глобализацијата и развојот на информатичката технологија овозможуваат зголемување на квалитетот на човековите комуникации и го поттикнуваат општиот економски развој. Меѓутоа, оваа дигитална еволуција влијае врз основните човекови права како што се: приватноста, заштитата на податоците и дигиталниот идентитет (како можно човеково право во иднината). Со оглед на брзите технолошки промени, многу е важно да се преземат потребни мерки за заштита на приватноста, затоа што многу често технолошките системи содржат скриени опасности кои тешко се надминуваат после основната изработка на податоците. Во овој контекст, исклучителна важност има идентификувањето на главните предизвици и ризици, како и можните проблеми за заштита на податоци.

Во последните години, важноста на заштитата на податоците е во фокусот на многу дебати од страна на политички и институционални структури, и не само заштитата на приватниот живот на поединците, туку и нивната слобода. Овој пристап се рефлектира од многу национални и меѓународни документи. На пример, Повелбата за основни права на Европската Унија го признава правото на заштита на податоци како фундаментално и автономно право.

Невозможно е да се даде еден сеопфатен концепт на правото на заштита на податоци. Заштитата на податоците претставува одредени идеи и изрази за обработката на личните податоци. Со примена на овие идеи, владите се обидуваат да ги хармонизираат основните вредности за општеството кои честопати претставуваат конфликтни вредности,

како што е приватноста, слободниот проток на информации, итн. Општо земено, заштитата на податоци нема забранета природа како кривичното право, бидејќи во принцип, субјектот на податоците не ги поседува своите податоци и честопати не може да ја спречи обработката на своите лични информации. Оттука, правото на заштита на податоци е прагматично: често се претпоставува дека обработката на личните податоци е неопходна од општествени причини. Регулативата за заштита на податоци не нè заштитува од обработката на податоците, туку од незаконската и непропорционалната обработка на нашите лични податоци.[1]

Приватноста или правото на почитување на приватниот живот и правото на заштита на личните податоци се поврзани во некои значајни контексти. Тие се изрази на една универзална идеја со силни етички димензии: достоинство, самостојност и уникатна вредност за секое човечко суштество. Меѓутоа, тие се разликуваат во однос на нивното значење. Концептот на заштита на личните податоци беше развиен со цел да им обезбеди правна заштита на поединците против несоодветната употреба и обработка на личните информации во информатичката технологија, без оглед на тоа дали таквата обработка се реализира во рамките на опсегот на правото на почитување на приватниот живот или не. Заштитните мерки во овој контекст, кои се однесуваат во принцип за секаква обработка на лични податоци, претставуваат еден систем од материјални услови, индивидуални права, процедурални одредби и независен надзор.[2] Концептот на правото за заштита на податоците во себе го носи и правото на приватност, меѓутоа тој е поширок. Заштитата на податоците ги формулира условите според кои се прави легитимна обработка на личните податоци, кои меѓу другото, подразбираат дека податоците мора да се обработуваат според законот, за определени цели и врз основа на согласноста на субјектот на податоците, или некоја друга легитимна основа утврдена со закон. Според ова, клучен елемент кој определува дали некоја основа е легитимна или забранета, претставува целта за која податоците се процесираат: податоците може да се обработуваат само за конкретни, експлицитни и легитимни цели.[3]

[1] De Hert and Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action', in S. Gutwirth et al. (eds.), *Reinventing Data Protection?* 1 (2009) , at p.3.
[2] Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation', in M. Cremona (ed.), *New Technologies and EU Law* 1 (2017) , at p.123.
[3] De Hert and Gutwirth, *supra* note 1, at p.4.

# Општествена и научна оправданост на темата

Надминувањето на националните граници при остварување на електронските активности, транснационализмот на информатичкото општество и телекомуникациските системи, креираа низа можности за појава на нови форми и начини на прекршување на основните човекови права, како што е правото на приватност и заштита на личните податоци.

Во последниот век, приватноста е еден од најголемите предизвици со кои сме соочени како корисници на технологијата во секојдневната комуникација и во работата. Со брзиот развој на информатичкото општество, драматично е променет начинот на кој личните информации се собираат, се чуваат и се споделуваат. Во современето општество, личните податоци се чуваат во дигитален формат, без оглед на тоа за која област се работи, дали е тоа здравство, социјална заштита или банкарство. Во исто време се овозможува лесен и евтин пристап, снимање, промена и дистрибуција, па затоа, драстично е зголемена и можноста да се загрози приватноста. Денес тоа можат да го прават поединци, приватни компании, но и владини институции и агенции.

Контролата што лицата ја имаат врз сопствениот живот, а особено изборот кој го прават во поглед на личните информации (на кого, во која мерка и за кои цели ќе одберат да ги откријат), се нарушува кога на владините служби, на приватни компании и различни агенции им е дозволено да собираат лични податоци од повеќе извори. Со собирањето на лични информации за индивидуалните лица, се добива одредена контрола врз субјектите на тие информации. Во најлош случај, личните податоци можат да се користат несоодветно за вршење на притисок врз политичари, новинари, итн. Со овие форми на чување на личните податоци, нашето минато сè повеќе и повеќе станува присутно во нашиот живот. Овие случувања секако претставуваат закана за приватноста, но што е конкретно проблемот? Начинот на кој се одговара на ова прашање може да има длабоки импликации на начинот на кој законот ќе се справи со проблемот во иднина.

Кога ќе падне во погрешни раце, технологијата претставува опасно оружје за животите на луѓето. Со прецизно определени методи и техники, технологијата може да нè информира за целосната комуникација, географската местоположба, финансиската

историја и сл., за одредена личност или групи од интерес. Во овој контекст, се наметнува прашањето: дали корисникот е свесен за трансферот на неговите лични податоци, кои се вршат на дневна база низ разни комуникациски канали помеѓу државни и приватни институции и корпорации? Денес, повеќе од кога било порано, потребно е корисникот да менаџира со своето виртуелно присуство, бидејќи со брзиот развој на нови техники за идентификација (со притисок на едно копче, со краток поглед во леќите на камерата, и сл.) и воедно носи сè поголем ризик тие информации да се злоупотребат. Личната одговорност и информирањето на поединците е круцијално во постапките за заштита на својата приватност. Од друга страна, покрај личната одговорност за менаџирање на своето виртуелно присуство и давање на лични информации, корисни мерки за заштита на приватноста и личните податоци претставуваат и законските регулативи на глобално и национално ниво. Имено, правото на приватност и на приватен живот е глобално признато човеково право.

Законите и подзаконските акти можат да ја заштитат приватноста и личните податоци на граѓаните, преку ограничување, надгледување, но и казнување на приватните компании и државните институции кои неовластено и спротивно на законот ги користат податоците на одредени лица. Како што компаниите стануваат сè поиновативни во прибирањето, складирањето и трансферот на личните податоци на граѓаните, така, со исто темпо би требало да ги следат и регулативите кои ќе го штитат граѓанинот и неговото право на приватност во секој од чекорите на обработка на неговите податоци. Обврска на државите е создавање на соодветна правна инфраструктура, која ќе ја штити приватноста на граѓаните, вклучително и од самите органи на власта. За жал, предложените законски решенија и политики многу често се неефикасни поради недостиг од јасно и универзално разбирање на самиот концепт на приватност и неефикасна имплементација на ова право. Многу често, во име на безбедноста и на сигурноста на граѓаните, владите го дерегулираат балансот помеѓу слободата и приватноста.

# Предмет на истражувањето

Предмет на проучување на темата под наслов „Приватност и заштита на личните податоци во дигиталната ера“ е токму анализирањето на концептите и правните механизми за чување на приватноста и заштита на личните податоци во информатичкото општество. Трудот претставува задлабочена анализа на правната форма и практичните импликации на приватноста и личните податоци во дигиталниот свет, вклучувaќи и дефиниции, елементи, стандарди и современи принципи за управување со безбедноста на информациите. Исто така се презентираат концептите за заштита на личните податоци и нивната примена во електронските комуникации, со цел да се докажат главните предизвици со кои приватноста на поединците се соочува во рамките на дигиталниот свет. Во исто време, се анализира законската регулатива на Европската Унија за заштита на личните податоци, која претставува главна легална основа за заштита од нелегални прибирања на лични податоци. Во овој контекст посебно внимание е посветено на чувствителните податоци, детската приватност на Интернет, онлајн профилирање, социјалните мрежи и медиуми, итн.

Примарната цел на ова истражување е да се утврдат, да се анализираат, проучат и презентираат концептите за заштита на личните податоци и нивната примена во електронските комуникации, како и да се докажат главните предизвици со кои приватноста на поединците се соочува во рамките на дигиталниот свет, со посебен осврт на регулативата на Европската Унија за заштита на личните податоци. Заклучоците покажуваат дека правната рамка за заштита на лични податоци на Европската Унија релативно успешно ги решава најчестите проблеми со кои се соочуваат корисниците на информатичките и комуникациските технологии, меѓутоа не обезбедува соодветно решавање на потенцијалните ризици и прашања кои се резултат на брзиот технолошки развој.

Проучувањето на предметот на истражувањето се врши со примена на дескриптивниот метод и теоретската анализа. Со овие методи се утврдуваат основните карактеристики и обележја на појавите кои се предмет на истражување. Исто така се користи историскиот метод кој овозможува да се даде одговор на прашањето за

развитокот на анализираните поими и принципи за приватност и заштита на лични податоци од моментот на нивното појавување, па се до нивните денешни облици.

Докторската дисертација е поделена на три главни делови. Во првиот дел - *Заштита на личните податоци во електронските комуникации, терминологија и правна рамка* - акцентот се става на анализата на основните концепти и поими на приватност и заштита на лични информации, вклучувајќи и дефиниции, елементи, стандарди и современи принципи за управување со безбедноста на информациите. Истовремено се проучуваат основните начела за заштита на личните податоци, како и согласноста како правна основа за обработка на лични податоци, со посебен фокус на родителската согласност за обработка на личните податоци на децата. Во овој дел исто така се прави анализа на правната рамка и развојни аспекти на правото на приватност и заштита на лични податоци, и посебен фокус се става на меѓународниот контекст и историјат на европското законодавство за заштита на лични податоци.

Вториот дел на дисертацијата – *Правата на субјектот на податоци и нивното спроведување* - целосно се однесува на правата на субјектот на податоците, додека продлабочена анализа се прави на правото да бидеш заборавен и правото на преносливост на податоци, која дава нови права во законската рамка на Европската Унија за заштита на лични податоци, кои беа воведени со Општата регулатива за заштита на лични податоци, и кои им овозможуваат на корисниците на онлајн услугите да имаат поголема контрола врз своите лични информации.

Во третиот дел –*Надзор како форма на социјална контрола* - се анализираат механизмите за надзор во 21-виот век, односно различни современи технологии за следење на поединците како што се: CCTV камери, технологија за препознавање на лицето (биометрика), беспилотните летала, итн., и предизвиците што овие технологии ги нанесуваат врз приватноста на луѓето. Истовремено се истакнува дека во отсуство на релевантни законски правила во оваа област, компаниите кои ги користат овие технологии од една страна, и поединците загрижени за нивната приватност од друга страна, се во постојан конфликт. Поради ова, во овој дел се сугерираат некои нови регулаторни пристапи кои ќе ги штитат интересите на граѓаните и истовремено нема да ја задушат иновацијата.

# Значење на истражувањето

Докторската дисертација има теоретско и практично значење. Од научен аспект, овој труд претставува екстензивно и сеопфатно истражување на основните правни мерки за заштита на приватноста и личните податоци во дигиталниот свет, каде секој ден се појавуваат нови форми и начини на злоупотреба и загрозување на нашата приватност во виртуелните интеракции. Круцијалното анализирање на правната рамка за заштита на лични податоци на Европската Унија, имено Општата регулатива за заштита на лични податоци,[4] кое моментално претставува најстрог закон за заштита на лични податоци во светот, ги става на увид главните предизвици со кои се соочуваат поединците при користење на електронски комуникации и се обезбедува информација за правните чекори кои субјектот на податоци треба да ги следи во ситуации кога има несоодветна обработка на податоците или нарушување на неговата/нејзината приватност.

На ваков начин, истражувањето претставува солидна основа за лоцирање на општествените проблеми поврзани со заштита на личните податоци и презентира ефективни механизми кои можат позитивно да влијаат во заштитата на правото на приватност на граѓаните на една држава. Според ова, дисертацијата може да има социјални придобивки, односно да ги информира граѓаните и да ја подигне свеста на поединците, особено на оние кои не се правни експерти и немаат основно познавање на нивните права на приватност и заштита на лични податоци кои би можеле да бидат загрозени при собирање, обработка, трансфер или чување од страна на давателите на електронските услуги.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 2016.

# ПРВ ДЕЛ – ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ЕЛЕКТРОНСКИТЕ КОМУНИКАЦИИ, ТЕРМИНОЛОГИЈА И ПРАВНА РАМКА

Пред таканаречената информациона револуција, информациите и податоците за една личност се чувале во традиционални досиеја или нешто слично на тоа. Пристапот до нив бил релативно редок, најчесто од носителот на податоците, а тежок бил пристапот за други корисници до слични информации или информации за истото лице. Леснотијата со која првата генерација на компјутери ги зачувуваше и управуваше со податоците, предизвика драматична промена во тој поглед и го олесни поврзувањето на информации за одредени лица чувани на различни места. Всушност, се појави нова индустрија од операцијата наречена поврзување на податоци, во која профилот на една личност се создава со податоци од различни извори.[5]

Верувањето дека поседувањето на повеќе информации носи повеќе безбедност, е политика за промовирање на собирање на податоци и информации, со кои се предвидува нашето однесување, нашите желби и потреби. Како последица на ова, се појавиле нови форми на идентитети, кои повеќе не мора да бидат поврзани со нашите реални имиња. Тие се базираат на информации и траги кои ние ги оставаме кога делуваме или комуницираме во дигиталниот свет. Тие се поврзани на пример со SIM картички на нашите мобилни телефони, нашите броеви на кредитни картички, нашите е-пошти, IP адреси на нашите компјутери итн. Како и традиционалните идентитети, овие нови форми на идентитети ни овозможуваат да  разликуваме едно лице меѓу една група на луѓе и да го определиме како член на една заедница или категорија.[6]

Колку далеку отидовме ние во овој процес? Во информатичкото општество нашиот идентитет стана една маска која ние ја избираме за да комуницираме едни со други. Правата, обврските , одговорностите, дури и нашиот углед сè повеќе се поврзани со овие маски. Од една страна овие маски се сметаат како клуч за пристап до доверливи

[5] Г. Наумовски et al., *„Право на инфоратичка технологија“* (2013), at p.138.
[6] D. Olivier and J. Chiffelle, *Identity Revolution: Multi-Disciplinary Perspectives* (2009), at p.2.

информации и користење на различни услуги. Од друга страна, во случај на измама или негативна репутација, сопственикот на таа маска може да биде казнет, така што пристапот до услуги се одбива.[7]

[7] *Ibid.*, at p.2-3.

# ГЛАВА ПРВА: ДЕФИНИЦИИ И ОСНОВНИ ПРИНЦИПИ ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

## 1. Правото на приватност и правото на заштита на лични податоци

Врската помеѓу поимите заштита на податоци, од една страна, и приватност од друга страна, отсекогаш била тешка за изедначување. Тука не помага ниту фактот дека се избегнува одредување на една дефиниција за приватност. И покрај тоа што прашањето за приватноста постоело уште со измислувањето на sидовите, правната академска дискусија започнала кон крајот на деветнаесетиот век.[8]

Основата на приватноста на информациите претставува барање на поединците да одлучуваат за себе, кога, како, и до кој степен нивните информации ќе им се соопштат на другите.[9]

Правото на приватност се однесува на правото на една личност да го живее својот живот во приватност, без мониторинг, без разлика дали ваквиот живот вклучува односи со други личности или не; додека правото на заштита на личните податоци ги заштитува овие податоци како и сите други податоци, без разлика дали се лични или не, под услов да се во врска со индентификацијата на личноста. Личните податоци не мора секогаш да се поврзани со правото на приватност, бидејќи самиот концепт на лични податоци е многу поширок од концептот на приватен живот. Оттука доаѓа и нивното издвојување во две автономни права.[10]

Приватноста честопати се поистоветува со безбедноста, но сепак тие се два различни концепти. Приватноста на информациите, пред сè, подразбира соодветно собирање, употреба и споделување на лични информации, додека безбедноста претставува заштита на таквите информации од загуба или неовластен пристап, употреба или споделување.

[8] Наумовски et al., *supra* note 5, at p.142-143.
[9] K. A. Bamberger and D. K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (2015), at p.20.
[10] Ѓуркова, „Правото на приватен живот и правото на заштита на лични податоци во Европското законодавство во судир со националната безбедност“, *Правник Бр.239* (2012) , at p.3.

Правото на приватност е поширок концепт за разлика од правото на заштита на личните податоци, и заштитата на личните податоци може да се смета како дел на правото на приватност.[11] Концептот за заштита на податоци се однесува на еден збир правни мерки и правила со кои се заштитуваат правата, слободите и интересите на поединците, чии податоци се собираат, чуваат, обработуваат, итн. Така на пример, правото на приватност го штити физичкиот интегритет на едно лице и неговиот домашен мир, без разлика на тоа дали целта на потенцијалните нарушувачи на ова право е да добијат лични информации за таа личност.[12] Меѓутоа, овие права се разликуваат според обемот, целта и содржината. Правото на заштита на податоци експлицитно ги штити вредностите кои не се основни за приватноста, како што се: барањето за законска обработка на податоците, согласноста на субјектот на податоците, легитимитет и недискиминација.[13]

Според Родота, разликата помеѓу правото на почитување на приватниот и семејниот живот и правото на заштита на податоци се опишува врз основа на однесувањата на третите лица. Во овој контект, Родота истакнува дека правото на почитување на приватниот и семејниот живот претставува индивидуалистичка компонента; претставува власт на едно лице да ги спречи третите лица и да им забрани да се мешаат во приватниот и семејниот живот. Со други зборови, тоа претставува еден вид на негативна заштита.[14] Спротивно од тоа, правото на заштита на податоците утврдува правила и одредби при обработка на личните податоци и овластува да се земат различни мерки за заштита на податоците; значи ова право претставува динамична заштита, која ги следи податоците во сите видови на нивната обработка. Субјектот на податоците не е овластен да ги заштити своите податоци, со оглед на тоа дека постои едно овластено тело постојано одговорно за тоа.[15]

[11] Hartlev, 'The Concept of Privacy: An Analysis of the EU Directive on the Protection of Personal Data', in D. Beyleveld et al. (eds.), *The Data Protection Directive and Medical Research Across Europe* (2004) , at p.25.
[12] *Ibid.*
[13] De Hert and Gutwirth, *supra* note 1, at p.9.
[14] Rodota, 'Data Protection as a Fundamental Right', in S. Gutwirth et al. (eds.), *Reinventing Data Protection?* (2009) , at p.79.
[15] *Ibid.*

## 2. Што се личните податоци?

Личните податоци како поим се строго поврзани со идентитетот на еден човек. Идентитет на една личност претставуваат некои елементи според кои таа личност се разликува од другите. Според член 2 на Законот за заштита на личните податоци на Република Северна Македонија[16], „личен податок“ е секоја информација која се однесува на идентификувано физичко лице, или физичко лице кое може да се идентификува. Лице кое може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на матичен број на граѓанинот или врз основа на едно или повеќе обележја специфични за неговиот физички, филозофски, ментален, економски, културен или социјален живот. Од вака дефинираниот израз на „личен податок“ произлегува дека секоја информација (податок, документ, факт, белег) во врска со севкупниот (физички, ментален, економски, културен, социјален) идентитет на едно лице претставува личен податок кој се заштитува.

Во правна смисла, „лични податоци“ значи: секоја информација во врска со идентификувано физичко лице, или физичко лице кое може да се идентификува, кој се наведува како ‘субјект на податоци’. Лицето може да се идентификува:

- Директно, или
- Индиректно - особено според еден идентификациски број или според еден или повеќе на број фактори кои се однесуваат на физички, генетски, ментални, економски, културен или социјален идентитет на едно лице.[17]

Поимот ‘секоја информација’ повикува за широко толкување. Во овој контекст, концептот на лични податоци вклучува секаков вид информации за една личност, кои можат да бидат објективни информации – како што е на пример возраста на субјектот на податоците, и субјективни информации – како што се мислењата на една личност.[18]

Личните податоци потекнуваат од три вида на податоци:

[16] „Службен весник на Република Северна Македонија“ бр. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015, 99/2016 и 64/2018.
[17] Europe University Institute, Guide on Good Data Protection Practice in Research, 2019, p.5.
[18] *Ibid.*, at p.5-6.

(а) Податоци пријавени од самите субјекти на податоци – ова се информаци кои луѓето ги откриваат за самите себе, како што е нивната е-пошта, работа, возраст, пол, итн.[19]

(б) дигитални податоци – на пример податоци за локација, историја на прелистување што се создава кога се користат мобилни уреди, веб-услуги или други технологии за поврзување.[20]

(в) податоци од профилирање – податоци кои произлегуваат од индивидуални профили кои се користат за предвидување на интересите и однесувањата на поединците.[21]

За одредени информации да се сметаат за лични податоци, треба да бидат присутни четири елементи:

- Информации – личните податоци вклучуваат информации за одредено физичко лице. Информацијата може да биде во различна форма – дигитална, графичка, фотографска, пишана, акустична и слично, а формата на податоците не е одлучувачка за утврдување на тоа дали информацијата е лична или не.[22]
- Поврзаност – за да се сметаат за лични податоци, информациите треба да бидат поврзани со одредено лице. Во многу случаи, поврзаноста може да се утврди несомнено, на пример, податоците на еден пациент содржани во медицински досиеја. Меѓутоа, во некои случаи утврдувањето на поврзаноста меѓу одредени информации и конкретното физичко лице не е толку јасна. На пример, податоците за вредноста на недвижен имот вообичаено се однесуваат на самата недвижност, но исто така можат да бидат поврзани со сопственикот на имотот, бидејќи оваа вредност може да ја открие неговата економска и финансиска состојба.[23]
- Идентификувано лице или лице кое може да се идентификува – личните податоци треба да бидат поврзани со едно лице кое може да се

[19] Shave, 'Privacy and Security in Our Complex Digital World (Online)', *IQ: The RIM Quarterly* (2016) , available at https://search.informit.com.au/documentSummary;dn=049096323490954;res=IELAPA , at p.21.
[20] *Ibid.*
[21] *Ibid.*
[22] Д. Тошкова, Водич за заштита на личните податоци, 2018, p. 6.
[23] *Ibid.*

идентификува. Одредено лице може да се смета за препознатливо (идентификувано) ако во рамките на една заедница или група на луѓе се издвојува од другите. Идентификацијата може да се направи според еден или повеќе фактори, специфични за физичкиот, физиолошкиот, генетскиот, менталниот, економскиот, културниот или социјалниот идентитет на физичкото лице. На пример, идентификацијата може да се направи според името и презимето на едно лице, адреса, место на раѓање, семејни односи, итн.[24]

- Физичко лице – личните податоци се однесуваат само на физичките лица. Правните лица или организации не поседуваат лични податоци и се исклучени од заштитниот режим на правилата за заштита на лични податоци.[25]

## 3. Различни перцепции за приватноста

Во филозофската и правната литература има многу обиди да се дефинира правото на приватност. Заштитата на личната приватност се однесува на можноста на поединците да имаат контрола врз тоа што другите знаат за нив и да имаат одреден степен на лична автономија.[26] Заштитата на приватноста исто така помага да се дефинираат односите меѓу граѓаните и државата, и односите меѓу консуматорите и интересот на корпорациите. Во основа, заштитата на правата на приватност се обидува да го балансира индивидуалниот интерес со општествениот интерес. Интригантното прашање е: кој одлучува каде лежи рамнотежата?[27]

Приватноста е еден од оние поими кои на прв поглед изгледаат многу лесно за дефинирање, меѓутоа бараат детална анализа. Сумирање на приватноста во една дефиниција е практично невозможно, бидејќи поимот приватност може да подразбира

[24] *Ibid.*, at p.7.
[25] *Ibid.*
[26] L. Stefanick, *Controling Knowledge: Freedom of Information and Privacy Protection in a Networked World* (2011), at p.29.
[27] *Ibid.*

различни вредности зависно од културата и законите на една држава. Бројни дефиниции се појавуваат за поимот приватност. Меѓутоа, меѓу највлијателните дефиниции е концептот на приватноста како право да се остане сам во својот дом, воведен од страна на Brandeis и Warren. Во нивната статија „Правото на приватност“[28] Louis Brandeis и Samuel Warren ја дефинираат заштитата на приватноста како основа за индивидуална слобода во модерната ера. Со оглед на зголемувањето на капацитетот на владата, медиумите и другите органи и институции да нападнат различни аспекти на лични активности, тие тврдат дека законот мора да се развива како одговор на технолошките промени. Традиционалните мерки против злосторство, напади и други инвазивни однесувања дадоа доволна заштита во претходните (поранешните) епохи, меѓутоа овие воспоставени принципи не можат, според нив, да ги заштитат луѓето од таканаречениот премногу претприемнички прес, фотограф, или друг сопственик на било кој друг модерен уред, со помош на кој може да се промени текстот или да се врши репродукција на сцени или звуци.[29] Brandeis и Warren го дефинираат правото на приватност  како право на еден човек да остане сам, како право да ужива во својот дом.[30] Во овој концепт, тие тврдат дека секоја личност има право да одлучува до кој степен своите мисли, чувства и емоции ќе бидат достапни за другите (поширокатa јавност). Правото да се биде сам во приватноста на својот дом значи дека никој нема да се меша во животот на одреденото лице, без разлика дали станува збор за мешање од страна на луѓе или држава. Правото на приватност, во оваа смисла, се смета како должност да се почитува приватноста на другите.[31]

Подоцна концептот за приватност беше развиен од страна на многу научници и правници, и во бројни дефиниции приватноста се гледа како ограничен пристап до некоја личност, всушност контрола над личните информации.

Според Daniel Solove, „приватноста е еден концепт, кој вклучува (меѓу другите работи) слободата на мислење, контрола над телото, осаменост во домот, контрола над

[28] Warren and Brandeis, 'The Right to Privacy', 4 *Harvard Law Review* (1890) , available at http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C%0D.
[29] *Ibid.*
[30] *Ibid.*, at p.193.
[31] van der Sloot, 'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data?', 5 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (2014) , available at https://www.jipitec.eu/issues/jipitec-5-3-2014/4097/sloot.pdf, at p.231.

своите информации, слобода од надзор, заштита на угледот и заштита од пребарувања и сослушувања“.[32]

Современиот концепт на приватност се поврзува со концептот на автономија, како што е капацитетот на една личност да се оддалечува од другите, да ги развие своите верувања и желби, да одржува одредено ниво на контрола врз внатрешните сфери на својот живот, да изврши одреден степен на индивидуална моќ, да направи избор, да го ограничува пристапот до себе и да биде одвоен од заедницата. Во овој концепт се вклучува и моралниот статус на лицето за неговото достоинство и однос со другите.[33]

Како концепт, приватноста речиси секогаш е поврзана со заштита на податоци, и тоа поради една голема причина: во дигиталниот свет е создадена една клима од несигурност за корисниците на Интернетот, бидејќи сè повеќе и повеќе различни компании и организации собираат лични податоци, со цел истите да ги користат во нивните маркетинг кампањи.

Балансирањето на различни општествени вредности, како и правни, социјални, политички и етички аргументи, имаат влијание врз можните мислења и концепти за заштитата на приватноста на податоците. Овие дефиниции се разликуваат меѓу себе, токму поради тоа што тие означуваат прогресивно вклучување на нови аспекти на слободата во проширувањето на концептот на приватност. Најновите дефиниции не ги заменуваат минатите, бидејќи тие се засноваат на различни барања на општеството во одреден временски период.

Во литературата, одредбите за заштита на податоци се класифицирани во две категории:

- Правила ориентирани кон интегритетот на поединците - овие правила најмногу се однесуваат на заштитата на приватната сфера на едно лице и неговата личност.[34]
- Правила ориентирани кон автономијата на поединците - овие правила се фокусираат на способноста на една личност да има контрола врз

[32] Solove, 'Conceptualizing Privacy', 90 *California Law Review* (2002) , available at http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2, at p.1088.
[33] S. Venier and E. Mordini, Competitiveness and Innovation Framework Programme: ICT Policy Support Programme (ICT PSP), 2011, p.20.
[34] Hartlev, *supra* note 11, at p.31.

обработката на своите податоци, без разлика дали информациите се чувствителни или нечувствителни. Во овој контекст, овие правила се ориентираат на можноста на поединецот да одлучува за користењето на своите податоци од страна на трети лица.[35]

## 4. Приватност во една променлива околина

Пред информатичката револуција, приватноста беше поврзана со личниот простор на еден човек да ужива во својот дом. Меѓутоа, во 21-виот век технологијата е дел од нашиот секојдневен живот. Во секоја наша Интернет комуникација, голема количина на нашите лични податоци се чуваат, се обработуваат и се процесираат. Тоа овозможува брз трансфер или пренос на личните податоци низ целиот свет. Во оваа смисла, заштитената зона на нашата приватност се менува, бидејќи во денешниот свет приватноста е многу тесно поврзана со користењето на електронските услуги и комуникации. Слика 1 ја илустрира промената на областа на приватност.


**Слика 1. Приватност во една променлива околина.**

[35] *Ibid.*

Концептот за приватност е организиран на следниов начин: Прво, приватноста претставува личен простор, или право на една личност да одлучува сама без да биде гонета од трети лица. Во горенаведената слика тоа се наоѓа во левиот круг. Тоа што претставува приватност во оваа област останува искуство на една личност, изолирана од светот. На пример, правото да седиш сам во една соба се однесува на таквиот вид на приватност. Второ, Интернетот се меша во зоната на приватноста. Тоа се наоѓа во горниот круг на фигурата. Приватноста во оваа област е тесно поврзана со информациите и користењето на електронските услуги. На пример, во секоја Интернет трансакција, нашата приватност зависи од технологијата и употребата на дигиталните уреди и апликации. Трето, физичките лица ја имаат и внатрешната приватност, која се однесува на нашите мисли и секојдневните обврски. Тоа најпрво се однесува на нашиот мир, кој е под влијание на внатрешни фактори, како што се: проверка и пишување на е-пошта, семејни обврски, телефонски повици и други одговорности што ги исполнуваат нашите денови. Како што се гледа од десниот круг на фигурата, внатрешната зона на приватноста се шири, што значи дека сè повеќе и повеќе таа се диктира од надворешни фактори.

## 5. Видови на приватност

Како што е прикажано во горенаведениот текст, поимот „приватност“ не е воопшто лесно да се дефинира. Најновите технолошки достигнувања го зголемуваат опсегот на приватноста, бидејќи развојот на технологијата поставува нови прашања за заштитата на приватноста. Во оваа смисла, научниците зборуваат за седум видови на приватност (кои се поврзани со развојот на седум видови на технологии), како што се: приватност на личноста, приватност на однесување и дејствување, приватност на лична комуникација, приватност на податоци и слика, приватност на мисли и чувства, приватност на локација и простор, и приватност на здружување (вклучително и групна приватност).[36]

[36] Finn, Wright and Friedewald, 'Seven Types of Privacy', in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (2013) , at pp.3-32.

## 5.1 Приватност на личноста

Приватноста на личноста го опфаќа правото на една личност да ги задржи приватни своите телесни функции и карактеристики (како што се генетските кодови и биометрика).[37]

Според Mordini, човечкото тело има силна симболичка димензија како резултат на интеграција на физичкото тело и умот, и поради тоа претставуваат културни вредности. Тој верува дека основната цел на безбедноста е да се заштити човековата личност во неговиот/нејзиниот физички, ментален и социјален интегритет. Почитувањето на човековото достоинство, интегритетот на телото и приватноста (физичка и информативна), според него, претставуваат основни компоненти на секоја безбедносна политика.[38]

Концептот на приватност на личноста и личното однесување најпрво беше развиено од Clarke,[39] а подоцна се прошири како приватност за однесување и акција.[40] Овој концепт вклучува чувствителни прашања како што се сексуалните преференци и навики, политичките активности и верските практики. Сепак, поимот 'приватност на лично однесување' се однесува на активности што се случуваат како на јавен простор, така и на приватен простор, а Clarke прави разлика меѓу секојдневните однесувања во јавен простор кои се набљудуваат од страна на блиски луѓе, и систематското снимање и складирање на информации за тие активности.[41]

## 5.2 Приватност на лична комуникација

Приватноста на комуникацијата има за цел да го избегне пресретнувањето на е-поштата, употребата на уреди за прислушување, следење или снимање на безжична

[37] *Ibid.*, at p.8.
[38] Mordini, 'Policy Brief on: Whole Body – Imaging at Airport Checkpoints: The Ethical and Policy Context', in R. von Schomberg (ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (2011) , at p.166.
[39] За повеќе информации, види: http://www.rogerclarke.com/DV/.
[40] Finn, Wright and Friedewald, *supra* note 36, at p.8.
[41] *Ibid.*

комуникација и пристап до е-маил пораки. Ова право е признато од многу влади кои бараат прислушувањето да се надгледува од страна на судовите или други авторизирани тела.[42]

Овој аспект на приватност им помага на поединците и на општеството со тоа што охрабрува дискусија за широк спектар на погледи и опции, така што овозможува раст во секторот за комуникации.

## 5.3 Приватност на податоци и слика

Приватноста на податоците и сликите вклучува загриженост за осигурување дека податоците на поединците не се автоматски достапни за други лица и организации. Тоа значи дека луѓето треба да имаат значителен степен на контрола врз тие податоци и нивната употреба.[43]

Таквата контрола врз личните податоци гради самостојност и им овозможува на поединците да се чувствуваат моќни. Исто како и приватноста на мислата и чувствата, овој аспект на приватност има социјална вредност бидејќи се однесува на рамнотежата на моќта меѓу државата и физичкото лице.

## 5.4 Приватност на мисли и чувства

Луѓето имаат право да не ги споделуваат своите мисли или чувства или истите да ги разоткријат според своите желби. Во оваа смисла, поединците имаат право да размислуваат што сакаат.[44]

Приватноста на мислите и чувствата може да се одвои од приватноста на личноста на ист начин како што се разликува умот од телото. Слично на тоа, се разликуваат

[42] *Ibid.*
[43] Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms', *Computer Science* (1997).
[44] Goold, 'Surveillance and the Political Value of Privacy', *Amsterdam Law Forum* (2009) , available at http://amsterdamlawforum.org/article/view/88/152, at pp.3-6.

мислата, чувството и однесувањето. Во оваа смисла, мислите не се преведуваат автоматски на однесувањето.[45]

## 5.5 Приватност на локација и простор

Според концептот на приватност на локација и простор, поединците имаат право на движење во јавен простор без да бидат идентификувани, или следени. Овој концепт го вклучува и правото на осаменост и правото на приватност во просториите како што се домот, автомобилот или фирмата.[46]

Овој концепт има голема општествена вредност, бидејќи кога граѓаните се слободни да се движат низ јавниот простор без страв од идентификација или следење, тие доживуваат чувство на живеење во демократија и слобода. Овие две субјективни чувства придонесуваат за здрава и добро прилагодена демократија.

## 5.6 Приватност на здружување (вклучително и групна приватност)

Последниот тип на приватност, односно приватноста на здружувањето (вклучително и групата) се однесува на правото на луѓето да се здружат со кого сакаат, без да бидат следени или гонети. Ова право е неодамна препознаено како потребен елемент за демократското општество, бидејќи ја подржува слободата на говор, вклучително и политичкиот говор, слобода на религија и други форми на здружување.[47]

Општествениот придонес на овој вид на приватност се однесува на промовирањето на широк спектар на групи на интереси, што може да помогне да се слушнат гласовите на различни луѓе во борба за политички или економски промени.[48]

[45] Finn, Wright and Friedewald, *supra* note 36, at p.9.
[46] *Ibid.*
[47] *Ibid.*
[48] *Ibid.*

# 6. Начелата за обработка на личните податоци

Во правна смисла, обработка на лични податоци значи секоја операција или збир на операции што се изведува врз лични податоци, како што е: собирање, снимање, организирање, складирање, чување, промена, употреба, откривање, пренесување, дисеминација или на друг начин правење достапни, усогласување или комбинација, блокирање, бришење или уништување.[49]

Општо, сè што правиме со личните податоци се смета за обработка. На пример:

- Создавање на еден список во е-пошта;
- Управување со една база на податоци;
- Споделување на одредени податоци со трети лица.[50]

При собирање и обработка на лични податоци треба да се почитуваат некои начела, како што се: безбедност, транспарентност и доверливост на податоци.

## 6.1 Безбедност

Безбедноста во информатичкото општество подразбира обврска на контролорот (водител на збирка на лични податоци) и на обработувачот да спроведуваат соодветни технички и организациски мерки заради спречување на неовластено мешање во операциите на обработката на податоците.[51] Тоа подразбира должност на сите лица да ја штитат и да ја осигураат доверливоста на податоците. Во овој контекст, безбедноста на личните податоци претставува должност на сите контролори и обработувачи на личните податоци да преземат соодветни мерки за заштита на личните податоци од неовластено користење, обработка или ширење.

За обработка на лични податоци на безбеден начин, треба да се спроведат соодветни мерки, како што се:

- Технички и организациски мерки за спречување на неовластен пристап;

[49] Europe University Institute, *supra* note 17, at p.7.
[50] *Ibid.*
[51] *Handbook on European Data Protection Law* (2014), available at https://fra.europa.eu, at p.90.

- Воспоставување на јасни правила за пристап;
- Обработка на начин кој дава најдобра можност за контрола;
- Користење на процесор кој обезбедува соодветни заштитни мерки.[52]

Во практична смисла, овие мерки може да резултираат во некои ситуации, како што се :

- автентикација на корисникот (проверка на идентитетот на корисникот) – користење на нешто што корисникот го знае (на пример, силна лозинка).
- Контрола на пристап – се однесува на механизам кој дозволува или негира пристап до одредени податоци.
- Безбедност на складирање – чување на податоци на еден начин кој спречува неовластен пристап (на пример: автентикација и контрола на пристап, употреба на лозинки за пристап до електронски документи, криптирање на база на податоци, итн.)[53]

Безбедноста на податоците честопати се постигнува со примена на технолошка опрема – хардвер и софтвер, каде што доминантно е користење на енкрипција. Меѓутоа, важно е да се наведе дека вистинските експерти не веруваат дека енкрипцијата е нешто повеќе од една алатка во целокупниот план за заштита на податоци. Кога Рос Андерсон, професор на компјутерска безбедност на Универзитетот во Кембриџ и еден од експертите за криптографија, беше прашан: „Колку добро треба да бидат шифрирани податоците за да бидат безбедни?“, тој одговорил:

„Од многу причини, ова е погрешно прашање. Кој мисли дека неговиот проблем е решен со енкрипција на податоците, не го разбира својот проблем и не разбира што значи енкрипција“[54]

Од моментот кога информациите не се контролираат од страна на корисникот, никој не може да гарантира дека тие ќе бидат целосно отстранети. Во оваа смисла, откако приватноста се „губи“, таа не може да се обнови. Поради оваа причина, личните податоци

[52] Europe University Institute, *supra* note 17, at p.12.
[53] *Ibid.*, at p.12-13.
[54] Bernal, 'A Right to Delete?', 2 *European Journal of Law and Technology* (2011) , available at http://ejlt.org/article/view/75/144, at p.6-7.

треба да бидат заштитени не само преку правни механизми, но и преку технички средства кои го спречуваат собирањето и поврзувањето на информациите.[55] Дури и во случаи кога законот се применува од страна на надлежните органи и технологијата се користи на соодветен начин и ефективно, сè уште ќе има проблеми и ризици кои никогаш не може да бидат целосно елиминирани. На крај, секогаш постојат податоци, и се смета дека единствен начин на кој податоците не можат да се злоупотребат е тие воопшто да не постојат.[56]

Можеби најдобриот и единствен начин за позитивна промена на овој проблем е развивањето на нови бизнис-модели. Клучот е да се најде начин за овие модели да се доближат и да ја прифатат смислата за минимизирање на податоци. Како може ова да се случи? Ако може да се најде начин за ставање на податоците на едно лице во контрола на процесот на минимизирање на податоци, тогаш не само што поединците ќе имаат контрола врз своите податоци, туку и институциите и компаниите мора да ги развијат овие бизнис-модели кои не зависат од нивната способност да соберат било какви податоци и да ги држат тие во своите системи колку што сакаат. Тоа води кон идејата за правото на бришење на податоците.[57]

## 6.2 Доверливост

Доверливоста е способност на една личност да знае кога и под кои услови неговите лични податоци може да бидат обелоденети.[58] Кога овластено лице чита и копира информација, резултатот е познат како загуба на доверливоста. За неколку вида информации доверливоста е многу важен атрибут. Примерите на ваквиот вид информации вклучуваат медицински и осигурителни записи, лични податоци на граѓаните, податоци добиени преку истражување, одредени инвестициски планови, итн. Во одредени средини може да постои законска обврска за заштита на приватноста на единката (банки и

[55] C. Diaz, *Privacy Risk Scenario*, 2006, Future of Identity in the Information Society, available at https://www.esat.kuleuven.be/cosic/publications/article-834.pdf (last visited 25 November 2018].
[56] Bernal, *supra* note 54, at p.8.
[57] *Ibid.*, at p.9.
[58] *Прирачник за Информатичка и комуникациска технологија*, available at http://aa.mk/WBStorage/Files/Priracnik IKT Mak.pdf (last visited 1 January 2019].

кредитни компании, болници, лекарски ординации, лаборатории за медицински испитувања, психолошки ординации итн.).[59]

## 6.3 Транспарентност

Taylor смета дека нема приватност без транспарентност. Според него, барањата за транспарентност треба да се зајакнат ако сакаме да се заштитиме од потенцијалните опасности на автоматизираното одлучување.[60]

Во Општата регулатива за заштита на личните податоци на Европската Унија (во понатамошниот текст GDPR),[61] се наведува обврската на контролорите да ги информираат субјектите на податоците за обработката на нивните лични податоци. Член 12 на GDPR утврдува дека на корисниците на онлајн услугите треба да им се обезбедат информации за обработка на нивните лични податоци „во една концизна, транспарентна, разбирлива и лесно достапна форма, користејќи јасен јазик.“ Посебно внимание се посветува на обработката на личните податоци на децата. Рецитал 58 на GDPR појаснува дека кога информациите им се посветени на децата, тие треба да бидат формулирани на јасен и едноставен јазик, кое детето може лесно да го разбере (член 40, параграф 2г).

# 7. Принципи за заштита на личните податоци

За да се избегнат случаите на злоупотреба на личните податоци во дигиталните комуникации, исклучителна важност имаат правните мерки и закони за заштита на лични податоци и зачувување на приватноста во дигиталните комуникации.

[59] *Ibid.*, at p.145.
[60] Taylor, 'No Privacy without Transparency', in R. Leenes et al. (eds.), *Data Protection and Privacy: The Age of Intelligent Machines* (2017).
[61] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 2016.

Секогаш кога се обработуваат лични податоци, контролорите треба да имаат во предвид дека обработката мора да биде пропорционална во однос на четири прашања: Што? Зошто? Како? Колку долго? [62]

Законот за заштита на лични податоци[63] на Република Северна Македонија е заснован на неколку водечки начела кои произлегуваат од одредбите на член 5 на овој закон, а кои исто така се во согласност со принципите на Директивата 95/46/ЕЗ и Општата регулатива за заштита на лични податоци[64] за заштита на приватноста во однос на обработката на личните податоци, кои се:

- Ограничено собирање на податоци:

Личните податоци треба да се собираат за посебни цели и натаму да не се обработуваат за други цели, односно не треба да се собираат повеќе податоци од колку што е неопходно за еден процес или трансакција, а сите прибирани податоци мора да се добијат по законски и правичен пат, со претходна согласност на граѓанинот.[65]

- Квалитет на податоци:

Собраните лични податоци мора да се релевантни за целта на именуваната активност, мора да се точни и често ажурирани.[66] Според ова, треба да се достават механизми за внатрешна контрола и заштита на лични податоци и редовно откривање на безбедност, спроведување на независни агенци за заштита на лични податоци, развивање на планови во случај на загуба, оштетување, неправилна употреба или други настани во текот на обработката на личните податоци; во случај кога личните информации биле откриени или изгубени, треба веднаш да се спречи понатамошното проширување на инцидентот и веднаш да се извести субјектот на податоците; кога се појавува голем настан, треба веднаш да се информираат органите за заштита на лични податоци.[67]

- Одредување на целта:

[62] Europe University Institute, *supra* note 17, at p.8.
[63] „Службен весник на Република Северна Македонија“ бр. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011, 43/2014, 153/2015, 99/2016 и 64/2018).
[64] *supra* note 4.
[65] *supra* note 58, at p.129.
[66] *Ibid.*, at p.129.
[67] Zeng, 'Research on Privacy Protection in Big Data Environment', *Journal of Engineering Research and Applications* (2015), at p.48.

Кога се собираат лични податоци, целта мора да биде јасно одредена и нивната понатамошна употреба треба да се ограничи на постигнување на целта.[68] Целта на прибирањето на личните податоци мора да биде специфична, разумна, и да не го проширува опсегот на употреба. Во овој контекст, може да се користи еден список на негативно однесување, односно да се утврди какво однесување не е дозволено при прибирање и употреба на лични податоци.

- Ограничување на користењето:

Личните податоци не смеат да бидат обелоденети, дадени или искористени за цели, различни од оние кои првично биле назначени, освен при евентуална согласност на лицето или примена на законски одредби.[69]

- Сигурност на податоци:

Сигурноста на личните податоци мора да се заштити од последици како губење или неовластен пристап, уништување или модификации на личните податоци.[70]

- Транспарентност:

Генерално, податоците не смеат да се собираат тајно. Како генерална политика, практиката и постапките кои се поврзани со собраните податоци мора да се транспарентни-граѓаните мора да бидат информирани за постоењето, природата и целта на базата на податоци, како и на институциите кои ги администрираат.[71]

- Пристап на граѓанинот:

Секој граѓанин има право на пристап до своите податоци. Овој пристап вклучува (а) потврда за постоење/непостоење на податоци за граѓаните; (б) добивање копии од податоците во одреден временски период по одредена цена, на разумен начин и во пристапен формат; (в) поткрепување на евентуално одбивање пристап и можност за спорење на наведените аргументи; (г) можност за оспорување на податоци на одреден граѓанин и, кога оспорувањето е оправдано, можност да се избришат, комплетираат или поправат погрешните податоци.[72]

- Одговорност:

[68] *supra* note 58, at p.129.
[69] *Ibid.*
[70] *Ibid.*
[71] *Ibid.*
[72] *Ibid.*, at p.130.

Институциите кои ги собираат податоците мора да бидат одговорни за спроведување на гореопишаните принципи.[73]

[73] *Ibid.*

# ГЛАВА ВТОРА: МЕЃУНАРОДНИОТ КОНТЕКСТ И ИСТОРИЈАТОТ НА ЕВРОПСКОТО ЗАКОНОДАВСТВО ЗА ЗАШТИТА НА ПОДАТОЦИТЕ

## 1. Историски осврт (потеклото на правото на заштита на податоци)

Принципот дека еден човек има право на целосна приватност на неговиот живот и неговиот имот, е стар колку самото обичајно право; меѓутоа од време на време било неопходно точно да се дефинира природата и обемот на таквата заштита. Политичките, социјалните и економските промени повлекоа потреба за нови права.

Во најраните времиња, законот познаваше само права за физичкиот живот и имотот. Правото на живот и слободата на живот претставуваше слобода од одредени воздржувања, а правото на сопственост им обезбедуваше на поедини земји и можност да ги соберат нејзините плодови. Подоцна дојде до признавање на интелектот на еден човек и неговите чувства. Опсегот на овие права се прошири и правото на живот претставуваше право на еден човек да ужива во својот дом, право да биде сам.[74]

Зголемувањето на писменоста и масовната дистрибуција на весниците помеѓу 1880 и 1890 година, ја зголемуваа загриженоста за информатичката приватност на Американците од сите општествени класи. Како никогаш порано, се создаде еден пазар на лични информации, кој предизвикуваше потенцијална закана за многу лица. Интелектуалците и социјалните елити како Warren, Brandeis, Godkin [75] се нафрлија против

[74] Warren and Brandeis, 'The Right to Privacy', in F. D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology* (1984) , at p.75-76.

[75] Г-ѓа Warren беше ќерка на еден Сенатор и нејзиниот сопруг беше еден богат производител на хартија, кој една година претходно се откажа од неговата професија како адвокат за да се посвети на својот бизнис кој го имаше наследено. Социјално гледано, Г-ѓа Warren беше дел од елитната класа и весниците на Бостон објавуваа лични информации за нејзините приватни настани. Поради ова, нејзиниот сопруг се обрати на неговиот поранешен колега Brandeis, исто така правник, и нивната соработка доведе до една статија/документ „Правото на приватност“ кое беше објавено во Harvard Law Review. За повеќе информации, види: W. L. Prosser, Privacy (A legal analysis), во: F D Schoeman, Philosophical Dimensions of Privacy: An Anthology, New York (Cambridge University Press, 1984), p. 104.

влијанието на новинарството и медиумите.[76]

Низ историските етапи, концептот на приватност бил толкуван и како политичка идеја поттикната од прашањата за суверенитет, моќ и автономија. Во 1960-тите и 1970-тите години, кога информатичката технологија се појави како инструмент за јавна администрација, компјутерските проекти предизвикуваа страв во општеството. Во Европа, оние кои ја доживеаја нацистичката окупација, имаа тенденција да не и веруваат на идејата за централизирана база на податоци. Во Велика Британија, воспоставувањето на владини бази на податоци доведуваше до иста загриженост како и проблемите со невработеноста и образованието. Овие ставови се променија помеѓу 1965 и 1990 година. Иако во средината на 1980-тите години анкетите покажуваа висок степен на загриженост во врска со компјутерите, овој проблем ретко беше поврзан со политички аспекти. Во овој период многу корисници се подготвени да се откажат од нивните лични податоци за размена на еден поевтин и побезбеден живот.[77]

Во крајот на XIX век, концептот на правото на приватност во Америка почна да има многу приврзаници од страна на општата јавност, новинари, адвокати, итн.[78] Историчарите за приватноста имаат предложено неколку теории кои ја објаснуваат појавата на правото на приватност.

- Густината на населението - бројот и процентот на луѓето кои живееја во градот се зголемува драстично после граѓанската војна. Северните индустриски градови беа преполни. Можеби зголемувањето на густината на населението во урбаните средини ги направи Американците свесни за физичката приватност. Иако животот во градот им нудеше голем степен на анонимност на луѓето во споредба со животот во руралните средини, истовремено поединците беа принудени да живеат поблиску до соседите и другите членови на семејството.[79]
- Закани на технологијата - конечното објаснување за зголеменото внимание за приватност се фокусира на појавата на нови технологии, почнувајќи со камерата. Освен еден вид на уметност и носталгија, фотографијата исто така претставува

[76] A. L. Allen and M. Rotenberg, *Privacy Law and Society* (2016), at p.36.
[77] Davies, 'Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity', in P. E. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape* (1997) , at p.143-145.
[78] Allen and Rotenberg, *supra* note 76, at p.35.
[79] *Ibid.*

технологија за надзор. Компанијата Кодак ја усовршуваше својата технологија за фотографии.[80] Токму ова беше причината за зголемената загриженост на Warren и Brandeis, слично како што се жалиме ние денеска за луѓето кои снимаат видеа со нивните паметни телефони.[81]

Како што Warren и Brandeis истакнуваат, модерната фотографија и печатењето имаа големо влијание врз способноста на луѓето да го штитат својот живот и приватноста. Телеграфот стана значаен инструмент за бизнисите и општествениот живот, но цената на приватноста беше многу висока: за да се употреби телеграфот за пренесување на пораки, беше неопходно да се открие содржината на пораката до трети лица како што се телеграфската компанија и нејзините вработени. Покрај тоа, за сметководствени цели, многу компании развија практика за чување (барем привремено) на копии од пораките испратени од една до друга канцеларија.[82]

## 2. Првата генерација на норми за заштита на податоци

Во повеќе земји во Европа, првите норми за заштита на податоци беа резултат на процесирањето на електронските податоци од страна на владата и големите корпорации и индустрии. Законот за заштита на податоци на Германската Покраина Хесен (1970), Шведскиот закон за податоци (1973), Статутот за заштита на податоци на Германската Покраина Рајнска област-Пфалз (1974), различните предлози за Германскиот Закон за заштита на податоци (1973), Австриските предлози за Закон за заштита на податоци

[80] Основачот на Кодак, George Eastman, немаше никаква друга цел освен да го создаде најголемиот фотографски бизнис во земјата. За да го оствари тоа, тој сфати дека мора да се доближи до јавноста. Неговата намера да создаде големо барање за неговиот производ беше премногу успешна. Додека другите компании создадоа евтини камери достапни за поширокатa јавност, производот на Eastman стана стандард за индустријата. Најважната културна последица на оваа стратегија беше тоа што целосно се промени концептот за тоа кој може да се занимава со фотографирање. Тоа значи дека веќе на фоторафијата не се гледаше како на професионално занимање, туку почна да се практикува од страна на илјадници луѓе. За повеќе информации, види: Anita L. Allen, Marc Rotenberg, Privacy Law and Society, (2016), p. 36-37.

[81] Allen and Rotenberg, *supra* note 76, at p.36.

[82] *Ibid.*, at p.37.

(1974), и Германскиот федерален закон за заштита на податоци (1977), можат сите да се земат како директна реакција на предвидените национални банки на податоци.[83]

Повеќето од нормите за заштита на податоци на првата генерација не се фокусираат директно во заштитата на приватноста на поединецот, туку се концентрираат на функцијата на обработката на податоците во општеството. Компјутерот се сметаше како опасност за обработка на информациите, и како последица на тоа, заштитата на личните податоци се гледаше како една алатка дизајнирана специјално за да ги спречи овие опасности. Нормите за заштита на податоци се сметаа како дел од еден поголем обид да се совлада технологијата. Ако технологијата е моќен инструмент, се сметаше дека таа мора да се користи во корист на социјалните и политичките промени. Според овој увид, обработката на податоци мораше да се регулира за да биде целосно во согласност со целите на општеството.[84]

Од 1970 година, Европските норми за заштита на податоци се претворија во динамична правна рамка. Додека заштитата на податоци беше еден прифатен концепт, неговата содржина честопати се измени за да се прилагоди на новите технолошки промени и предизвици, земајќи ги во предвид и филозофските и идеолошките трансформации.

## 3. Меѓународното законодавство за приватност

Со развојот на технологијата, прашањата за приватност ја преминуваат државната граница. Правните норми за заштита на приватност усвоени од еден регион можат да имаат значајна улога низ целиот свет.

Меѓународното право на приватност се појави во неколку етапи. Прво, постоеја правилата за човекови права утврдени на крајот на Втората светска војна. Со формирањето на Обединетите Нации и зголемувањето на посветеноста за заштита на правата на поединците, земјите членки се согласија да ја формираат Универзалната

[83] Mayer-Schönberger, 'Generational Development of Data Protection in Europe', in P. E. Agre and M. Rotenberg (eds.), *Technology and Privacy* (1997) , at p.221.
[84] *Ibid.*, at p.223.

декларација за човекови права од 1948 година.[85] Член 12 на оваа Декларација го признава правото на приватност:

„Никој не смее да биде изложен на произволно мешање во приватниот живот, семејството, станот или преписката, нику на напади врз честа и угледот. Секој има право на заштита од законот против вакво мешање или напад.“[86]

Конвенцијата на Советот на Европа за човекови права и основни слободи, донесена во 1950 година, а стапи на сила во 1953 година, со член 8 предвидува дека:

„Секој има право на почитување на неговиот приватен и семеен живот, домот и преписката. “[87]

Член 8 на Европската конвенција за човекови права (ЕКЧП) претставува еден значаен принцип на модерното право на приватност. Државите имаат меѓународна обврска да ја почитуваат оваа Конвенција. Сите држави членки на Советот на Европа ја спровеле Конвенцијата во своето национално законодавство, со што се обврзани да постапуваат во согласност со одредбите на Конвенцијата.[88] Во судската пракса овој член честопати се наведува од страна на судовите кои не се предмет на Европската конвенција. Во последните години, Европскиот суд на правдата, посебно од Европскиот суд за човекови права, за неколку клучни одлуки во врска со приватноста се базирал на текстот на член 8 на Конвенцијата, особено за прашања што се однесуваат на следењето на комуникациите, различните облици на надзор, и заштитата од складирање на лични податоци од страна на државни органи.[89] Иако во Конвенцијата не се вклучуваат современите средства за комуникација, Европскиот суд за човекови права, применувајќи една динамична и широка интерпретација, под опсегот на член 8 на Директивата успеал да

[85] Allen and Rotenberg, *supra* note 76, at p.1297.
[86] *The Universal Declaration of Human Rights*, 1948, available at https://www.un.org/en/universal-declaration-human-rights/.
[87] *European Convention on Human Rights*, 1950, available at https://www.echr.coe.int/Documents/Convention_ENG.pdf.
[88] *Прирачник за европското законодавство за Заштита на податоците* (2016), at p.15.
[89] *Ibid.*

донесе прашања кои се однесуваат на телефонски броеви, телефонски разговори, компјутери, видео надзори, Интернет и е-пошта, и др.[90] Во многу од овие широки пресуди, Европскиот суд за човекови права применува широка дефиниција за поимот „приватен живот“ од член 8 на Европската конвенција за човекови права, проширувајќи го овој концепт подалеку од sидовите на приватната куќа и интимната сфера. Во овој контекст, приватниот живот го опфаќа и развојот на меѓучовечките односи.[91]

Во 1981 година била отворена за потпишување Конвенцијата за заштита на поединците во однос на автоматската обработка на личните податоци (Конвенција бр. 108).[92] Оваа Конвенција беше единствениот правен обврзувачки меѓународен инструмент на полето на заштита на податоци. Во поглед на прибирањето и обработката на личните податоци, оваа Конвенција во член 5 утврдува некои начела, кои се однесуваат на праведно и законито прибирање на податоци, за определени легитимни цели, кои не се користат за цели кои не се спојливи со нив, ниту се чуваат подолго отколку што е потребно. Исто така овој член бара податоците да бидат соодветни, релевантни и точни. Освен тоа, Конвенцијата ја забранува обработката на чувствителните податоци, како што се расата, политичката определба, здравјето, верата, сексуалниот живот и криминалното досие на лицето (член 6).

Усвојувањето на Конвенцијата бр. 108 во 1981 година претставува значајна улога за развојот на нормите за обработка на личните податоци во европските земји. Тоа не значи дека оваа Конвенција беше единствената референца за националните норми

[90] De Hert and Gutwirth, *supra* note 1, at p.16.

[91] Види на пример: ECHR, Niemietz v. Germany, Application No. 13710/88, Judgement of 16 December 1992, каде што Судот смета дека не е можно и не е неопходно да се даде детална дефиниција на поимот ‘приватен живот’. Сепак, според Судот, би било премногу рестриктивно поимот приватен живот да се ограничи на еден ‘внатрешен круг’ во кој поединецот може да го живее својот личен живот како сака и да се исклучи целосно од надворешниот свет (кој не е вклучен во тој круг). Почитувањето на приватниот живот мора да опфати до одреден степен и односи со другите човечки суштества. Понатаму, се чини дека не постои никаква причина за неопфаќање на таквите односи во поимот на ‘приватниот живот’ и исклучување на активностите од професионална или деловна природа, бидејќи евентуално во текот на својот живот сите луѓе имаат можност да развиваат односи со надворешниот свет. Овој поглед е поддржан од фактот дека, како што беше праведно укажано од страна на Комисијата, не е секогаш можно да се разликуваат точно и јасно кои активности на одредена личност се поврзани со неговиот/нејзиниот професионален или деловен живот, а кои не се. Според ова, особено кога станува збор за личност која врши либерална професија, неговата/нејзината работа претставува дел од неговиот/нејзиниот животот до тој степен што е невозможно да се определува дали тие активности беа релевантни за дефинирање на поимот ‘приватен живот’ во одреден момент.

[92] *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 1981, available at https://rm.coe.int/1680078b37.

одобрени после 1981 година, меѓутоа принципите и одредбите на оваа Конвенција се искористија како основа за наредната Европска легислатива.[93]

Повелбата за Основните права на Европската Унија[94] исто така во член 7 го потврдува постоењето на правото на приватен и семеен живот, дом и комуникација, додека член 8 на истата Повелба предвидува дека правото на заштита на податоците има статус на фундаментално човеково право:

„Секој има право да се почитува неговиот или нејзиниот приватен и семеен живот, дом и комуникација.

Ваквите податоци мора да се обработуваат само за конкретни цели и во согласност со засегнатото лице или некоја друга легитимна основа утврдена со закон. Секој има право на пристап до податоците собрани за него или неа и право за исправка на истите.

Почитувањето на овие правила ќе подлежи на контрола од страна на независен авторитет.“

## 4. Законодавството на Европската Унија за заштита на податоци

Од 1970-тите години, кога почна употребата и собирањето на личните информации, структурата на законите за заштита на лични податоци се префрлува од артикулација на основни права, во детални законски рамки со кои се дефинираат конкретни права и одговорности поврзани со собирањето и процесирањето на личните информации.

### 4.1 Директива 95/46/ ЕЗ

Една од најзначајните модерни инструменти за заштита на лични податоци е Европската директива за заштита на лични податоци „во однос на обработката на личните

[93] G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (2014), at p.93.
[94] Charter of fundamental rights of the European Union No2000/C 364/01.

податоци и на слободниот пренос на таквите податоци“ (Директива 95/46/ ЕЗ)[95], донесена во 1995 година од страна на Парламентот и Советот на Европската Унија, која заедно со следните Директиви со кои се регулираат електронските комуникации и задржувањето на податоците, обезбедува една силна и сеопфатна основа со цел да обезбеди усогласување на законот за приватност помеѓу земјите членки на Европската Унија.

### 4.1.1 Целта на Директивата 95/46/ ЕЗ

Целта на Директивата 95/46/ЕЗ е да обезбеди слободно движење на лични податоци од една земја членка на Европската Унија во друга земја членка за да ги обезбеди целите на еден внатрешен пазар, со тоа што основните права и слободи на поединците (особено приватноста) се заштитени (член 1(1)). Оваа Директива е изработена со цел да ги потврди и да ги прошири начелата на правото на приватност кои веќе беа содржани во Конвенцијата бр. 108. Европската Комисија има забележано дека иако во теорија се смета дека и двете цели имаат иста важност, од правен аспект, економската перспектива и аргументите за внатрешен пазар се позначајни.[96] Воспоставувањето на независен надзор како иструмент за подобра усогласеност со правилата за заштита на податоци, се покажало како важен придонес за ефикасното функционирање на европското законодавство за заштита на податоците (во 2001 година тој инструмент беше преземен во правото на Советот на Европа со Дополнителниот протокол кон Конвенцијата бр.108).

Иако оваа Директива се смета како инструмент за заштита на личните податоци, треба да се истакне дека Директивата формално не го подржува поимот „заштита на лични податоци“ или „лични податоци“. Официјалниот наслов на Директивата не се однесува на ‘личните податоци’, туку на заштитата на поединците во однос на обработката на нивните лични податоци. Освен тоа, во Директивата се опишува една од нејзините две главни цели, која ги обврзува земјите членки на Европската Унија да ги штитат не ‘личните

[95] *Directive 95/46/EC*, 1995, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.
[96] *First Report on the Implementation of the Data Protection Directive (95/46/EC) COM(2003) 265 Final* (2003), available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF.

податоци', туку основните права и слободи на поединците, а особено правото на приватност.[97]

### 4.1.2 Обем на Директивата 95/46/ЕЗ

Во преамбулата на Директивата 95/46/ЕЗ се наведуваат принципите за заштита на правата и слободите на поединците, особено правото на приватност,[98] кои им даваат суштина на принципите содржани во Конвенцијата 108. Заедно со националните норми на земјите членки на ЕУ, Конвенцијата 108 е основен извор на Директивата 95/46/ЕЗ, како резултат на целта на Европската Комисија да комбинира различни пристапи на европското законодавство.

Директивата 95/46/ЕЗ се однесува на 'автоматската обработка на личните податоци целосно или делумно, како и на обработката на личните податоци на друг начин кои се дел на еден систем или се наменети да создадат дел на еден архивски систем.'[99] Обемот е поширок од Конвенцијата 108, која се однесува само на автоматската обработка на личните податоци.

Лични податоци, според Директивата, се 'сите информации кои се однесуваат на идентификувано физичко лице или физичко лице кое може да се идентификува, а лице кое може да се идентификува е лице чиј идентитет може да се утврди директно или индиректно, посебно врз основа на матичен број на граѓанинот или врз основа на едно или повеќе обележја специфични за неговиот физички, физиолошки, ментален, економски, културен или социјален идентитет.'[100] Во споредба со Конвенцијата 108, Директивата 95/46/ЕЗ е порестриктивна во смисла на тоа што таа не се применува на податоци кои се однесуваат на правни лица. Според Конвенцијата 108, заштитата на податоците се занимава, пред сè, со заштитата на физички лица, меѓутоа, договорните страни во рамките

[97] González Fuster, *supra* note 93, at p.129.
[98] Recital 11 of Directive 95/46/EC.
[99] Article 3(1) of Directive 95/46 EC.
[100] Article 2(a) of Directive 95/46 EC.

на националното законодавство можат да ја прошират заштитата на податоците и на правни лица, како што се деловни компании и здруженија.[101]

Два големи исклучоци го разграничуваат обемот на примена на Директивата 95/46/ЕЗ. Прво, Директивата не се применува врз дејности кои се надвор од опсегот на Законот на Заедницата, и во случаите кога обработката на податоците се однесува на јавната безбедност, одбраната, државната безбедност и во подрачјата на кривичното право. И второ, Директивата не се применува за обработката на личните податоци на едно физичко лице за лична или домашна активност.[102]

## 4.2 Директивата 97/7/ЕЗ

Во средината на 1990-тите години зборот „приватност“ не беше користен само во однос на заштита на лични податоци, туку и во областа на електронските комуникации. Во оваа смисла, во 1997 година се усвои Директивата 97/7/ЕЗ за заштита на консуматорите во однос на договорите на далечина,[103] која експлицитно наведува дека треба да се заштити приватноста на консуматорите, особено од несакани средства за комуникација.[104] Во овој контекст, Директивата 97/7/ЕЗ постави ограничувања за употребата на одредени средства за комуникација во далечина за склучување на договори.[105]

## 4.3 Директивата 97/66/ЕЗ

Друг значителен правен инструмент на Европската Унија претставува Директивата 97/66/ЕЗ за обработка на личните податоци и заштита на приватноста во

[101] Article 3(b) of Convention 108.
[102] Article 3(2) of Directive 95/46 EC.
[103] Directive 97/7/EC, 1997, OJ L 144, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A31997L0007
[104] Recital (17) of the Directive 97/7/EC
[105] Ibid.

телекомуникацискиот сектор[106], која беше усвоена во декември 1997 година**.** Оваа Директива обезбедува усогласување на одредбите на земјите членки на Европската Унија и бара да се обезбеди еднакво ниво на основните права и слободи, а особено на правото на приватност, во однос на обработката на личните податоци во телекомуникацискиот сектор. Исто така бара да се обезбеди слободно движење на податоците и на телекомуникациските средства и услуги во Заедницата.[107] Иако Директивата 97/66/ЕЗ формално беше замислена како *lex specialis*[108] за еден конкретен сектор во телекомуникацискиот сектор, сепак, таа не беше ограничена за таа цел. Во правилата со кои се дефинира обемот на оваа Директива, се наведува дека нејзините одредби „ги специфицираат и ги дополнуваат одредбите на Директивата 95/46/ЕЗ".[109] Меѓутоа, оваа Директива не претставува јасна слика до кој степен ги подобрува и ги надополнува одредбите на Директивата 95/46/ЕЗ.

## 4.4 Регулативата (ЕЗ) бр. 45/2001

Бидејќи Директивата 95/46/ЕЗ се однесува само на државите членки на Европската Унија, бил неопходен дополнителен правен инструмент со цел да се воспостави заштита на податоците при обработка на личните податоци од страна на институциите и телата на Европската Унија. Таквата задача ја исполнува Регулативата (ЕЗ) бр. 45/2001 на Европскиот Парламент и на Советот од 18 декември 2000 година за заштита на поединците во врска со обработката на личните податоци од страна на институциите и телата на Заедницата и со слободно движење на таквите податоци.[110]

[106] Directive 97/66/EC, 1997, OJ L 24, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31997L0066.
[107] Article 1(1) of Directive 97/66/EC.
[108] González Fuster, *supra* note 93, at p.141.
[109] Article 1(2) of Directive 97/66/EC.
[110] Regulation (EC) No 45/2001, 2001, *OJ L 8, available at:* https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32001R0045.

## 4.5 Директивата 2002/58/ЕЗ

За да се постигне потребната јасност за обработката на податоците во електронските комуникации, подетални одредби беа наведени во Директивата 2002/58/ЕЗ на Европскиот Парламент и на Советот од 12 јули 2002 година во врска со обработката на личните податоци и заштитата на приватноста во секторот за електронските комуникации (Директива за приватност и електронски комуникации).[111] Како што е наведено во преамбулата на оваа Директива, таа обезбедува заштита на основните човекови права, и ги следи принципите признати особено од Повелбата за основните права на Европската Унија, особено правата кои произлегуваат од членот 7 и 8 на оваа Повелба.[112] Со Директивата 2002/58/ЕЗ се дава дефиниција за податоци на сообраќај, кои се дефинираат како податоци кои се обработуваат за пренос на една комуникација во електронска комуникациска мрежа што се неопходни за да се идентификува крајниот претплатник или корисник.[113] Директивата исто така воведе една нова категорија на податоци, 'податоци на локација', опишувајќи ги како податоци кои се обработуваат во електронска комуникациска мрежа, и кои се однесуваат на географската положба на опремата на корисникот на јавно достапни електронски комуникациски услуги.[114]

Во врска со податоци за сообраќајот, Директивата 2002/58/ЕЗ предвидува дека земјите членки на Европската Унија имаат можност да донесат законодавни мерки за задржување на податоците за сообраќајот за одреден период, кога станува збор за одредени цели, како што е безбедноста, одбраната, или превенција на кривични дела.[115] Според оваа одредба, за наведените цели, земјите членки имаат можност да постапуваат против одредбите за заштита на податоци за сообраќајот, според кои податоците за сообраќајот треба да се избришат или да се анонимизираат во најкраток можен рок.[116]

[111] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.
[112] Recital 2 of Directive 2002/58/EC.
[113] Article 2(b) of Directive 2002/58/EC.
[114] Ibid. 2(c).
[115] Article 15(1) of Directive 2002/58/EC.
[116] Article 6 of Directive 2002/58/EC.

## 4.6 Директивата 2006/24/ЕЗ

Горенаведената можност за задржување на податоците за сообраќајот подоцна се појави повторно во правото на Европската Унија, во форма на обврска на земјите членки на задржување на таквите податоци во период од 6 месеци до 2 години, со цел да се обезбеди достапност до таквите податоци кога станува збор за истрага, откривање или гонење на кривични дела. Оваа обврска беше наведена со Директивата 2006/24/ЕЗ за задржување на податоци што се создадени или обработени во врска со обезбедувањето јавно достапни електронски комуникациски услуги или јавни комуникациски мрежи и за изменување на Директивата 2002/58/ЕЗ[117] (Директива за задржување на податоци), прогласена за неважечка на 8 април 2014 година од страна на Европскиот суд на правдата.

Обврската за задржување на податоците за сообраќајот во период од 6 месеци до 2 години се смета како сериозна пречка за почитување на приватниот живот и заштита на личните податоци (како две основни права во согласност со Повелбата за основните права на Европската Унија), бидејќи задржаните податоци се однесуваат на прецизни информации за приватниот живот на лицата чии податоци се чуваат. Директивата за задржување на податоци, во овој контекст, надминува некои граници и барања поставени од принципот на пропорционалност.[118] Судот забележува дека задржувањето на таквите податоци овозможува, пред сè: да се дознае идентитетот на едно лице со кого комуницирал субјектот чии податоци се задржуваат, и според тоа, да се идентификува времето на комуницирањето и местото од каде комуникацијата се остварила; да се дознае фреквенцијата на комуникациите на лицето чии податоци се задржуваат со трети лица во одреден временски период. Како резултат на тоа, податоците кои се задржуваат, обезбедуваат многу прецизни информации за приватниот живот на лицата чии податоци се задржуваат, како што се навиките на секојдневниот живот, местото на живеење, дневни активности, социјални односи со трети лица, итн.[119]

---

[117] Directive 2006/24/EC, 2006, OJ L 105, available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32006L0024.

[118] Види: Judgment of the Court of 8 April 2014 in Joined Cases C-293/12 and C-594/12, available at: http://curia.europa.eu/juris/documents.jsf?num=C-293/12.

[119] Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, Press Release no.54/14 of 8 April 2014, available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.

## 4.7 Рамковната одлука за заштита на податоците 2008/977/ЈНА

Рамковната одлука 2008/977/ЈНА за заштита на личните податоци што се обработуваат во рамките на полициската и правосудната соработка во кривични предмети (Рамковна одлука за заштита на податоците),[120] како и Директивата 2002/58/ЕЗ и Директивата 2006/24/ЕЗ, во својата преамбула зборува за почитување на основните права признати особено од страна на Повелбата за човекови права на Европската Унија, а особено за правото на приватност и заштита на личните податоци кои произлегуваат од член 7 и член 8 на оваа Повелба.[121] Рамковната одлука за заштита на податоците во голема мера се потпира на начелата содржани во Конвенцијата бр.108 и во Директивата 95/46/ЕЗ за заштита на податоците, истакнувајќи дека заштитата на личните податоци им служи на основните права и слободи, а особено на правото на приватност.[122] Меѓутоа, спротивно на Директивата за заштита на податоци и Директивата бр.108, Рамковната одлука за заштита на податоци не содржи принципи за слободен проток на податоци.

Целта на Рамковната одлука за заштита на податоци е да обезбеди заштита на личните податоци на физички лица кога нивните податоци се обработуваат во рамките на полициската и правосудната соработка во кривични предмети[123] со цел на спречување, истрага, откривање или прогон на кривични дела или поради извршување на казни.[124]

Според последните реформи во правото на Европската Унија за заштита на личните податоци, во 2018 година Рамковната одлука за заштита на податоци беше укината бидејќи стапи на сила Директивата на Европскиот Парламент и на Советот на Европа од 27 април 2016 година за заштита на физичките лица во однос на обработката на личните податоци од страна на надлежните органи за целите на спречување, откривање и

[120] Council Framework Decision 2008/977/JHA, 2008, OJ L 350, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977.
[121] Recital 48 of Council Framework Decision 2008/977/JHA.
[122] Ibid. Article 1(1).
[123] Article 1(1)of Council Framework Decision 2008/977/JHA.
[124] *supra* note 20, at p.149.

гонење на кривични дела или извршување на кривични казни, и за слободното движење на тие податоци и за укинување на Рамковната одлука на Советот 2008/977/ЈНА.[125]

## 4.8 Регулативата бр. 1049/2001

Регулативата бр. 1049/2001 во врска со јавниот пристап до документи на Европскиот Парламент, на Советот и на Комисијата (Регулатива за пристап до документи)[126] во име на отвореност, транспарентност, и на правото на пристап на документи, го гарантира правото на пристап до документи на Европскиот Парламент, на Советот и на Комисијата. Меѓутоа, Регулативата вбројува неколку ограничувања од овој принцип, така што согласно член 4 (1)(б) на Регулативата, Европските институции имаат право да го одбијат пристапот до нивните документи кога правото на пристап до документи доаѓа во судир со правото на заштита на податоците и интегритетот на поединците, односно кога со откривањето (пристапот) на некој документ се откриваат податоци на друго лице.

## 4.9 Општа регулатива за заштита на лични податоци- Регулатива (ЕУ) 2016/679

На 23 јануари 2012 година Европската Комисија претстави еден предлог за нови правила за заштита на лични податоци. Со новите мерки Комисијата имаше за цел да ја зајакне заштитата на податоците на граѓаните на Европската Унија и да воспостави унитарни мерки за остатокот на светот. Овие правила стапиле на сила на 25 мај 2018 година, така што во истиот период Европската директива за заштита на податоци 95/46/ЕЗ беше заменета од страна на Општата регулатива за заштита на личните податоци (во

[125] Directive (EU) 2016/680, 2016, OJ L 119, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680.
[126] Regulation (EC) No 1049/2001, 2001, OJ L 145, available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32001R1049.

понатамошниот текст GDPR или 'Регулатива'),[127] кои се основани врз принципите и одредбите на Директивата 95/46/ЕЗ. За разлика од Директивата, овој закон има директен ефект, што значи не треба да се имплементира во националните законодавства за да има легални последици.[128]

Целта на Општата регулатива за заштита на личните податоци е да ги усогласува законите за приватност низ цела Европа, да ги штити правата на приватност на граѓаните на Европската Унија и да го реконструира начинот на кој организациите се однесуваат кон приватноста на поединците. Иако клучните принципи за приватност и заштита на лични податоци остануваат исти со претходната директива, односно со Директива 95/46/ЕЗ, Регулативата донесува нови сознанија и измени во регулаторните политики, како што се:

- Зголемен територијален опсег (вонземска применливост) – од регулативен аспект, најголемата промена во приватноста на податоците доаѓа со проширувањето на надлежноста на GDPR, бидејќи овој закон се однесува на сите компании кои обработуваат податоци на субјектите на личните податоци кои живеат во ЕУ, без оглед на локацијата на компанијата. Со други зборови, иако територијалниот опфат на GDPR најпрво се однесува на компаниите кои ја вршат својата дејност во земјите членки на Европската Унија, законот има правни последици и за компаниите надвор од ЕУ кои:
  a) ги пласираат (продаваат) своите производи на жителите на ЕУ, односно ги нудат своите услуги на граѓаните на ЕУ[129], или кои
  b) го следат однесувањето на граѓаните на ЕУ.[130]

Општата регулатива за заштита на личните податоци (GDPR) ја прави својата применливост многу јасна – таа се однесува на обработката на личните податоци од контролори и обработувачи во ЕУ, без оглед на тоа дали обработката се одвива во ЕУ или не.

- Големи казни – компаниите кои ги кршат одредбите на GDPR можат да бидат казнети со казна до 20 милиони евра. Ова е максимална парична казна што може да

[127] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.
[128] S. Kulk and F. Borgesius Zuiderveen, *Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe* (2018), The Cambridge Handbook of Consumer Privacy, at p.15.
[129] L. B. Beasley, *Did You Know GDPR Compliance Affects Your Data Collection for European and Some Non-European Residents?*, 2018, available at https://beasleydirect.com/gdpr-countries/ (last visited 4 December 2019].
[130] *Ibid.*

се изрече за најсериозни прекршувања, на пример, кога не постои согласност од клиентот за обработка на неговите/нејзините податоци, или кога доаѓа до повреда на основните принципи за заштита на приватноста.[131]

- Согласност – условите за согласност се зајакнуваат, а компаниите не можат да користат долги правила и услови, кои би биле неразбирливи за физичките лица. Барањето за согласност мора да биде дадено во разбирлива и лесно достапна форма, а приложена треба да биде и целта за обработка на податоците во одредениот случај.[132]

Во GDPR, меѓу другото, се вклучуваат нови обврски за прашања кои се однесуваат на анонимизацијата на податоците, прекуграничниот пренос на податоците, изедначувањето на службеници за заштита на податоци, итн.

### 4.9.1 Влијание врз организациите

Општата регулатива за заштита на лични податоци (GDPR) е еден од најстрогите закони во светот. Секоја компанија, организација или агенција, чија дејност е предмет на овој закон, треба да се придржува на одредбите на овој закон. Меѓу другите обврски кои компаниите треба да ги применат во рамките на законот на ЕУ за заштита на податоците, се вклучуваат:

(1) Информирање - личните податоци мора да бидат обработени правично и законски и само за определени легални цели (член 6 (а) на GDPR). Оваа обврска бара од компаниите да бидат транспарентни за тоа како и за какви цели ги собираат податоците и истите не можат и не смеат да ги користат за нови или дополнителни цели, освен ако таквата употреба е фер (т.е. во разумни очекувања на поединците).[133]

[131] За повеќе информации види: An overview of the main changes under GDPR and how they differ from the previous directive, available at: https://eugdpr.org/the-regulation/ (last visited 13 January 2019).
[132] *Ibid.*
[133] Ustaran, 'The Scope of Application of EU Data Protection Law and Its Extraterritorial Reach', in *Beyond Data Protection:Strategic Case Studies and Practical Guidance* (2013) , at p.137.

(2) Пропорционалност - личните податоци треба да бидат соодветни, релевантни и не претерани во однос за целите за кои тие се собрани или понатаму обработени (член 6 (ц)).

(3) Зачувување и бришење на податоци – личните податоци не треба да се чуваат подолго отколку што е потребно (член 6 (е)).

(4) Безбедност на податоците – личните податоци треба да бидат безбедни, користејќи соодветни технички и организациски мерки за заштита од неовластена или незаконска обработка, и против случајна загуба, уништување или оштетување (член 17(1)).

(5) Меѓународни ограничувања за трансфер на податоци – личните податоци не треба да се пренесуваат во земја надвор од Европската Унија, освен ако се преземат соодветни мерки за заштита (член 25(1)).

(6) Почитување на правата на субјектите на податоците – таквите права вклучуваат:

- Право на пристап до една копија на информациите,[134]
- Право да се спротивстават на користење на нивните информации кои можат да им нанесат штета или неволја,[135]
- Право да бараат корегирање, блокирање, бришење или уништување на неточни податоци,[136]
- Право да ги спротивстават одлуките донесени од автоматски средства (т.е. одлука која е донесена од машина, односно од програми на Вештачка интелегенција, без човечка интервенција,[137]
- Право на приговор за информациите што се користат за директни маркетинг цели.[138]

[134] *Ibid.*
[135] *Ibid.*
[136] *Ibid.*
[137] *Ibid.*
[138] *Ibid.*

# ГЛАВА ТРЕТА : СОГЛАСНОСТ КАКО ПРАВНА ОСНОВА ЗА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ

## 1. Елементи на валидна согласност

Согласноста на субјектот на личните податоци претставува слободно дадена изјава на волја на субјектот на податоци, со која се согласува за обработка на неговите лични податоци за однапред определени цели. Во рамките на Општата регулатива за заштита на личните податоци (GDPR), согласноста останува законска основа за пренос на личните податоци. Сепак, дефиницијата за согласност е значително ограничена. Регулативата истакнува некои елементи на валидната согласност, кои се разликуваат од Директивата 95/46/ЕЗ во неколку контексти.

Суштински елемент при одлучување дали субјектот на податоци се согласува за одредена обработка на своите лични податоци претставува анализата дали постои јасна индикација за желбите на субјектот на податоците. GDPR појаснува во дефиницијата за согласност дека субјектот на податоците треба да даде афирмативна согласност за обработка на податоци. Во одредбите на GDRR се наведува дека согласноста мора де се даде слободно, специфично и недвосмислено.[139] Додека Директива 95/46/ЕЗ исто така бара недвосмислена согласност (член 7 (а) на Директивата), GDPR бара таквата согласност да се изрази со изјава или со јасна афирмативна акција. Рецитал 32 на GDPR појаснува дека афирмативна акција за давање согласност за обработка на податоци може да вклучува штиклирање во одреден простор на една веб-страница, избирање на технички алатки за услугите на информатичкото општество, или една изјава или однесување, која јасно укажува на одобрение за обработка на личните податоци на една личност. Неактивноста се смета како несоодветна согласност за обработка на податоците. Во овој контекст, GDPR има судир со Директивата 95/46/ЕЗ.

[139] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection regulation) OJ L 119, 2016, recital 32.

Во согласност со правилата за транспарентност, Директивата 95/46/ЕЗ бара од контролорот на податоци да даде точни и целосни информации за сите релевантни прашања (Рецитал 38 на Директивата), вклучувајќи ја природата на информациите кои ќе бидат обработени, целите за обработка, идентитетот на контролорот и идентитетот на сите други приматели на податоци (член 10 на Директивата). Согласноста мора да се даде специфично на обработката на информациите во одреден момент и контролорот не може да бара согласност за идна обработка на лични податоци. Додека согласноста може да се даде со изречна изјава од страна на субјектот на податоците, исто така се смета дека согласноста е дадена во случаи на неактивност во околности кога тоа дејство (неактивност) јасно означува давање на согласност. Ова произлегува од член 3, точка х на Директивата 95/46/ЕЗ за заштита на податоци:

„Согласност е секое слободно дадено, конкретно и информирано навестување на желбите на субјектот на податоците, според кои субјектот на податоците ја означува неговата согласност за обработка на податоците“.

Според ова, Директивата остава отворена можност за обработка на податоци и во случаи кога субјектот не податоците не дава конкретна, експлицитна согласност.

Можноста за давање на согласност за обработка на личниите податоци со неактивност се отстранува со одредбите на GDPR, барајќи од субјектот на податоците да даде јасна изјава или афирмативна акција. GDPR вклучува три нови барања, и тоа:

1. Прво, член 7 (3) му овозможува на субјектот на податоците да ја повлече неговата/нејзината согласност во секое време и „тоа би требало да биде исто толку лесно колку што е давањето на согласност“. Контролорите мораат да го известат субјектот на податоците за неговото/нејзиното право за повлекување на согласност пред истата да биде дадена од страна на одредената личност.

2. Второ, во рецитал 43 на GDPR се дава претпоставката дека согласноста не е слободно дадена ако има „јасна нерамнотежа помеѓу субјектот на податоците и контролорот, особено кога контролорот е јавен орган“. Според ова, контролорот не може да бара согласност како услов за користење на една услуга ако одредената личност има

право да ги користи таквите услуги и без давање на согласност, освен ако обработката на податоците е потребна за користење на услугата.

3. Трето, GDPR означува дека согласноста треба да биде специфична и конкретна за секоја операција на обработка на податоците. За да се задоволат барањата за специфичност од член 7 на GDPR, согласноста за обработка на податоците мора „јасно да се разликува“ од било кои други прашања поставени во писмена форма и мора да се обезбеди „во разбирлива и лесно достапна форма, со користење на јасен и едноставен јазик“.[140]

Меѓутоа, законот ги ослободува контролорите од обврската за добивање на согласност за понатамошна и дополнителна обработка на истите податоци, ако целите за обработка се компатибилни. Така, „обработката на личните податоци за други цели освен за оние за кои биле првично собрани, е дозволена само во случај кога обработката е компатибилна со целите за кои личните податоци првично беа собрани“.[141] Рецитал 50 укажува дека компатибилноста треба да се оценува според одредени фактори, вклучувајќи, *inter alia*, врската меѓу целите на понатамошната обработка со првичната обработка на податоците, разумните очекувања на субјектот на податоците, природата и последиците на понатамошната обработка, и постоењето на соодветни заштитни мерки за субјектот на податоците. Така на пример, согласно член 5 (1) (б) на GDPR, дополнителна обработка за архивирање од јавен интерес, статистички цели или научни и историски истражувања општо се сметаат како компатибилни цели, па затоа не се бара согласност од субјектот на податоците. Овие исклучоци се пошироко објаснети со член 89 на GDPR, кој означува дека контролорите не мора да ги избришат податоците откако субјектот на податоците ќе ја повлече својата согласност. Меѓутоа сметам дека овие одредби се многу широко формулирани и можат да доведат до различни несогласувања, бидејќи не може таксативно да се определува кои услови треба да се исполнат за една одредена ситуација да се смета како јавен интерес. Таквите одредби можат да доведат до различни толкувања на законот од страна на различни личности. Исто така оваа одредба има влијаение врз принципот на ограничување на обработка на податоци, принципот за преносливост на

[140] *Ibid.*, at recital 39.
[141] *Ibid.*, at recital 50.

податоци, и правото на субјектот на податоците да се спротивстави и да биде информиран за сите операции кои се однесуваат на обработката на неговите/нејзините податоци.

## 2. Конкретна (експлицитна) согласност за посебни категории на лични податоци-чувствителни податоци

Општата регулатива за заштита на личните податоци (GDPR) во член 9 бара повисоко ниво на согласност - експлицитна согласност за обработка на таканаречени „посебни категории на лични податоци“. Овие категории се однесуваат на личните податоци кои се особено чувствителни во врска со фундаменталните права и слободи, па затоа, според член 9 на законот, заслужуваат посебна заштита. Тие вклучуваат податоци за раса или етничка припадност, политички размислувања, религиозни или филозофски убедувања или членство во синдикати, како и обработка на генетски податоци, биометриски податоци според кои уникатно се идентификува едно физичко лице, податоци за здравјето на една личност и податоци поврзани со сексуалниот живот или сексуалната орентација на едно физичко лице.[142]

Принципот на експлицитна согласност останува ист како и според Директивата 95/46/ЕЗ, која исто така бара од контролорите да добијат експлицитна согласност за обработка на посебните категории на лични податоци (член 8 (2) на Директивата). Според Директивата, член 29 Работната група на Европската Комисија ја дефинира согласноста како „сите тие ситуации во кои на лицата им се презентира предлог да се согласуваат или да не се согласуваат со одредена употреба или откривање на нивните лични податоци, и тие активно одговараат на прашањето, усно или во писмена форма“.[143] GDPR исто така им дозволува на земјите членки на Европската Унија да донесат домашни закони кои ја ограничуваат обработката на посебните категории на податоци, дури и кога субјектот на податоците експлицитно се согласува (рецитал 10 на GDPR).

[142] *Ibid.*, at article 9(1).

[143] European Commision Article 29 data protection Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, 01197/11/EN WP187, Article 8.2 (a), available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

Единствената разлика меѓу Директивата 95/46/ЕЗ и Општата регулатива за заштита на личните податоци се однесува на проширувањето на дефиницијата за чувствителни податоци од страна на Општата регулатива за заштита на личните податоци. Така, според овој закон, за чувствителни податоци се сметаат и генетските податоци, биометриските податоци и податоците за сексуалната ориентација на една личност.

## 2.1 Генетски податоци

Поимот 'генетски податоци' се однесува на сите податоци, од било кој тип, што се однесуваат на наследни карактеристики на поединецот.[144] Генетските податоци, според член 4 на Општата регулатива за заштита на личните податоци се дефинираат како:

„лични податоци кои се однесуваат на наследени или стекнати карактеристики на физички лица кои даваат уникатни информации за физиологијата или здравјето на физичкото лице, и кои произлегуваат особено од анализата на еден биолошки примерок на одреденото физичко лице".

Генетските информации се директно поврзани со здравствената состојба на поединецот, бидејќи се собираат и се користат во здравствената грижа и од страна на здравствените работници. Согласно член 9, параграф 1 на GDPR, собирањето и обработката на генетските информации е забрането, освен ако:[145]

- Субјектот на податоци дал експлицитна согласност за обработка на тие податоци;
- Обработката е неопходна за извршување на обврски и остварување на специфични права на контролорот или на субјектот на податоци;

[144] Lehtonen, 'Genetic Information and the Data Protection Directive of the European Union', in D. Beyleveld et al. (eds.), *The Data Protection Directive and Medical Research Across Europe* (2004) , at p.107.
[145] *supra* note 4, at article 9, paragraph 2 (a-j).

- Обработката е неопходна за да се заштитат виталните интереси на субјектот на податоци или друго физичко лице кога субјектот на податоци е физички неспособен да дава согласност;
- Обработката се прави за легитимни активности со соодветни заштитни мерки од страна на фондација, здружение, или било кое друго непрофитабилно тело со политичка, филозофска, верска или синдикална цел и под услов обработката да се однесува само на членовите или на поранешните членови на телото и податоците да не се откриваат надвор од тоа тело без согласност на субјектите на податоците;
- Обработката се однесува на лични податоци кои субјектот на податоци сам ги објавил;
- Обработката е неопходна во судски постапки;
- Обработката е неопходна од причини за јавен интерес, врз основа на законодавството на Европската Унија или земјите членки, според кои се обезбедуваат соодветни мерки за заштита на основните права и интереси на субјектот на податоци;
- Обработката е неопходна за цели на превентивната медицина;
- Обработката е неопходна за научни или историски истражувања.

Интересно е да се забележи дека Директивата 95/46/ЕЗ нема специфични одредби кои се однесуваат на користењето на генетските податоци во медицински истражувања, сепак, во некои случаи Директивата спомнува медицински цели и има одредби кои се однесуваат на користење на податоците кои се поврзани со здравствената состојба на едно лице. Така, генетските податоци, како и податоците за здравствената состојба на еден човек, се таканаречени 'сензитивни информации' и нивната обработка е забранета (член 8(1) на Директивата 95/46/ЕЗ). За обработка на генетските податоци, како и за другите сензитивни податоци треба да се даде експлицитна согласност од субјектот на податоците или одобрение од еден надзорен орган, во случаи кога интересот на општеството е поголем и порелевантен од правото на приватност на еден човек.[146]

Што се однесува на експлицитната согласност за обработка на податоците за здравствената состојба на еден човек, научниците истакнуваат дека овој критериум може

[146] Lehtonen, *supra* note 144, at p.112.

да биде многу проблематичен кога станува збор за обработка на такви информации за цели на истражување. На пример, епидемиолозите набројуваат неколку аргументи кои тврдат дека одредбите за експлицитна согласност не треба да се земат во предвид. Според нив, барањето на согласност од пациентот би било невозможно, премногу скапо и би одземало премногу време. Од друга страна, тие се сомневаат дека одредени пациенти немаат способност да дадат експлицитна согласност. Во овие случаи, ова барање би можело да доведе до селективен одговор кој би ја намалил вредноста на истражувањето.[147]

Член 8(3) на Директивата 95/46/ЕЗ предвидува исклучок на забраната за обработка на здравствените податоци, кога тоа е потребно за потребите на превентивната медицина, медицински дијагнози, обезбедување на нега и третмани или поради управување на здравствени услуги, така што податоците се обработуваат од страна на професионални здравствени лица, во согласност со националното законодавство, со обврска за професионална тајност. Меѓутоа, како што Lehtonen тврди, многу е важно да се дефинира здравствениот систем и што тој претставува, затоа што во модерното општество, многу функции се поврзани со социјалните услуги, и здравствениот систем честопати е дел од социјалните служби, така што здравствените услуги и обработката на медицинските податоци може да се користат за финансиски одлуки во јавниот сектор.[148]

Заштитата на приватноста на поединците во медицинските истражувања не зависи само од законот за заштита на податоци, туку и од етичките правила, кои треба да се оценат од страна на етичките комитети.

На прв поглед, изгледа дека автоматската обработка на сите генетски информации е ограничена. Меѓутоа, некои информации кои се обработуваат во здравствениот систем воопшто не се сметаат како сензитивни информации. На пример, возраста и местото на живеење на едно лице, имаат длабоко влијание врз тоа каде и од кого ќе биде третиран пациентот. Овие информации не се сметаат како медицински информации, иако се обработуваат од страна на здравствени работници.[149] Според ова, фактот дека некои информации се собираат и се обработуваат од страна на медицинскиот персонал не ги прави таквите податоци сензитивни податоци.

[147] Nys, 'The Scope of Exemptions for Medical Research', in D. Beyleveld et al. (eds.), *The Data Protection Directive and Medical Research Across Europe* (2004) , at p.52-53.
[148] Lehtonen, *supra* note 144, at p.109.
[149] *Ibid.*, at p.107.

## 2.2 Биометриски податоци

Биометриските податоци според Општата регулатива за заштита на личните податоци се лични податоци кои идентификуваат една личност врз основа на „специфична техничка обработка“ на физичките, физиолошките карактеристики, или карактеристиките на однесувањето на една личност, според кои се утврдува единствена идентфикација на тоа лице (член 4 (14)). Во рецитал 51 се забележува дека фотографиите се квалификуваат како биометриски податоци само кога тие се обработуваат според специфични технички средства кои овозможуваат уникатна идентификација или автентикација на едно физичко лице.

Од перспективата на личните податоци, биометриските податоци претставуваат лични податоци, и како такви треба да се обработуваат во рамките на законодавството на Европската Унија за заштита на лични податоци. Во однос на принципот на индивидуално учество, процедурите за идентификација претставуваат голем ризик за заштита на личните податоци кога тие се чуваат во централизирани бази на податоци и поединецот не може да има целосна контрола врз своите лични информации. Биометријата исто така има потенцијал да собере дополнителни информации, кои можат да откријат емотивни состојби на одредени лица или информации за нивната медицинска состојба. Овие практики можат длабоко да влијаат врз принципот на пропорционалност.[150] Примерите вклучуваат слики од мрежницата/ирисот што можат да го откријат здравствениот статус (дијабетес) на една личност, како и навики во животот (употреба на дроги), или препознавање на одење што може да открие мускулно-скелетни пореметувања. Исто така овие слики можат да ја откријат емоционалната состојба на една личност, како што е на пример депресија, гласовните снимки можат да откријат ларингитис или рак на грлото, и слично. Биометријата на човекот, компјутерскиот интерфејс може да открие и психијатриски и невролошки состојби, бидејќи некои сензори можат да детектираат хируршка модификација на телото.[151]

Според горенаведеното, некои биометриски податоци би можеле да се сметаат како чувствителни податоци. Така на пример, скенерот за снимање на целото тело, кој се

[150] Venier and Mordini, *supra* note 33, at p.21.
[151] *Ibid.*, at p.22.

користи особено на големи аеродроми, претставува грижа за загрозување на приватноста, бидејќи произведува слики на голи тела на физички лица и нивната медицинска состојба, кои се сметаат како дел од личните податоци. Загриженоста околу заштитата на приватноста се врти околу заштитата на личните податоци што ги генерираат скенерите, односно на складирањето и пренесувањето на сликите генерирани од тие скенери.

Кога станува збор за биометриски податоци, голема загриженост претставува користењето на технологијата за препознавање на лице. Како што застапниците за приватноста напишаа во една изјава: „Ние веруваме дека луѓето имаат основно право на приватност. Тие имаат право да контролираат кој ги добива нивните чувствителни информации и како се споделуваат тие информации, и не постои сомнеж дека биометриските информации се исклучително чувствителни. Можете да ги промените вашата лозинка и број на кредитна картичка, но не можете да ги менувате отпечатоците или димензиите на вашето лице. Преку препознавање на лицето, овие непроменливи, физички факти можат да се користат за да ве идентификуваме, оддалечено и во тајност.“[152]

Степенот на чувствителност на биометриските податоци варира во зависност од видот на биометриските карактеристики на една личност (физички карактеристики или однесувањето).

## 2.3 Нови видови на чувствителни податоци во современиот свет: идентификатори и податоци за контакт

Традиционално, личните податоци беа се тоа што можеме да го наречеме „библиографски податоци“. Овој концепт се однесува на податоци директно поврзани со минатите или сегашните настани во животот на поединците: нивната домашна адреса, нивните здравствени проблеми, нивната локација во одреден момент, итн. Ние сме навикнати да ги класифицираме овие податоци според нивната чувствителност и, врз основа на тоа, да применуваме одредени правила. Меѓутоа, кога се зборува за оваа

[152] *Privacy Advocates Statement on NTIA Facial Recognition Process FINAL*, 2015, available at https://www.documentcloud.org/documents/2104377-privacy-advocates-statement-on-ntia-facial.html (last visited 7 July 2019].

категорија на податоци во денешно време, треба да се има во предвид фактот дека капацитетот за складирање на овие податоци се зголемува секој ден сè повеќе, и станува сè поевтино, што предизвикува собирање на повеќе тривијални податоци и моментални парчиња од нашиот живот. Ризикот повеќе не се поврзува со природата на податоците кои се собираат, туку со множењето на собраните податоци и можноста за дефинирање на индивидуалните профили.[153]

Покрај библиографските податоци, еволуцијата на Интернетот води кон целосно два нови вида на податоци.

(1) Првиот вид на податоци може да се опише како идентификатори, бидејќи главната улога на овие податоци е да овозможат поврзување на податоци кои припаѓаат на различни бази на податоци, со цел да го профилизираат, односно да го идентификуваат поединецот кој стои зад собраните податоци. Овие податоци доаѓаат на увид како резултат на достапноста и користењето на методи за идентификација и автентикација на корисниците на електронски услуги. Овие методи им овозможуваат на корисниците да се идентификуваат себеси и заедно со системите за управување со идентитетот, се овозможува пристап до информатички ресурси или услуги.[154] Освен тоа, можно е да се извлекуваат нови информации за корисниците од други извори, односно од сите веб-страници без никакви ограничувања.[155] Овие „дигитални идентитети“ се еден вид на метаподатоци кои овозможуваат поврзување на информации за поединци достапни на различни бази на податоци. Поради ова, треба да се потенцира опасноста на користењето на истиот дигитален идентитет во различни области на електронски услуги. Јасно е дека иста идентификација или метод за пристап во различни бази на податоци може полесно да се памти од луѓето, меѓутоа ова ја зголемува можноста за поврзувањето на податоците за една личност.

Примарните дигитални идентификатори се директно поврзани со една личност, како што се: име, адреса, телефонски број, лозинка или електронски потпис. Секундарните идентификатори се индиректни, но се засноваат на познати информации за

[153] Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?', in S. Gutwirth, Y. Poullet and P. De Hert (eds.), *Data Protection in a Profiled World* (2010) , at p.11.
[154] *Ibid.*
[155] Rundle, 'International Personal Data Protection and Digital Identity Management Tools', *Berkman Center Research Publication No. 2006-06* (2006) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=911607.

поединецот. Така на пример, колачиња, IP адреси и сл., иако не мора да се знае кој е поединецот зад компјутерот, тие се поврзани со страницата која ја користи поединецот; овие техники за лична идентификација ги совладуваат луѓето или деловните субјекти кои ги сместуваат таму.[156]

(2) Другиот вид на податоци кои остануваат релевантни во нашето информатичко општество се контактните податоци. Податоците за контакт се користат со цел да им овозможат на контролорите на податоци да стапат во контакт со субјектот на податоци. Во овој контекст можеби е интересно да се потенцира како мобилните телефони се повеќе и повеќе ќе се користат од системите на амбиентална интелигенција[157] за испраќање на рекламни пораки, но исто така и за утврдување на точната локација на одредената личност. Значи, податоците за контакт ја овластуваат компанијата која ги процесира податоците да донесе одлуки за лицето идентификувано од податоците за контакт.[158]

[156] Poullet, *supra* note 153, at p.11-12.

[157] Во информатичката технологија, амбиентална интелегенција (AmI) се однесува на електронските средини кои се чувствителни и одговараат на присуството на луѓето. За повеќе информации, види: Cook, Augusto and Jakkula, 'Ambient Intelligence: Technologies, Applications, and Opportunities', *Pervasive and Mobile Computing* (2009) , at pp.277-298.

[158] Poullet, *supra* note 153, at p.12.

# ГЛАВА ЧЕТВРТА: РОДИТЕЛСКА СОГЛАСНОСТ ЗА ОБРАБОТКА НА ЛИЧНИТЕ ПОДАТОЦИ НА ДЕЦАТА

## 1. Вовед

Честопати децата стануваат предмет на мониторинг уреди кои генерираат лични податоци за нив,[159] а во многу законски рамки нема експлицитни правила за заштита на нивната приватност.

Според едно истражување спроведено во 2015 год., повеќе од 80 % од тинејџерите ги користат социјалните медиуми како една значајна арена за личен и социјален развој.[160] На глобално ниво, се проценува дека еден од тројца корисници на Интернет се на возраст под 18 години.[161] На Интернет децата не само што уживаат возбудливи можности за играње, учење, самоизразување, експериментирање со своите идентитети, итн., но исто така откриваат големи количини на податоци. Поради нивните посебни карактеристики на однесување, емоционална нестабилност и импулсивност, децата (особено тинејџерите) се сметаат како ранлива група во компарација со возрасните луѓе.[162] Според емпириските податоци на интернет-сајтовите на ЕУ, 9 % од децата на возраст од 11-16 години во Европа доживеале злоупотреба на нивните лични податоци.[163]

[159] Lupton and Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights', 19 *New Media and Society* (2017) , available at http://journals.sagepub.com/doi/full/10.1177/1461444816686328 , at p.1.

[160] Montgomery, 'Youth and Surveillance in the Facebook Era: Policy Interventions and Social Implications', 39 *Telecommunications Policy* (2015) , available at http://dx.doi.org/10.1016/j.telpol.2014.12.006 , at p.771. Montgomery and Chester, 'Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework', 1 *European Data Protection Law Review* (2015) , available at https://edpl.lexxion.eu/article/EDPL/2015/4/6.

[161] Livingstone, Carr and Byrne, 'One in Three: Internet Governance and Children's Rights', *Global Commission on Internet Governance Paper Series No. 22* (2015).

[162] Bessant, 'Hard Wired for Risk: Neurological Science, "the Adolescent Brain," and Developmental Theory', 11 *Journal of Youth Studies* (2008) , at pp.347-358. (Bessant тврди дека некои млади луѓе понекогаш се изложени на ризик не затоа што нивните мозоци се различни, туку затоа што тие немале искуство или можност да развијат вештини и проценки за одредени активности и искуства).

[163] S. Livingstone et al., *Risks and Safety on the Internet: The Perspective of European Children: Full Findings and Policy Implications from the EU Kids Online Survey of 9-16 Year Olds and Their Parents in 25 Countries*, 2011, EU

Поради горенаведените предизвици и потребата за подобра заштита на детската приватност во електронските активности, со усвојувањето на Општата регулатива за заштита на личните податоци (GDPR) се воведоа нови правила за пренос на личните податоци, особено за согласноста на субјектите на личните податоци за обработување на нивните лични информации, кое се бара како законска основа за таквиот пренос. Со овој закон, кој стапи на сила во мај 2018 год., Европската Унија ја истакна улогата на родителската согласност, со цел да ги заштити личните податоци на малолетниците кои имаат пристап до онлајн комуникации. Со член 8 кој бара родителска согласност за обработка на личните податоци на децата, GDPR воведува специфична заштита за децата, со ограничување на нивната способност да се согласат за обработката на нивните лични податоци, без овластување на еден родител. За првпат, законот бара родителите да дадат согласност пред да се обработуваат податоците на лицата помлади од 16 години од страна на давателите на услугите на информатичкото општество.

Одредбите се однесуваат на децата кои се под 16 годишна возраст, но законот им овозможува на земјите членки на Европската Унија да постават пониска возраст, односно овој принцип да се применува за лица кои се помлади од 13 години (член 8 (1) на GDPR). Така, доколку поинаку не е предвидено со домашна регулатива на земјите членки на Европската Унија, контролорите имаат обврска до добијат согласност од еден родител или старател при обработка на личните податоци на дете под 16 годишна возраст. Исто така, контролорите мора да прават „разумни напори“ за проверка на фактот дека родителот или старателот обезбедил соодветна согласност (член 8(2) на GDPR). Можноста на земјите членки на Европската Унија да донесат различни правила за возраста на детето, би можеле да создаде значителни предизвици за компаниите кои нудат меѓународни услуги. Како што Lievens и Verdoodt забележуваат, ако земјите членки на Европската Унија заземат различен пристап за ова прашање, тоа би значело дека во пракса би имале различни правни мерки низ цела Европска Унија. Тоа би било голем финансиски товар за компаниите кои нудат онлајн услуги во различни земји на Европската Унија, бидејќи за да

Kids Online Network, available at http://eprints.lse.ac.uk/33731/1/Risks and safety on the internet%28lsero%29.pdf (last visited 11 February 2019].

се придржуваат кон различните правила утврдени во земјите членки на ЕУ, тие би требало да преземат дополнителни напори и инвестиции.[164]

Важноста на заштитата на децата во дигиталните комуникации се спомнува неколку пати во GDPR, меѓутоа во пракса можно е да има суштински ограничувања поради постоењето на националните закони или кодекси на однесување на одредени држави. Анализата на законодавната историја на член 8 на GDPR докажува дека нема доволно докази во смисла на усвоените материјални барања во финалната верзија на законот. Најчесто дебатата е фокусирана на економското влијание врз активностите на контролорите на податоците и дигиталниот единствен пазар, наместо за заштитата на субјектите на личните податоци. За да се применуваат новите одредби за согласност според GDPR, важна задача претставува објавувањето на политиката на приватност на давателите на дигиталните услуги.

Меѓутоа, на глобално ниво, се посветува големо внимание на соодветната заштита на податоците на децата. Казна од 170 милиони американски долари против YouTube,[165] казна од 5,7 милион долари против ТикТок за нелегално собирање на лични информации на децата,[166] казна од 32,5 милиони долари против Apple поради дозволување на децата да купат или да симнат апликации без согласност на родителите,[167] и казна од 20.700 долари против едно училиште во Шведска поради експериментирање со технологија за препознавање на лицето на децата,[168] покажуваат дека проблемот е сериозен и има соодветно внимание.

---

[164] Lievens and Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation', 34 *Computer Law and Security Review* (2018) , available at https://doi.org/10.1016/j.clsr.2017.09.007 , at p.272.

[165] C. Metz, *The Week in Tech: YouTube Fined $170 Million Over Child Privacy Violations*, 2019, The New York Times, available at https://www.nytimes.com/2019/09/06/technology/youtube-fine-child-privacy.html (last visited 26 November 2019].

[166] J. Fingas, *FTC Fines TikTok $5.7 Million over Child Privacy Violations*, 2019, available at https://www.engadget.com/2019/02/27/ftc-fines-tiktok-over-child-privacy/#:~:targetText=The creators of TikTok are,its lip-syncing video app. (last visited 25 November 2019].

[167] L. Whitney, *Apple to Refund at Least $32.5M for Kids' in-App Purchases*, 2014, available at https://www.cnet.com/news/apple-to-refund-at-least-32-5m-for-kids-in-app-purchases/ (last visited 25 November 2019].

[168] M. Ehrenkranz, *Sweden's First GDPR Fine Goes to a High School Piloting Facial Recognition Attendance*, 2019, available at https://gizmodo.com/swedens-first-gdpr-fine-goes-to-a-high-school-piloting-1837616893 (last visited 25 November 2019].

## 2. Член 8 на Општата регулатива за заштита на лични податоци (GDPR) – истражување на контекстот

За разлика од Директивата 95/46/ЕЗ која беше донесена пред ерата на Интернетот, и која немаше експлицитни одредби во однос на заштитата на децата во електронските комуникации, регулаторниот контекст на GDPR беше драстично променет. Зголемувањето на вниманието за заштита на приватноста на децата дојде како резултат на движење, односно развој на неколку фактори (контекстуални и легални), кои имаа голема улога во признавањето на децата како посебни субјекти во GDPR.

### 2.1 Контекстуални фактори

Постојат неколку настани кои можат да се сметаат како подготовка на теренот за усвојување на специфични одредби во GDPR во врска со заштитата на малолетните лица во однос на обработката на нивните лични податоци.

Прво, во последните години се посвети големо внимание на децата и нивните права во политиката на Европската Унија. Важноста на промовирање на правата на децата се истакнува многупати низ различни документи и законодавни средства на Европската Унија. Согласно член 24 на Европската повелба за основни права[169] Европската Унија се посветува да ги заштити правата на децата. Покрај тоа, важноста за ефективна заштита на правата на децата се истакнува како главен приоритет во стратешките документи на Европската Унија.[170]

[169] Charter of Fundamental Rights of the European Union
*OJ C 326, 26.10.2012.*

[170] Види: Commission (EC),'European Strategy for a Better Internet for Children' (Communication) COM/2012/0196 final, 2 May 2012; Commission (EC),'An EU Agenda for the Rights of the Child' (Communication) COM/2011/0060 final, 15 February 2011 (воспоставува голема посветеност во сите институции на Европската Унија и во сите земји членки на Европската Унија за промовирање, заштита и исполнување на правата на детето во сите релевантни политики на Европската Унија; наведува дека стандардите и принципите на Конвенцијата на Обединетите Нации за Правата на детето мора да продолжат да ги водат политиките и активностите на Европската Унија кои имаат влијание врз правата на детето; повикува да се земе во предвид „перспективата за детските права" во сите закони на Европската Унија кои влијаат врз децата).

Овие документи ги трансформираат целите на Европската Унија во активности. Потребата за обезбедување и зајакнување на правата на приватност на децата се истакнува во сите предлози на законодавството на Европската Унија и сите донесени одлуки беа признати од страна на институциите на Европската Унија. Всушност, во Агендата на Европската Унија за Правата на детето[171] достигнувањето на високо ниво на заштита на децата во дигиталниот простор (вклучително и нивните лични податоци) се признава како една од нејзините цели, додека целосно се почитува нивното право на пристап до Интернет во корист на нивниот социјален и културен развој.[172] Посветеноста на институциите на Европската Унија за промовирање, заштита и исполнување на правата на децата во сите релевантни области значи дека при изготвувањето на законодавните предлози треба да се земе во предвид најдобриот од интерес за детето.

Истражувањата кои покажуваа ризици и загрозување на правата на децата на Интернет исто така имаа важна улога во политиката за приватност на Европската Унија. Така на пример, според едно истражување во 2014 година се потврдуваше дека најважните грижи за децата остануваат поврзани со злоупотребата на нивните лични податоци на Интернет, како што е хакирање на нивни профили на социјални мрежи, создавање на лажни профили и персонализација.[173]

Неколку инспекции на терен предизвикаа загриженост за зголемувањето на бројот на веб-страници и апликации за мобилни телефони користени од млади деца, и недостатокот на специфични правила на овие веб-страници за заштита на податоците кои би биле во корист на уникатните потреби на децата како субјект на податоци. Во 2012 година, Федералната комисија за трговија (FTC) во САД ги разгледа информациите кои им беа дадени на корисниците на одредени апликации од страна на 400 деца, и откри дека многу од тие информации имаат недостаток на транспарентност и јасно објавување на практиките за собирање на податоци на децата.[174] Во 2015 година, додека GDPR беше во процес на разгледување, 29 органи за заштита на податоци (DPA) од целиот свет спроведоа еден заеднички преглед на 1494 веб-страници и апликации насочени кон

[171] Commission (EC),'An EU Agenda for the Rights of the Child', COM/2011/0060 final, 15 February 2011.
[172] *Ibid.*
[173] G. Mascheroni and K. Ólafsson, *Net Children Go Mobile: Risks and Opportunities* (2014), 2nd Ed. Educatt.
[174] Federal Trade Commission (FTC), *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing (Staff Report)* (2012), available at https://www.ftc.gov/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing.

деца.[175] Во резултатите се наведоа многу проблеми, како што се несоодветни политики за приватност неприлагодени за деца, прекумерно собирање на лични податоци на децата, и често објавување на овие податоци на трети лица. Во врска со верификација на возраста на детето и родителската согласност, во извештајот се вели дека „иако многу страници и апликации тврдат дека во нивните политики за приватност го спречуваат пристапот за деца под одредена возраст, само 15 % од веб-страниците и апликациите имаа верификација на возраст или забранување за помлади деца за пристап кон страницата или апликацијата. Исто така се открива дека некои од овие контроли не функционираа (на пример дете што кажува дека има десет години сè уште може да пристапи до страницата), а другите правила беа само пасивни (на пример еден pop-up прозорец кој укажува дека дете под одредена возраст не треба да пристапи до страницата). Вреди да се обежи дека само 24 % од страниците и апликациите го поттикнаа вклучувањето на родителите.“[176]

## 2.2 Легални фактори: недостаток на хармонизација на законодавството на Европската Унија

Вниманието за заштитата на децата на Интернет беше предизвикано од недостатокот на унитарни мерки за заштита на детската приватност низ цела Европска Унија. Директивата 95/46/ЕЗ не успеа експлицитно да го реши проблемот на согласност бидејќи во многу земји членки на Европската Унија имаше недостиг на јасност. Прашањето - на која возраст можат децата да дадат согласност за обработка на нивните лични податоци дури иронично стана наречено ‘прашање за милион евра’ од страна на експертите за заштита на личните податоци.[177] Недостатокот на усогласување на законите за заштита на лични податоци низ Европската Унија предизвикуваше правна несигурност

[175] GPEN, *2015 GPEN Sweep – Children’s Privacy*, 2015, available at https://www.garanteprivacy.it/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf (last visited 26 November 2019].
[176] *Ibid.*
[177] Macenaite and Kosta, 'Consent for Processing Children’s Personal Data in the EU: Following in US Footsteps?', 26 *Information & Communications Technology Law* (2017) , at p.151.

за контролорите на податоци кои беа изложени на различни правни мерки при собирање на лични податоци на одредени лица.[178]

## 3. Посебни услови за согласност на децата

Општо, согласно член 7 на Општата регулатива за заштита на лични податоци (GDPR),[179] постојат четири специфични услови во однос на давање на согласност за обработка на лични податоци (кои исто така имаат голема важност во контекст на согласноста на малолетните лица), и тоа:

(А) Контролорот на податоци треба да има можност да докаже дека согласноста на субјектот на податоци е предвидена за одредени цели (член 7(1) на GDPR).

Контролорите на податоци имаат одговорност да докажат дека согласноста е дадена на валиден начин за една специфична операција на обработка на лични податоци. Тие исто така треба да користат сигурни средства за добивање на согласност, земајќи ја во предвид чувствителноста на секоја обработка на лични податоци во одредена ситуација. Европскиот супервизор за заштита на податоци (EDPS) смета дека во Европската регулатива за заштита на податоци треба да се прецизира дека при посета на една веб-страница треба активно да се штиклира кутија за да се обезбеди валидна согласност. Тој исто така потсетува дека товарот на докажување лежи врз контролорот, и сигурноста на согласноста може да варира во зависност од користените средства (штиклирање на одредении кутии, или електронски потписи).[180]

(Б) Кога субјектот на податоци дава согласност како дел од една писмена изјава што се однесува на друга цел, барањето за согласност треба да биде претставено во јасно

[178] European Data Protection Supervisor (EDPS), *Opinion on the Communication: A Comprehensive Approach on Personal Data Protection in the European Union*, 2011, available at https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf (last visited 11 November 2019].

[179] *supra* note 4.

[180] European Data Protection Supervisor (EDPS), *Opinion on the Data Protection Reform Package*, 2012, available at https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf (last visited 22 November 2019].

различна форма од другите елементи напишани во декларацијата, во разбирлива и лесно достапна форма, користејќи едноставен јазик (член 7 (2) на GDPR).

Примената на овие правила за валидна согласност е особено сложена кога се зборува за малолетни лица кои користат електронски услуги. На пример, барањето за слободно давање на согласност станува многу сложено во околности кога децата би можеле да ја дадат својата согласност без знаење на нивните родители. Ова е особено проблематично со оглед на тоа што многу често нивните избори можат да се манипулираат и да се искористуваат за комерцијални цели заради нивната голема моќ на трошење.[181] Исполнувањето на барања за информирана согласност е голем предизвик во случај на малолетни лица, бидејќи нивното ниво на разбирање и можност да ги предвидуваат потенцијалните последици се разликуваат од возрасните. Иако политиките за приватност на различни веб-страници претставуваат една вообичаена практика и многу од нив формално следат законски барања за задолжителни информации, не може секогаш да се каже дека тие ја постигнуваат својата цел.[182] Освен тоа, со оглед на сложените техники за профилирање и голема анализа на податоци кои се тешки за разбирање дури и за возрасните, многу малолетни лица немаат можност правилно да го измерат значењето на нивната согласност во однос на влијанието врз нивната приватност и лична автономија. Многу политики за приватност се долги, тешки за наоѓање и навигација, напишани на комплициран јазик и се над капацитетот на разбирањето на едно просечно возрасно лице.[183]

(B) Согласноста треба да се даде слободно, без надворешен притисок.

Ако има надворешно влијание со цел да се манипулира одлуката на субјектот на податоците за обработка на неговите податоци, се смета дека согласноста не е дадена слободно. Меѓутоа, секое вежбање на надворешен притисок не доведува до неважечка согласност. Рецитал 42 на GDPR јасно истакнува дека согласноста не се смета дека е дадена слободно ако субјектот на податоци нема оригинален или слободен избор или не е во состојба да ја повлече својата согласност без нанесување на штета. Слично на тоа,

[181] Macenaite and Kosta, *supra* note 177, at p.159.
[182] Van Eecke and Truyens, 'Privacy and Social Networks', 26 *Computer Law and Security Review* (2010) , available at http://dx.doi.org/10.1016/j.clsr.2010.07.006 , at p.542.
[183] Micheti, Burkell and Steeves, 'Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand', *Bulletin of Science, Technology & Society* (2010) , at pp.130-143.

согласноста нема да се смета за слободно дадена доколку се однесува на повеќе од една операција на обработка на лични податоци и не е можно да се издвои согласноста за секоја индивидуална операција за обработка на податоци (рецитал 43). Покрај тоа, рецитал 43 исто така објаснува дека согласноста не треба да се смета за слободно дадена, па затоа и обработката на личните податоци не треба да се потпира на тоа, во случаите кога има јасна нерамнотежа помеѓу субјектот на податоците и контролорот на податоците, особено кога контролорот е јавен орган и според сите околности се укажува дека согласноста не е дадена слободно (рецитал 43 на GDPR).

## 4. Разбирање на родителската согласност во пракса

Практичното спроведување на член 8 на Општата регулатива за заштита на лични податоци предизвикува многу прашања, како на пример: За кои услуги ќе се применат нормите на член 8?; Како ќе се ограничуваат услугите наменети за деца?; Како треба да се провери согласноста и возраста на едно лице? Овие прашања заслужуваат големо внимание не само од страна на научниците, но исто така од страна на органите за заштита на податоците.

Општите одредби на GDPR се применуваат за секоја услуга која вклучува обработка на лични податоци, целосно или делумно со автоматски средства или кога личните податоци се дел од архивски систем (член 2 на GDPR). Член 3 експлицитно наведува дека се однесува на бесплатни услуги понудени на субјектот на податоци во Европската Унија од страна на еден контролор или процесор кој не подлежи на територијата на Европската Унија. Спротивно на тоа, родителската согласност, регулирана со член 8 на GDPR има специфичен материјален обем и се применува за услугите на информатичкото општество кои се нудат директно на децата. За да се дефинира значењето на специфичниот обем во смисла на член 8, GDPR ја користи дефиницијата на 'услуга на информатичкото општество', содржана во Директивата (ЕУ) 2015/1535,[184] која ги дефинира таквите услуги како „сите услуги кои обично се

[184] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society

обезбедуваат за надомест, на далечина, преку електронски пат и лично барање на примателот на услугата“ (точка (б) од член 1 на Директивата 20115/1535). Поимот „надомест“ според оваа дефиниција може да се толкува на рестриктивен начин, според кој се бара од корисникот на податоци да плати за одредената услуга. Меѓутоа, треба да се има во предвид дека во денешно време повеќето услуги нудени во информатичкото општество се бесплатни и не бараат директен надомест од корисниците (на пример социјални мрежи, играње преку Интернет, праќање е-пошта и др.). Според ова, концептот на надомест и поимот на „услуги на информатичкото општество“ треба да се толкува пошироко.

Како резултат на пошироко толкување на услугите на информатичкото општество, родителската согласност според одредбите на GDPR има широк потенцијален опсег на примена на онлајн услуги. Единствен јасен предуслов е фактот дека личните податоци се обработуваат од страна на давателот на услугата, и согласноста претставува правна основа врз која се заснова прибирањето и обработката на личните податоци. Меѓутоа, хипотетички може да се постави прашањето дали електронските услуги директно наменети за деца можат да останат надвор од областа на родителската согласност, со оглед на фактот дека иако многу веб-страници можат да се користат без активно обезбедување (давање) на лични податоци (како што се вестите или веб-страници за забава), сепак личните податоци честопати се собираат на пасивен начин, т.е. преку техники за следење како што се на пример колачиња (cookies).[185]

## 4.1 Услуги кои им се нудат директно на децата

Одредбите на приватност според Општата регулатива за заштита на лични податоци (GDPR) се однесуваат на електронски услуги кои им се нудат директно на децата. Намерата на законодавецот да создаде специфичен режим за заштита на личните податоци на децата е јасна, меѓутоа точното разликување на услугите кои се објект на

services (codification), available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535&rid=4 (last visited 23 November 2019).

[185] Macenaite and Kosta, *supra* note 177, at p.171.

овие одредби е комплексно прашање. Во пракса, услугите насочени кон децата оставаат еден мал дел од целокупниот број на услуги до кои децата можат да имаат пристап, да ги користат или во кои можат да се регистрираат. Според ова, големиот број на општи и мешани услуги достапни до општеството создава големи грижи за приватноста на децата во пракса. Различни студии во Европа[186] и Северна Америка[187] известуваат дека најпопуларните веб-страници што децата ги користат во денешно време (на пример Facebook, Youtube, Google) честопати не се наменети за децата (барем не за оние под 13 годишна возраст). Според едно истражување спроведено во 2018 година, 95 % од тинејџерите имаат пристап до паметен телефон, а 45 % велат дека скоро постојано се на Интернет.[188] Ова потврдува дека во пракса голем број на мали деца всушност се корисници на веб-станиците кои не се наметени за малолетни деца. Според тоа, младиот неовластен корисник на електронските услуги сè уште останува активен корисник и се третира како возрасен и има пристап до исти информации како возрасните луѓе, без оглед на нивните посебни потреби или ризици во онлјан комуникацијата. Останува прашањето: До кој степен може Европската регулатива за заштита на податоци да ги утврди правилата за родителска согласност кога станува збор за услуги наменети за општата публика? Во овој контекст, GDPR нема јасни одредби. Меѓутоа, Законот за заштита на приватноста на децата на Интернет (COPPA)[189] на Соединетите Американски Држави наведува неколку критериуми според кои може да се утврди дали една веб-страница е наменета за деца или не. Овие критериуми вклучуваат: визуелна содржина, употреба на анимирани карактери или стимулации ориентирани кон децата, музика или друга аудио содржина, возраст на модели, присуство на познати деца или познати личности кои им се допаѓаат на децата, јазик или други карактеристики на веб-страницата или електронската услуга, како и тоа дали рекламите кои се појавуваат на одредената веб-страница се ориентирани кон деца.[190]

[186] UK Information Commissioner's Office (UK ICO), *Consultation GDPR Consent Guidance*, 2017, available at https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf (last visited 23 November 2019].
[187] Steeves, 'Young Canadians in a Wired World, Phase III: Life Online', *MediaSmarts* (2014).
[188] M. Anderson and J. Jiang, *Teens, Social Media & Technology*, 2018, available at https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/ (last visited 23 November 2019].
[189] Federal Trade Commission, Children's Online Privacy Protection Rule Vol. 78, No. 12 of 17 January 2013.
[190] *Ibid.* § 312.2 (1).

Треба да се истакне дека одредбите за заштита на личните податоци на децата не можат да ги спречат децата да имаат пристап до одредени веб-страници. Законот има за цел да им даде на родителите контрола над прибирањето, користењето или откривањето на личните податоци на децата при користење на Интернет услуги.[191]

## 4.2 Верификување на родителската согласност

Општата регулатива за заштита на лични податоци[192] на Европската Унија бара од контролорот да ја верификува родителската согласност, односно да провери дека согласноста е всушност дадена или овластена од родителот на детето. Согласно член 8, точка 2 на овој закон, контролорот треба да направи разумни напори за да провери дека согласноста е дадена или е овластена од носителот на родителската одговорност над детето, земајќи ја во предвид достапната технологија.

Оваа одредба може да има различни импликации за контролорите на податоци. Должноста да прават разумни напори за 'потврдување' на согласност се однесува на верификација на родителската согласност само еднаш (т.е. единствен момент на верификација) кој треба да се исполнува пред собирањето на личните податоци на децата. Според ова, законот не бара потврдена согласност, туку само напори за потврдување на согласноста. Упатувањето за потврдена, односно верифицирана согласност би значело дека согласноста не може да се даде ако истата не може да се провери од страна на контролорите. Во оваа смисла, контролорите на податоци би имале две опции: или да обезбедат верификација преку технолошки средства, или кога тоа не е можно, да се воздржат од потврдување на согласност. Меѓутоа, во одредбите за родителската согласност, законот не бара потврдена согласност. Оваа значи дека согласноста не треба да се провери, односно да се верификува во секое време (т.е. постојана можност за

[191] Federal Trade Commission (FTC), *Complying with COPPA: Frequently Asked Questions*, 2017, available at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General Audience (last visited 20 November 2019].
[192] *supra* note 4.

повторно потврдување), кое наметнува помал товар за контролорите на податоци кои нудат онлајн услуги насочени кон децата.[193]

Барањето за вложување на разумни напори за верификација на родителската согласност им дозволува на контролорите да покажат дека тие направиле разумни напори за потврдување на согласноста и, во околности кога тоа не е можно, контролорот на податоците сè уште може да се потпре на непроверена согласност за обработка на податоците на децата. Оваа одредба претставува флексибилен стандард за одговорност, бидејќи доволно е да се направат разумни напори за добивање на потврдена родителска согласност, и не се бара тоа нужно да се добие во сите случаи. Ова алудира на фактот дека контролорите на податоци не можат да гарантираат потврдена согласност поради ситуации кога тоа е над нивната контрола.[194] Во оваа смисла, товарот на докажување ослабува.[195]

### 4.2.1 Стандарди за верификација на родителската согласност

Кога обработката на лични податоци се заснова на согласност, контролорот треба да докаже дека субјектот на податоци се согласил за обработката на неговите лични податоци (член 7(1) на GDPR). Општата регулатива за заштита на лични податоци (GDPR) утврдува општ услов за верификување на родителската согласност, преку преземање на разумни напори од страна на контролорите, земајќи ја во предвид достапната технологија (член 8 (2)). Меѓутоа, оваа одредба остава простор за различни толкувања.

Прво, не е јасно колку напор треба да направат контролорите за верификација на согласноста во ситуации  кога е тешко да се добие проверена (веродостојна) родителска согласност (на пример, кога не може да се открие местото на живеење на родителот или кога информациите за контакт се недостапни, или кога правата на родителите над детето се прекинати, а законскиот застапник на детето не може да се пронајде). Во овој контекст,

[193] Macenaite and Kosta, *supra* note 177, at p.177.
[194] *Ibid.*
[195] Hornung, 'A General Data Protection Regulation For Europe? Light And Shade In The Commission's Draft Of 25 January 2012', *SCRIPTed 64* (2012).

останува прашањето: Колку напор треба да се направи од страна на контролорите за да стапат во контакт со родителот или законскиот застапник на детето? Како ќе се документираат разумните напори? Освен тоа, ако контролорот на податоци нема родителска согласност, а сепак ги обработува личните податоци на децата, важно е да знаеме според какви критериуми ќе се процени дали напорите се разумни.

Второ, специфичните механизми кои можат да ги користат контролорите на податоци за проверување на родителската согласност не се наведуваат во одредбите на GDPR, и поради тоа бараат понатамошно објаснување. На контролорите на податоци им останува да изберат решенија за добивање на родителска согласност, која може да доведе до многу високи трошоци за спроведување. Поради ова, важно е да се воспостават јасни упатства за тоа кои алатки за верификација на согласност се сметаат за доволни и како ќе се проценат трошоците и придобивките за верификација на согласност. Во спротивно, нејаснотијата на разумни напори и алатки за потврдување на согласноста може да доведе до непочитување на законските услови за родителска согласност.

Додека дефиниции за ‘разумни напори’ и ‘механизми за проверување’ не се обезбедат во одредбите на GDPR, им останува на судовите да ги разгледаат и да ги проценат напорите на контролорите и обемот на технолошките способности за добивање на верифицирана родителска согласност, според конкретните факти и околности на секој случај.

# ВТОР ДЕЛ –ПРАВАТА НА СУБЈЕКТОТ НА ПОДАТОЦИ И НИВНОТО СПРОВЕДУВАЊЕ

Главниот принцип на законите за заштита на лични податоци е дека лицата треба да имаат влијание врз обработката на нивните податоци од страна на други лица или организации. Според овој принцип произлегуваат правилата за согласност, кои им овозможуваат на носителите на податоци да одлучуваат во каква мера и за какви цели ќе се прибираат и обработуваат нивните лични информации.

Општата регулатива за заштита на лични податоци (GDPR)[196] им дозволува на луѓето, во своите капацитети како корисници на електронските комуникации, т.е. како потрошувачи, граѓани и слично, спектар на специфични права кои можат да ги остварат под посебни услови. Организациите треба да им понудат на поединците информации како можат да ги остварат овие права при користење на електронски комуникации и услуги и треба веднаш да ги исполнат нивните права. Неуспехот да го прават тоа може да доведе до големи казни предвидени со закон.

Правата на субјектот на податоците никогаш не се апсолутни. Секогаш има исклучоци и услови кои треба да се земат во предвид. Така на пример, правото на изразување може да има влијание врз правото на бришење на податоци.

Освен тоа, правата на субјектот на податоците можат да бидат контекстуални. Така на пример, во некои околности контролорите кои обработуваат лични податоци не можат да ги исполнат правата на субјектот на податоците. Добар пример е правото на повлекување на согласност. Согласноста е само една од законските основи за обработка на лични податоци, и, ако постои друга законска основа, која е во согласност со одредбите на GDPR, нема основа за повлекување на согласноста.

[196] *supra* note 4.

# ГЛАВА ПРВА: ОСНОВНИ ПРАВА НА СУБЈЕКТОТ НА ПОДАТОЦИТЕ

## 1. Фундаментални права на субјектот на податоците

Главниот принцип на законите за заштита на податоци е дека лицата, односно субјектите на податоци треба да учествуваат и да имаат влијание во обработката на нивните податоци од страна на трети лица или организации.[197]

Општата регулатива за заштита на личните податоци (GDPR)[198] содржи поглавје посветено на „Правата на субјектот на податоците“ (Поглавје 3), кое ги детализира и ги збогатува правата кои постоеја во Директива 95/46/ЕЗ, меѓутоа додава нови права, како што е таканаречената „право да бидеш заборавен“ и правото на преносливост на податоци. Сепак, ниту едно од овие права не се сосема нови во законот за заштита на податоци на Европската Унија, бидејќи и двете права своите корени ги имаат во Директивата 95/46/ЕЗ, и тоа во рамките на правото за бришење на податоци и правото на примање копија за обработените податоци.

GDPR во член 12 воведува правила кои се однесуваат на постапките и механизмите за остварување на правата на субјектот на податоците, вклучувајќи и средства за електронски барања, со кои се бара одговор за барањето на субјектот на податоците во определен рок.[199]

Според GDPR, правата на субјектот на податоците (кои се прикажани на слика 1) се систематизирани во три категории:

(1) информации и пристап (право на субјектот на податоци да биде информиран – член 14, и право на пристап до податоци – член 15);

(2) исправка и бришење (право на исправка – член 16, право да бидеш заборавен – член 17, и право на преносливост на податоци – член 20); и

[197] L. A. Bygrave, *Data Protection Law. Approaching Its Rationale, Logic and Limits* (2002), at p.63.
[198] *supra* note 4.
[199] *Ibid.*, at paragraph 2, 3.

(3) право на приговор и профилирање (право на приговор – член 21 и право да не бидеш предмет на профилирање – член 22).


**Слика 1. Правата на субјектот на податоците.**

Во овој дел накратко ќе бидат објаснети сите права на носителот на податоци, а пошироко ќе се зборува за правото да бидеш заборавен и правото на преносливост на податоци во глава 2 и глава 3 од овој дел, како две нови права во обемот на законот за заштита на личните податоци, предвидени со Општата регулатива за заштита на лични податоци (GDPR), кои беа многу дебатирани од страна на општата јавност, медиумите и истражувачите.

Европската регулатива за заштита на лични податоци (GDPR) се смета како една од најважните реформи на Европската Унија во обемот на заштитата на личните податоци. Додека зајакнувањето на правата на субјектот на податоците беше една од главните теми на оваа реформа, ако се направи подетална анализа може да се констатира дека одредбите можат да нè доведат до несигурност и честопати го ограничуваат обемот на правата. На пример, точен е фактот дека  правото на субјектот на податоци да биде информиран,

според новиот закон содржи поцелосен и поконзистентен сет на детали кои треба да ги достави контролорот на податоците, меѓутоа согласно член 14 (5) (б), ова право не се применува кога контролорот не ги собира податоците директно од субјектот на податоци и обезбедувањето на конкретните информации се чини дека е невозможно или бара непропорционален напор. Слично на тоа, член 14 (5) (ц) го ограничува опсегот на правото на субјектот на податоците да биде информиран, исклучувајќи ја примената на ова право во ситуации на индиректно прибирање на личните податоци, која е утврдена со закон. Во овој случај законот не бара никакви дополнителни заштитни мерки.

Овие специфичности значително ги ограничуваат правата на субјектот на податоците, бидејќи во денешно време случаите во кои податоците не се обезбедуваат директно од субјектот на податоци, туку од други извори, се бројни. Спротивно на тоа, Директива 95/46/ЕЗ имаше специфична одредба која се однесуваше на податоците кои се собираат индиректно, од страна на трети лица. Додека Директивата исто така предвидуваше ограничувања (член 11 (2)), таму е јасно дека обработката на таквите податоци може да се направи само за статистички или истражувачки цели. Можеби најголемата разлика меѓу одредбите на Директивата 95/46/ЕЗ и Општата регулатива за заштита на лични податоци е моментот на објавувањето на податоците, односно моментот кога тие се прават достапни за субјектот на податоците. Додека член 11 (1) на Директивата предвидува дека информациите мора да бидат достапни „во моментот на собирањето на личните податоци“, новиот закон за заштита на лични податоци, односно GDPR (рецитал 61) вели дека информациите кои се собираат од индиректни извори треба да му се дадат на субјектот на податоците „во разумен период, во зависност од околностите на одредениот случај“.

## 1.1 Право на транспарентност

Ова право се предвидува со одредбите на член 12 на GDPR. Според правото на транспарентност, контролорот треба да презема соодветни мерки за да обезбеди концизна, транспарентна, разбирлива и лесно достапна форма за обработка на личните податоци. Според барањето на субјектот на податоци, контролорот треба да достави информации до

субјектот на податоци во рок од еден месец од приемот на барањето. Доколку е потребно, тој период може да биде продолжен за уште два месеци, земајќи ги во предвид сложеноста и бројот на барањата. Контролорот треба да го извести субјектот на податоците за секое такво продолжување во рок од еден месец од приемот на барањето, заедно со причините за одложувањето. Кога субјектот на податоци го поднесува барањето по електронски пат, информациите треба да се обезбедат преку електронски средства, доколку е можно, освен ако не е поинаку побарано од субјектот на податоците.

## 1.2 Правото да бидеш информиран

Ова право се регулира со член 13 на GDPR и значи дека секој субјект на податоци има право да знае кои податоци контролорите ги собираат за нив. Ова право има за цел да им обезбеди на физичките лица детални информации за обработката на нивните податоци. Меѓу другото, субјектот на податоци има право да го знае идентитетот и деталите за контакт на контролорот, деталите за контакт на офицерот за заштита на лични податоци, целите за обработка за кои се наменети личните податоци, правната основа за обработка, временскиот период за кој ќе се чуваат личните податоци, или ако тоа не е можно, критериумите што се користат за одредување на тој период, и др.

## 1.3 Право на пристап/увид

Ова право го гарантира правото на субјектот на податоците да дознае кои лични податоци се собираат и се чуваат за него (член 15 на GDPR). Тоа значи дека секоја личност има право да се обрати до било која организација која обработува лични податоци (контролори), на пример: продавница, училиште, банка, невладина организација, итн. и тие имаат обврска да одговорат на барањето на субјектот на податоците. Правото на пристап се состои од правото на субјектот на податоците да бара потврда од контролорот, со која, меѓу другото, се бара добивање на следниве информации: целите на обработка;

категориите на личните податоци што се обработуваат; категориите на примателите на кои им се откриени или ќе бидат откриени личните податоци, особено примателите во трети земји или меѓународни организации; кога личните податоци не се собираат од субјектот на податоците, сите достапни информации за нивниот извор; во случај на пренос на личните податоци во трета земја или меѓународна организација, субјектот на податоци има право да биде информиран за соодветните заштитни мерки во врска со преносот; и др. Значи со правото на пристап до податоци, субјектите на податоците имаат еден вид на контрола врз точноста на нивните лични податоци.

## 1.4 Право на исправка и бришење

Доколку личните податоци се неточни, нецелосни, застарени и сл., субјектот на податоци има право да бара од контролорот исправка на податоците што се однесуваат на него или неа (член 16 на GDPR). Субјектот на податоците исто така има право да бара од контролорот бришење на личните податоци без непотребно одложување, кога се применува еден од следниве услови предвидени со член 17 на GDPR:

(а) Личните податоци веќе не се потребни во однос на целите за кои се собрани или на друг начин обработени;

(б) Субјектот на личните податоци ја повлекува својата согласност за обработка на лични податоци и каде што не постои друга правна основа за обработка;

(в) Субјектот на податоци приговара на обработката и нема преовладувачки легитимни основи за обработка;

(г) Личните податоци се незаконски обработени;

(д) Личните податоци треба да бидат избришани за почитување на законската рамка на една земја членка на Европската Унија на која подлежи контролорот;

(е) Личните податоци се собрани во врска со понуда на услуги на информатичко општество директно на дете.

Правото на бришење, според член 17 на GDPR се однесува на правото да бидеш заборавен, за кое пошироко ќе се зборува во понатамошниот текст.

## 1.5 Право на ограничување на обработка, односно прекин на процесирање

Субјектот на податоци има право да бара од контролорот ограничување на обработката кога се применува еден од следниве услови предвидени со закон (член 18 на GDPR):

а) Точноста на личните податоци ја оспорува субјектот на податоците во одреден период што му овозможува на контролорот да ја потврди точноста на личните податоци;

б) Обработката е незаконска, а субјектот на податоците се спротивставува на бришење на личните податоци и наместо тоа бара ограничување на нивната употреба;

в) Контролорот повеќе нема потреба од личните податоци за целите на обработката, но се бара од субјектот на податоците за утврдување, извршување или одбрана на правни барања;

г) Субјектот на податоците приговара во текот на проверката, дали легитимните основи на контролорот ги надминуваат оние на субјектот на податоците.

## 1.6 Право на приговор

Субјектот на податоци има право да се спротивстави на обработката на своите лични податоци врз основа на неговата или нејзината особена ситуација, ако обработката се заснова на две специфични законски основи:

(1) Обработката е неопходна за извршување на задача која е извршена од јавен интерес или во вршење на службено овластување доделено на контролорот;[200]

(2) Обработката е неопходна за целите на легитимните интереси што ги следи контролорот или трето лице, освен кога таквите интереси се преовладани од интересите или основните права и слободи на субјектот на податоците за кои е

[200] Тошкова, *supra* note 15, at p. 54.

потребна заштита на личните податоци, особено кога субјектот на податоците е дете.[201]

Правото на приговор исто така се однесува на профилирање врз основа на двете горенаведени законски основи за обработка на податоци.

Во случај на остварување на правото на приговор контролорот нема повеќе да ги обработува личните податоци, освен ако контролорот докаже легитимна основа за обработката на податоците, која ги надминува интересите, правата и слободите на субјектот на податоците или за утврдување, извршување или одбрана на правни барања.[202]

Кога личните податоци се обработени за цели на директен маркетинг, субјектот на податоци има право да приговара во секое време на обработката на лични податоци кои се однесуваат на него или неа за таков маркетинг, што вклучува профилирање до степен до кој е поврзан со таков директен маркетинг. Доколку субјектот на податоците се спротивстави на обработката за потребите на директен маркетинг, контролорот ќе престане да обработува лични податоци за такви цели.[203]

## 1.7 Право да не се биде предмет на автоматизирано индивидуално донесување одлуки, вклучувајќи и профилирање

Согласно член 22 на GDPR, субјектот на податоци има право да не биде предмет на одлука заснована исклучиво на автоматска обработка, вклучувајќи профилирање, што произведува правни последици кои се однесуваат на него или неа или слично значително влијае врз него или неа.

Ова право не се применува ако:

а) Одлуката е неопходна за склучување или извршување на договор помеѓу субјектот на податоците и контролорот на податоците (член 22, точка а);

[201] *Ibid.*
[202] Член 21(1) на Општата регулатива за заштита на личните податоци L 119/1 од 04.05.2016 год.
[203] Член 21, точка 2 и 3 на Општата регулатива за заштита на личните податоци L 119/1 од 04.05.2016 год.

б) Овластено е со закон на кој контролор е предмет и кој, исто така, поставува соодветни мерки за заштита на правата и слободите и легитимните интереси на субјектот на податоците (член 22, точка б); или

в) Се основа на изречна согласност на субјектот на податоците (член 22, точка ц).

Во случаите наведени во точките (а) и (в) погоре, контролорот на податоците треба да спроведе соодветни мерки за заштита на правата и слободите на субјектот на податоците и нивните легитимни цели, барем правото да се добие човечка интервенција од страна на контролорот, правото да ја искаже својата гледна точка и правото да ја оспори одлуката (член 22, параграф 3 на GDPR).

Автоматизираните индивидуални одлуки за донесување одлуки не смеат да се базираат на посебни категории на лични податоци, освен ако субјектот на податоци не дал изречна согласност за обработување на неговите/нејзините лични податоци, или обработката е неопходна заради значителен јавен интерес. Контролорот треба да воспостави соодветни мерки за заштита на правата и слободите и легитимните цели на субјектот на податоците (член 22, параграф 4).

# ГЛАВА ВТОРА : ПРАВО ДА БИДЕШ ЗАБОРАВЕН

## 1. Вовед

Развојот на телекомуникациските технологии и Интернетот доведоа до акумулација на огромна количина на информации во онлајн светот. Тоа им дозволува на луѓето лесно и ефикасно да најдат информации и одговори за секое прашање, што значи дека сите информации се достапни за јавноста. Во секоја електронска комуникација, за секое физичко лице се чуваат голем број на податоци. Некои податоци може да се сметаат за неважни, како што е на пример сликата од средно училиште, додека другите можат да бидат од голема важност, како што е на пример едно видео кое содржи информации за сексуалниот живот на една личност. Највознемирувачки е фактот што некои информации се внесуваат од самите субјекти на податоци, меѓутоа многу често тие се објавуваат од страна на трети лица. Штом се објавени на Интернет, податоците веднаш се дистрибуираат, можат да се обработуваат и да се објават повторно, без одобрение на субјектот на податоците. Со оглед на тоа, многу луѓе станаа жртви на јавно искористување и злоупотреба.

Брзиот развој на технологијата и големиот број на електронски комуникации во текот на 1990-тите години донесе многу закани за приватниот живот на поединците и како последица на тоа дојде до израз еден нов вид на право: правото на заштита на личните податоци.[204] Европската Комисија го предложи правото да бидеш заборавен како дел од ревизијата на одредбите на Директивата за заштита на личните податоци (Директива 95/46/ЕЗ). Предлогот доби широк јавен интерес и беше дебатиран од страна на медиумите и законодавците.

Дискусијата за правото да бидеш заборавен беше предизвикана од еден судски случај донесен пред Судот на правдата на Европската Унија. Тоа беше случајот со број C-131/12, за кој пошироко ќе се дискутира подоцна. Меѓутоа, дури и пред овој случај, Европската Унија имаше правни мерки кои се однесуваа на правата на поединците да

[204] W. J. Schünemann and M.-O. Baumann, *Privacy, Data Protection and Cybersecurity in Europe* (2017), at p.20.

побараат од контролорите[205] да ги бришат, односно да ги отстранат сите нецелосни или неточни информации што ги поседуваат, согласно член 12 на Директивата 95/46/ЕЗ, под наслов „Право на пристап“, дел (б). Сепак, одлуката на Европскиот суд за правда беше многу значајна, бидејќи според таа одлука се изготви едно ново право, таканаречено „право да бидеш заборавен“.

Правото да бидеш заборавен се однесува на прашањето за овозможување на корисниците на Интернет да бараат бришење на нивните лични податоци како што се: слики, текстови, мислења, официјални документи и сите други активности испратени на веб-страници, социјални мрежи, итн.[206] Ова право се темели врз идејата дека корисникот на Интернет има право да влијае врз обработката на своите податоци и кога смета дека тоа е потребно, исто така има право да бара отстранување на личните податоци изработени од трети лица. Значи правото на заборавање и бришење на податоците произлегува од основните принципи на почитување на приватноста и идентитетот на поединците.

Во понатамошниот текст анализата ќе биде фокусирана на правото да се биде заборавен како законско право (а не, на пример, како апстрактна вредност), бидејќи за судската пракса е многу важно прашањето каков правен статус произлегува од тоа право.

## 2. Дефиниција

Таканаречената „право да бидеш заборавен“ е многу сложен правен инструмент. Во правната литература постојат бројни дефиниции за правото да бидеш заборавен, кои произлегуваат од принципите за заштита на приватниот живот и личните податоци на поединците во онлајн комуникацијата. Во некои случаи се користи терминот „право на

[205] Природни или правни лица, јавна власт, агенции, итн. кои ги утврдуваат целите и средствата на обработката на личните податоци (член 2(д)) на Директива 95/46 ЕЗ.

[206] Andrade, 'Oblivion: The Right to Be Different from Oneself. Reproposing the Right to Be Forgotten', *Revista de Internet Derecho y Política* (2012) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033155 , at p.124.

бришење“ или „право на заборавање“ кои произлегуваат од француската терминологија “*le droit a l’oubli*” или италијанската терминологија “*ildirittoal’oblio*”.[207]

Општо, правото да бидеш заборавен им дава можност на корисниците на Интернетот да бараат бришење или отстранување на нивните јавни податоци кои веќе не се релевантни или не се чуваат за легитимни цели. Правото се базира врз идејата дека на луѓето и организациите треба да им се дозволи да ги контролираат информациите за нив и да одлучуваат за себе кога, како, и во која мера треба и може да се пренесат тие информации кон другите лица.[208] Во поширок контекст, целта е да се ребалансира моќта помеѓу субјектите на податоците и оние кои ги прибираат и обработуваат личните податоци. Во оваа смисла, субјектот на податоците станува носител на правото над своите лични податоци.[209]

Во својата статија, Јасмине го опишува правото да бидеш забравен како: „Правото да бидеш заборавен е нов инструмент поврзан со приватноста на тужителите, за да можат да ги отстранат нивните информации задржани од страна на организациите и од достапноста на Интернет“.[210]

Според Комитетот на Европската Унија, правото да бидеш заборавен му овозможува на субјектот на податоците да добие бришење на линкови поврзани со своите податоци, кои субјектот на податоците ги смета штетни за себе.[211] Ова право генерално има два заеднички елементи: употребата на казни против правни лица кои помагаат во дистрибуција на забранети материјали, како и создавање на приватен надоместок за оштетените лица.[212]

Во академската литература, се разликуваат три перспективи на правото да се биде заборавен, како што се:

---

[207] Tamò and George, 'Oblivion, Erasure and Forgetting in the Digital Age', 5 *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2014) , available at http://www.jipitec.eu/issues/jipitec-5-2-2014/3997 , at p.72.

[208] Lagone, 'The Right to Be Forgotten: A Comparative Analysis', *SSRN Electronic Journal* (2012) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229361 , at p.5.

[209] Tamò and George, *supra* note 207, at p.72.

[210] McNealy, 'The Emerging Conflict between Newsworthiness and the Right to Be Forgotten', 39 *Northern Kentucky Law Review* (2012) , at p.134.

[211] European Union Committee, *EU Data Protection Law: A ‘Right to Be Forgotten’?* (2014), available at https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf.

[212] Bolton, 'The Right to Be Forgotten: Forced Amnesia in a Technological Age', *John Marshall Journal of Computer and Information Law* (2015) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2513652 , at p.134.

(1) Доминантната перспектива, нагласувајќи дека личните податоци треба да бидат избришани после одреден период;
(2) Социјалната перспектива, според која застарените и негативните информации не треба да се користат против луѓето; и
(3) Индивидуалната перспектива, која нагласува дека луѓето треба да се чувствуваат сигурни и да немаат страв од последиците од минатото.[213]

## 3. Потеклото на правото да бидеш заборавен

Во правото на Европската Унија, правото да бидеш заборавен, иако официјално не беше дефинирано и кодифицирано како такво, беше принцип вклучен во Директивата 95/46/ЕЗ од 1995 година, кое укажува дека во име на заштита на приватноста, поединците имаат право да управуваат со обработката на нивните лични податоци. Врз основа на член 6(1) на Директивата, државите членки треба да обезбедат дека личните податоци:

„ќе се чуваат во форма која овозможува идентификација на субјектите на податоците не подолго отколку што е потребно за целите за кои податоците се собрани и за кои се обработуваат“.

Понатаму, со член 12(б) му се гарантира на секој субјект на податоци правото да бара од контролорот на податоците:

„соодветна исправка, бришење или блокирање на обработувањето на податоците, кои не се во согласност со одредбите на оваа Директива, особено поради нецелосни или неточни податоци“.

[213] Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the ‘Right to Be Forgotten’ in Big Data Practice', *Tilburg Law School Legal Studies Research Paper Series No. 08/2012* (2011) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986719 , at p.6.

Брзиот развој на технологијата и дигиталните комуникации доведе до многу закани за приватниот живот, претставувајќи ризик за личната слобода на поединците. Кога Директивата 95/46/ЕЗ се преговараше, онлајн комуникациите не беа толку присутни како што беа во наредните години. Google е основан во 1998 година, три години по усвојувањето на Директивата. Во наредните години, технологијата за прибирање, обработување и достапност до секакви информации беше целосно променета и Директивата повеќе не претставуваше солиден правен инструмент за решавање на новите потреби.[214] На пример, Google знае повеќе за нас отколку ние сами се сеќаваме за себе. Facebook собира огромни количини на податоци за нашите преференци, и тоа не само за своите корисници, но исто така и за луѓето кои немаат профил на Facebook, но посетуваат сајтови кои го содржат логото на Facebook каде што се прикажува "*Like this*", дури и без кликнување на тоа од нивна страна.[215] Корисниците на Интернетот станаа свесни за потенцијалната штета која информациите зачувани вечно на Интернет можат да ја предизвикаат. Многу лица се соочуваат со зголемен страв дека нивното дигитално минато ќе им нанесе проблеми во иднината.

Како реакција на новите закани и проблеми, во 2012 година Европската комисија објави „Предлог за Регулатива за заштита на поединците во однос на обработката на личните податоци и слободното движење на таквите податоци"[216] или познато како Општа регулатива за заштита на личните податоци (за кое пошироко е објаснето во првиот дел на овој труд), од каде произлегува правото да бидеш заборавен,[217] кое е дефинирано како право на една личност да бара бришење на своите податоци од Интернет, кога се исполнуваат одредени услови. Предлогот доби широк јавен интерес и беше многу дебатиран во медиумите, судовите и од страна на законодавците. Главниот пример во судската пракса и правната наука се поврзува со лицата кои биле осудени и кои сакаа овој вид на информации да го отстранат од Интернет после одреден временски период.[218]

---

[214] European Union Committee, *supra* note 211, at p.5.
[215] Koops, *supra* note 213, at p.7.
[216] Види: *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to Processing of Personal Data on the Free Movement on Such Data (General Data Protection Regulation) COM/2012/011 Final - 2012/0011 (COD)*, 2012, available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012PC0011 (last visited 10 January 2019].
[217] *supra* note 4, at article 17.
[218] Weber, 'The Right to Be Forgotten: More than a Pandora's Box?', 2 *JIPITEC* (2011) , at p.120.

Правото да бидеш заборавен им овозможува на корисниците на Интернетот да ги корегираат податоците што се стават на Интернет, барајќи од контролорот за обработка на личните податоци дополнителни (разумни) чекори за да обезбедат бришење на информациите, вклучувајќи ја и обврската на контролорите да ги информираат третите лица за барањето на субјектот на податоците да ги отстранат сите линкови кои навлегуваат во приватноста на корисниците на Интернетот.[219] Во овој поглед, се чини дека концептот на правото да бидеш заборавен не е сосема јасен, бидејќи тешко е да се определува какви разумни обврски треба да преземат контролорите и според кои услови треба да се почитуваат таквите обврски. И покрај тоа што како идеја е привлечна, правната форма и практичните импликации на правото да бидеш заборавен досега не се доволно анализирани.

Правото да бидеш заборавен се применува кога се исполнуваат следниве услови: податоците треба да бидат несоодветни, ирелевантни или во спротивност со целите за кои се обработуваат.[220] Многу корисници на Интернет се повикуваат на правото да бидеш заборавен кога сметаат дека поради одредени причини нивните податоци треба да се отстранат од резултатите на пребарување (види табела 1, 2 и 3).

**Табела 1: Барања за отстранување на лични податоци од Google во ЕУ/ЕФТА.**

| Држава | Вкупен број на барања | Процесирани барања | Процент на избришани |
|---|---|---|---|
| **Франција** | 191,417 | 686,309 | 49,4% |
| **Германија** | 141,170 | 556,840 | 49,4% |
| **Обединето Кралство** | 103,735 | 461,012 | 43,6% |
| **Шпанија** | 81,682 | 270,422 | 37,9% |
| **Италија** | 71,638 | 299,328 | 37,4% |
| **ЕУ\ЕФТА*** | 860,168 | 3,405,112 | 45% |

*ЕУ= Европска Унија; ЕФТА= Европската асоцијација за слободна трговија

Извор: https://transparencyreport.google.com/eu-privacy/overview (посетено на 5 декември 2019 година)

[219] *supra* note 4, at article 17.

[220] *Case C-131/12 Google Spain SL and Google Inc. v. Agencia Espanola de Protección de Datos (AEPD), Mario Costeja González*, 2014, available at http://curia.europa.eu/juris/liste.jsf?num=C-131/12.

**Табела 2. Барања за бришење на URL адреси според видот на веб-страницата.**

| Тип на страница | Криминал | Името не е пронајдено | Недоволна информација | Разно | Политички | Лични информации | Професионални информации | Професионални престапи | Авторство | Чувствителни лични податоци |
|---|---|---|---|---|---|---|---|---|---|---|
| **Дирекција** | 1% | 17% | 19% | 13% | 0% | 19% | 27% | 1% | 2% | 1% |
| **Влада** | 6% | 7% | 17% | 16% | 4% | 3% | 41% | 4% | 1% | 1% |
| **Вести** | 17% | 9% | 19% | 9% | 6% | 3% | 15% | 17% | 4% | 2% |
| **Социјални мрежи** | 2% | 22% | 24% | 13% | 1% | 3% | 6% | 2% | 26% | 1% |
| **Разно** | 5% | 17% | 31% | 13% | 2% | 4% | 17% | 5% | 5% | 3% |

Извор: https://transparencyreport.google.com/eu-privacy/overview (посетено на 5 декември 2019 година)

**Табела 3. Видови на барања по категори.**

| Држава | Индивидуални барања | Малолетници | Влада\ Политичар | Корпорација | Невладина јавна личност | Друго |
|---|---|---|---|---|---|---|
| **Франција** | 101,715 (89.3%) | 6,22 | 2,131 | 1,853 | \ | 0,865 |
| **Германија** | 69,166 (89.0%) | 3,527 | 2,514 | 1,608 | \ | 940 |
| **Обединето Кралство** | 51,167 (90.1%) | 2,366 | 1\ | 945 | 1,367 | 954 |
| **Шпанија** | 40,986 (89.8%) | 971 | 1,809 | 1,101 | \ | 765 |
| **Италија** | 38,227 (86.3%) | \ | 2,091 | 1,333 | 1,250 | 1,420 |
| **ЕУ\ЕФТА*** | 435,051 (88.4%) | 23,844 | 12,605 | 10,777 | | 9,694 |

*ЕУ= Европска Унија; ЕФТА= Европската асоцијација за слободна трговија

Извор: https://transparencyreport.google.com/eu-privacy/overview (посетено на 5 декември 2019 година)

## 4. Видови на податоци за кои може да се достави барање за отстранување

Главно прашање е: За кои податоци може да се бара бришење, односно отстранување од резултатите на пребарување? Меѓу многуте видови на класификација на информациите, важно е тие да се класифицираат врз основа на тоа кој ги објавил податоците, бидејќи со барањата за отстранување може да се постапува различно во зависност од овие информации. Оттука, информациите можат да се класифицираат во три вида: информации објавени од барателот; информации прво објавени од барателот, а потоа повторно објавени од некој друг; и информации објавени од некој друг.[221]

Првиот тип на информации е најмалку контроверзен, бидејќи секој кој објавува информации на една веб-страница, треба да има право истите да ги отстрани подоцна.

Вториот тип на информации се однесуваа на информациите објавени од субјектот на податоците, а потоа пак објавени од некој друг. Овој тип може да содржи некои контроверзии. Така на пример, претпоставуваме дека една личност А прави еден клип и го остава на училиште. Иако лицето А не го објавува клипот на ниедна веб-страница и не го покажува на никого, другарите го наоѓаат клипот и го објавуваат на Интернет. Во овој случај, се поставува прашањето: До кого треба да го поднесе своето барање лицето А - Facebook, YouTube, Google, Yahoo? Можеби за веб-страници како што се Facebook и YouTube би било полесно да го исполнат барањето за отстранување, така што со едно пребарување на нивниот сервер ќе ги пронајдат сите копии на податоци кои треба да се избришат. Меѓутоа, за машините за пребарување како што се Google и Yahoo, ситуацијата може да биде многу комлицирана, бидејќи тие само произведуваат список на резултати од пребарувањето, кои произлегуваат од клучни зборови и поголемиот дел од резултатите се всушност зачувани во серверите на други веб-страници. Според ова, најдобриот можен одговор би бил блокирањето на бараната содржина. Меѓутоа, тоа не значи дека блокираната содржина ќе биде отстранета од серверот. За да се избегне таквиот проблем,

[221] R. J. R. Levesque, *Adolescents, Rapid Social Change, and the Law: The Transforming Nature of Protection* (2016), at p.48.

друг можен одговор би бил известувањето на конкретните веб-страници дека имало барање за отстранување на одредената содржина на податоци или информации.[222]

Конечно, третиот вид на информации се оние кои се објавуваат од трети лица. Дури и за овој вид на информации, субјектот на податоците има право да бара отстранување. Меѓутоа овој тип на информации се соочува со големи контроверзии, затоа што субјектот на податоците бара од контролорите да избришат информации кои биле објавени од страна на трето лице. Во таа смисла, не е лесно да се докаже кој ја поседува сопственоста на конкретните информации. Како резултат на тоа, може да дојде до ситуации кога чесни производители го имаат товарот на докажување дека информациите се чуваат за историски, статистички или научни цели.[223]

## 5. Случајот Google-Шпанија

Судското признавање на правото да бидеш заборавен се случи во 2014 година со случајот *Google-Шпанија*.[224] Г-дин Гонзалез, шпански државјанин, во 2010 година ја тужел филијалата на Google во неговата држава, основно во Националната агенција за заштита на податоци. Тој побарал да се отстранат неговите лични податоци од резултатите за пребарување на Google. Неговата жалба се засноваше на фактот дека ако некоја личност го напише неговото име на Google, најпрво се појавуваат информации кои се однесуваа на некои долгови поврзани со неговиот недвижен имот, кои г-дин Гонзалез веќе ги имаше наплатено, и истите беа стари повеќе од десет години. Тој побарал да се отстранат неговите лични информации од резултатите на пребарување на Google, врз основа на тоа што тие податоци се ирелевантни, бидејќи долгот бил наплатен во целост веќе неколку години.[225]

Шпанскиот суд го доставил предметот до Европскиот суд на правдата, сакајќи да разјасни дали Европската директива за заштита на податоци се применува за Google,

[222] *Ibid.*, at p.49.
[223] *Ibid.*
[224] *supra* note 220.
[225] *Judgment of the Court on Case C-131/12, of 13 May 2014*, available at: http://curia.europa.eu/juris/liste.jsf?num=C-131/12.

бидејќи серверот за обработка на податоци се наоѓал во Северна Америка, и дали едно лице има право да бара отстранување на податоци. Европскиот суд во својата пресуда навел објаснување дека штом Google има филијала во континентот каде се применуваат Европските закони, треба да се почитува таканаречното „право да бидеш заборавен“, кое доаѓа во предвид кога податоците се неточни, небитни, непотребни или несоодветни.[226]

Се смета дека случајот Google-Шпанија се однесува на деиндексирање, а не на бришење на одредени податоци. Во овој контекст, правото да бидеш заборавен не треба да се меша со една дигитална алатка која овозможува промена на историјата, дозволувајќи на поединците да ги бришат нивните несакани траги.[227]

## 6. Влијание и критики

Иако правото да бидеш заборавен е претставено само за Европа, истото ќе има влијание врз организациите надвор од Европа. Ако правото се применува во својата сегашна форма, тоа значи дека правото на Европската Унија станува *de facto* стандард низ целиот свет за сите онлајн комуникации. Како еден голем пазар, во суштина Европската Унија ќе има можност да ги диктира меѓународните правила за сите оние компании кои својата дејност ја вршат во онлајн комуникацијата.[228]

Европската агенција за безбедност на мрежи и информации (ENISA) има објавено коментари за ова право. Во суштина, агенцијата се согласува дека правото е соодветно и разумно во теоретска смисла, но не е јасно како ова право ќе се имплементира и ќе се спроведува од техничка перспектива, особено поради тоа што неовластеното копирање на информациите на Интернет е невозможно да се спречи.[229] Како што Svantesson истакнува,

[226] *Judgment of Court of Justice of European Union of 13 May 2014 in Case C-131/12, Google Spain SL and Google Inc. v. Agencia Espanola de Protección de Datos (AEPD), Mario Costeja González*, available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf.

[227] Gstrein, 'The Right to Be Forgotten in the General Data Protection Regulation and the Aftermath of the "Google Spain" Judgment (C-131/12)', *PinG Privacy in Germany: Datenschutz Und Compliance* (2017) , available at https://www.pingdigital.de/ce/the-right-to-be-forgotten-in-the-general-data-protection-regulation-and-the-aftermath-of-the-google-spain-judgment-c-131-12/detail.html , at pp.9-18.

[228] Koops, *supra* note 213, at p.11.

[229] 'Problems with the EU's Proposed 'Right to Be Forgotten'', *Info Security* (2012) , available at https://www.infosecurity-magazine.com/news/problems-with-the-eus-proposed-right-to-be/.

многу е полесно да се дистрибуираат податоците отколку да се отстранат од Интернет.[230] Во неговата книга тој зборува за "Street View" системот на Google, кој им овозможува на корисниците на Интернетот да гледаат панорамски слики на улиците. На овие фотографии се фатени различни луѓе кои беа присутни на улиците за време на фотографирањето. Една слика која привлече големо внимание покажува една жена која влегува или излегува од една кола, така што горниот дел на нејзиното тело е видлив на фотографијата. Кога Google дозна за ова фотографија ја отстрани од Интернет, меѓутоа таа фотографија веќе беше копирана од многу луѓе и може да се најде онлајн и денес.

Во пракса постојат многу проблеми, бидејќи податоците можат да се копираат и да се дистрибуираат многу брзо, а социјалните мрежи би имале многу потешкотии да ги идентификуваат и да ги контролираат третите лица. Европската агенција за безбедност на мрежи и информации исто така е загрижена во врска со широката дефиниција на личните податоци и за прашањето кој точно може да бара бришење на податоците. На пример, на една фотографија каде што се две лица, едно лице може да побара сликата да се „заборави", додека другото лице би сакало сликата да се задржи.[231] Чии желби треба да се почитуваат? Што ако повеќе лица се појавуваат на една фотографија? Кој ќе одлучи дали треба и кога треба фотографијата да се „заборави"? Значи не е јасно според кои критериуми ќе се применува ова право и кои услови треба да бидат исполнети за одлучување во одредена ситуација.

## 7. Правото да бидеш заборавен и неговата закана за другите основни права

Правото за бришење на податоци најмногу се повикува во случаи кога на јавноста и се изложува несакано минато на едно лице, кои ги повредува фундаменталните права на тоа лице до тој степен што не може да се оправда со било кој легитимен јавен интерес. Во

[230] D. J. Svantesson, *Extraterritoriality in Data Privacy Law* (2013).
[231] Lagone, *supra* note 208, at p.13.

оваа смисла, дебатите околу ова право се слични со случаите во кои правата на приватност на јавните личности се во судир со слободата на изразување.[232]

Правото да бидеш заборавен се критикува од повеќе аспекти. Иако ова право беше дизајнирано за заштита на личните податоци од незаконско искористување, истото се појави како пречка за применување на две групи на основни права, како што се: самоопределувањето на поединците и слободниот проток на податоците[233] од една страна, и приватноста и слободата за изразување[234] од друга страна. На пример, ако некоја личност објавува нешто за нас, дали имаме право да бараме таквите информации да се отстранат од Интернет? Кое право би преовладувало: правото на бришење, односно правото да бидеш заборавен или правото на приватност и заштита на лични податоци? Ова прашање, се разбира, предизвикува сериозна загриженост за слободата на изразување. Истите можат да се спротивстават и да ја нарушат должноста за заштита на историските факти и јавниот интерес.

Bolton тврди дека правото да бидеш заборавен ги има своите придобивки за општеството, меѓутоа тој истакнува дека во едно време кога весниците и медиумите често вклучуваат статуси, "tweets" и други јавни коментари напишани од граѓаните, правото на бришење може сериозно да ги ограничи новинарите да ја извршуваат својата работа ефикасно.[235] Во овој контекст, јавниот и општествениот интерес за пристап до информации (право за информирање) и слободата на говор и изразување (право на медиумите да ја информираат јавноста, која исто така го опфаќа правото на поединците да бидат информирани) треба да триумфираат, и според ова, правото на бришење на податоци треба да биде избалансирано со други конкурентни права и вредности. Така на пример, лицата кои се сведоци на кривичните дела, не треба да имаат можност да се повикуваат на одредбите на правото да бидеш заборавен. Во суштина овој аргумент вели дека правата на приватност се занимаваат само со лични податоци и информации, па затоа

[232] Graux, Ausloos and Valcke, 'The Right to Be Forgotten in the Internet Era', *ICRI Research Paper No.11* (2012) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2174896 , at p.4-5.
[233] Lindroos-Hovinheimo, 'Legal Subjectivity and the 'Right to Be Forgotten': A Rancie`rean Analysis of Google', 27 *Law Critique* (2016) , available at http://rdcu.be/koh1 , at p.290.
[234] Kang et al., 'A Study for Security Scheme and the Right to Be Forgotten Based on Social Network Service for Smart-Phone Environment', *Communications in Computer and Information Science* (2011) , available at https://link.springer.com/chapter/10.1007/978-3-642-23141-4_33 , at p.329.
[235] Bolton, *supra* note 212, at p.141.

истите не можат да се однесуваат за информации од јавен карактер. Според ова, општеството треба да има пристап до информациите од јавен карактер.[236]

Меѓутоа, треба да се има во предвид дека слободата на изразување не е неограничена. Во ниедна држава не е дозволено да се шират лаги со кои се загрозува интегритетот на една личност, а особено не е дозволено да се шири омраза врз верска, етничка или друг вид основа.

Проблеми произлегуваат кога се работи за политичари, јавни личности и слично, чија транспарентност е многу важна за политичкиот кредибилитет и демократското општество.[237] Ова е тесно поврзано со правото на општеството да биде информирано од страна на медиумите. Меѓутоа, како што научниците забележуваат, новинарите треба да прават разлика помеѓу јавните личности "par exellence", односно јавни личности кои имаат политичка функција и јавните личности кои не вршат политичка дејност.[238] Доколку личните податоци на јавните личности кои не влегуваат во групата на "par exellence" не се од јавен интерес, односно не се релевантни за пренесување на одредена вест, тогаш тие не треба да бидат објавени. Во оваа смисла, љубопитноста на одредени лица да имаат информации за јавните личности не треба да се сфати како јавен интерес.[239]

Многу е дебатирана и примената на правото да бидеш заборавен во однос на бришење на криминалното минато. Противниците на правото да бидеш заборавен често истакнуваат дека ова право многу лесно може да се злоупотреби од страна на криминалците, кои имаат голем интерес да ги отстранат кривичните податоци од очите на јавноста, без разлика на тоа што истите би биле релевантни за општеството.

Правото на отстранување на јавните кривични досиеја се признава во законодавството на неколку земји[240], и тоа е оправдано со потребата на поединците да се рехабилитираат и да имаат можност да го живеат својот живот без да бидат гонети од минатото. На пример, во *НТ1 и НТ2 против Google*[241], Високиот суд на Англија и Велс го зема во предвид применувањето на правото да бидеш заборавен во случаи кои вклучуваат

[236] Andrade, *supra* note 206, at p.126.
[237] *Ibid.*, at p.133.
[238] Е. Стојановска and Ј. Ананиевска, *Приватност,информирање,и јавниот интерес: правото на приватност наспроти правото на јавноста да знае*, at p.14.
[239] *Ibid.*
[240] Weber, *supra* note 218, at p.121.
[241] *NT 1 & NT 2 v Google LLC [2018] EWHC 799 (QB)*, 2018, available at http://www.bailii.org/ew/cases/EWHC/QB/2018/799.html.

криминалци. Во овие два придружни случаи се работи за двајца бизнисмени (анонимизирани како НТ1 и НТ2), кои претходно биле судени за кривични дела. Тие побараа од судот да донесе наредба со која се упатува Google да ги отстрани нивните податотоци од резултатите на пребарување, врз основа на тоа што резултатите содржат неточни, застарени и небитни информации, и не се од никаков јавен интерес или на друг начин претставуваат нелегитимно мешање во нивното право да бидат заборавени.[242]

Општо, не постојат таксативни критериуми според кои се одлучува дали правото за бришење на одредени податоци преовладува над другите фундаментални човекови права, како што е слободата на изразување. Кога доаѓа до судир на овие права, правниот одговор се состои во балансирањето на конкурентните вредности и интереси[243] и често судовите одлучуваат врз проценувањето на околностите на одредениот случај. Така на пример, во случајот *Вон Хановер против Германија*[244] субјектот на податоците поднесува жалба до германскиот суд со кое бара да се забрани и да се спречи понатамошното објавување на одредени фотографии објавени во германски списанија (направени без нејзино знаење), кои се однесуваат на нејзиниот приватен живот. Субјектот на податоците тврди дека објавувањето на тие слики го нарушува нејзиното право за приватен живот и сопствен интегритет. Барањето се отфрла од страна на германскиот суд и се третира како незаконско и неосновано, и поради тоа жалителот се обраќа кон Европскиот суд за човекови права, кој пресуди дека имало повреда на член 8 (право на почитување на приватниот живот) на Европската конвенција за човекови права, утврдувајќи дека германските судови во конкретниот случај не постигнале рамнотежа меѓу засегнатите интереси. Европскиот суд за човекови права исто така забележува дека иако во одредени ситуации општата јавност би имала право на информирање, вклучувајќи, во посебни околности и право на информирање за приватниот живот на јавните личности, во конкретниот случај, таквото право не постои. Во овој случај, според Европскиот суд за

[242] За повеќе информации, види:A. Mendonca-Richards, *The Right to Be Forgotten, Rehabilitated, and to Know: Two Important Cases against Google*, 2018, available at https://www.farrer.co.uk/news-and-insights/the-right-to-be-forgotten-rehabilitated-and-to-know-two-important-cases-against-google/ (last visited 25 September 2019].

[243] de Terwangne, 'The Right to Be Forgotten and Informational Autonomy in the Digital Environment', in A. Ghezzi, Â. Guimarães Pereira and L. Vesnić-Alujević (eds.), *The Ethics of Memory in a Digital Age: Interrogating the Right to Be Forgotten* (2014) , at p.90.

[244] Види: *VON HANNOVER v. GERMANY (Application No. 59320/00)*, 2004, available at https://hudoc.echr.coe.int/eng#%7B%22itemid%22:[%22001-61853%22]%7D.

човекови права, интересот на субјектот на податоците за чување на приватниот живот преовладува над интересот на списанието да објавува фотографии.[245]

Меѓутоа, во некои случаи криминалните досиеја остануваат како јавен интерес. На пример, во случајот на Вилијам,[246] тој беше осуден за фотографирање на малолетници во непристојни околности. Како резултат на тоа, тој ја загуби неговата работа и му беше тешко да најде друга работа поради неговото криминално минато. Вилијам поднесе барање до Google за отстранување на податоците кои содржат информации за неговото судско минато, но Google одлучи дека таквото барање го оштетува јавниот интерес, бидејќи веруваше дека деталите за неговота пресуда остануваат многу важни за општеството.[247]

Интересно е да се забележи дека правото да бидеш заборавен не е заштитено со правната рамка на Република Северна Македонија, каде што се чини дека преовладува слободата на изразување. Во 2017 година, Генералниот секретар на агенцијата за заштита на податоци на Република Северна Македонија истакнува дека поединците треба да издржат одредени мешања (од страна на медиумите) во нивниот живот, кои не можат да се избегнат поради разумни причини. Во овој случај, „разумни причини“ се однесуваат на ситуации кога јавниот интерес, правото на информирање и слободата на говорот се повредни и преовладуваат над потенцијалните повреди на правата на приватност.[248]

Слободата на информирање и заштитата на приватноста може подобро да се разберат кога се гледаат низ една заедничка призма, бидејќи промоцијата на едно право доаѓа со оштетување на другото право. Во овој случај нема добра или погрешна позиција, освен тоа што демократијата сака да биде некаде на средина и одредената позиција треба да ги претставува вредностите и приоритетите на своите граѓани. Иако барањата и целите

[245] Chamber Judgment of European Court of Human Rights in the case of Von Hannover v. Germany (application no. 59320/00), of 24.6.2014, available at: http://hudoc.echr.coe.int/eng-press#{"itemid":["003-1036787-1072690"]}.
[246] Case of William-Do spent convictions relating to possession of indecent images get de-listed from internet search engines?, available at: http://www.unlock.org.uk/policy-issues/policy-cases/case-of-william-do-spent-convictions-relating-to-possession-of-indecent-images-get-delisted/.
[247] *Ibid.*
[248] I. Kuzevski, *Personal Data Protection Vis-à-Vis Freedom of Expression and Information*, 2017, available at https://cloudprivacycheck.eu/latest-news/article/personal-data-protection-vis-a-vis-freedom-of-expression-and-information/ (last visited 5 January 2019].

на приватниот сектор се различни од јавниот сектор, тие мора да најдат рамнотежа помеѓу пристапот на информации и правото на приватност.[249]

## 8. Други недостатоци

Научниците истакнуваат некои недостатоци на правото да бидеш заборавен, според кои применувањето на ова право честопати станува многу проблематично. Меѓу другите, може да се вбројат следниве проблеми:

- Ограничен обем - се чини дека правото да бидеш заборавен претпоставува договорен однос, бидејќи може да се применува само во ситуации во кои поединецот дава согласност за обработка на своите лични податоци. Ова значи дека концептот не е соодветен за прашања на приватноста, односно за ситуации каде што личните податоци се добиени и се чуваат врз основа на законот, без согласност на поединецот.[250]
- Анонимни податоци - многу луѓе одлучуваат да останат анонимни на Интернет, и во смисла на овие податоци правото да бидеш заборавен не нуди никакво решение.[251]
- Индиректна цензура - еден од најпознатите аргументи против правото да бидеш заборавен е дека тоа претставува скриена форма на цензурирање. Дозволувајќи им на луѓето да бараат бришење на своите лични податоци по своја волја и во секое време, може да доведе до ситуации во кои важни информации за општеството би станале недостапни и нецелосни.[252]
- Проблематична терминологија - формулирањето „право да бидеш заборавен“ може да доведе до нереални очекувања. Овој поим нагласува ограничување или обврска за другите, и поради тоа предизвикува негодување од страна на многу лица. Наместо да им се наметнува како должност на другите „да заборават“, некој посоодветен поим како на пример „право на бришење“ фокусиран на податоци, би бил пообичен за разбирање и попрактичен. Со други зборови, ова право не е, и не

[249] Stefanick, *supra* note 26, at p.23-24.
[250] Ausloos, 'The 'Right to Be Forgotten' - Worth Remembering?', 28 *Computer Law & Security Review* (2012) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1970392 , at p.7.
[251] *Ibid.*
[252] *Ibid.*

треба да се претставува како алатка за контрола на слободата на луѓето да примат или прошират различни информации. Одредбата едноставно има за цел да им овозможи на субјектите на податоците ефикасна контрола на своите податоци.[253]

## 9. Заклучок

Како заклучок, може да се констатира дека иако правото да бидеш заборавен *a priori* изгледа многу практично и привлечно, во судската пракса и во академската литература ова право се соочува со многу прашања кои уште немаат соодветен одговор. Пред потенцијална имплементација, треба да се направи внимателен баланс помеѓу правото на бришење на податоци и другите основни човекови права. За да се избегнат негативни и несакани ефекти и особено да се обезбеди ефикасна заштита на слободата на говор и изразување, правото треба да има добро дефиниран опсег на примена и треба да се наведат некои значајни исклучоци (на пример: кога податоците се важни за национална безбедност, ова право не треба да се земе во предвид).

Сметам дека државите треба да донесат специфични национални закони со кои ќе ги идентификуваат и прецизираат сите импликации на правото да бидеш заборавен, во форма на три генерални клучни прашања: Против кого може да се повикува ова право? Кога и зошто може да се применува ова право? Со какви правни инструменти може да се реализира ова право во правниот систем на една држава?

Меѓутоа, иако ова право се соочува со многу предизвици, со развивањето на технологијата и информатичкото општество, секој ден се зголемува неговата легална важност. Луѓето сакаат да имаат контрола врз своите податоци споделени со други лица во дигиталниот свет. Само времето ќе покаже дали ова право претставува соодветен и ефективен начин кој ќе придонесе поголема моќ над личните податоци.

[253] Graux, Ausloos and Valcke, *supra* note 232, at p.16.

# ГЛАВА ТРЕТА: ПРАВО НА ПРЕНОСЛИВОСТ НА ПОДАТОЦИ ВО КОНТЕКСТ НА ОПШТАТА РЕГУЛАТИВА ЗА ЗАШТИТА НА ЛИЧНИ ПОДАТОЦИ

## 1. Вовед

Глобалната дебата за преносливост на податоци започна поради потребата на корисниците на Интернет да ги преместуваат своите списоци на пријатели, книги на адреси на е-пошта, и други податоци кои корисниците ги собираат со часови поминати на Интернет. Така на пример, корисниците на Facebook и Google поминаа многу време во градењето и одржувањето на списоци со пријатели и кога сакаа да ги пренесат ваквите информации од една онлајн услуга на друга, честопати беше невозможно да ги извлечат своите податоци. Така, преносливоста на податоците се појави како начин кој ќе го направи возможно споделувањето на социјалните информации помеѓу веб-страниците.[254]

Европската Комисија изјави дека со зголемената употреба на одредени мрежни услуги, количината на лични податоци собрани во одредена услуга станува пречка за промена на услугите, без разлика дали овие услуги се подобри, поевтини или нудат повисоко ниво на заштитата на приватност. Како последица на тоа, може да дојде до губење на информации, размена на интерперсонални комуникации и други видови на лични или социјално релевантни податоци, кои не можат да се креираат или обноват на лесен начин.[255]

Развојот на правото на преносливост беше многу брз. Застапниците на правото на преносливост на податоци тврдеа дека таквиот отворен пристап не само што ќе го олесни животот на корисниците кои сакаат да мигрираат помеѓу различни веб-сајтови, но исто

[254] K. Allison, *Social Networks May Find It Does Not Pay to Be Too Possessive*, 2008, available at https://www.ft.com/content/8b6351e4-c843-11dc-94a6-0000779fd2ac (last visited 1 January 2019].
[255] *European Commission Working Paper SEC(2012) 72 Final*, 2012, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN (last visited 15 October 2019].

така тоа би можело да ја смени самата економија на веб-страниците, бидејќи компаниите ќе изградат нови услуги за да го користат слободниот проток на социјални информации.[256]

Поради горенаведеното, беше разбирливо зошто Европската Комисија во реформата на законската рамка за заштита на податоци одлучи да вклучи одредби за преносливост на податоци. Директивата 95/46/ЕЗ за заштита на лицата во однос на обработка на лични податоци[257] беше донесена во 1995 година кога Интернетот не беше дел од секојдневниот живот. Како што европскиот комесар за правда Viviane Reding наведе на една конференција во 2012 година „пред 17 години помалку од 1% од Европејците го користеле Интернетот. Денеска големи количини на податоци се пренесуваат и се разменуваат низ континенти и низ целиот свет во делови од секундата".[258]

Овој дел има за цел да ги открие карактеристиките на преносливост на податоци како правен концепт во современиот свет на приватност и заштита на лични податоци. Ќе се дискутира за влијанието на преносливоста на податоците врз конкуренцијата и меѓународниот трансфер на податоци.

## 2. Преносливост: нов концепт во правната рамка на Европската Унија

Преносливоста на податоците и содржината на ова право се појави како автономен нов концепт во Европската рамка за заштита на лични податоци. На 25 јануари 2012 година, Европската Комисија предложи реформа на правилата за заштита на личните податоци во Европската Унија, и беше изработена Општата регулатива за заштита на лични податоци (GDPR),[259] со цел да се зајакне заштитата на личните податоци на Интернет и да се зајакне дигиталната економија на Европа. Законот стапи на сила во мај

[256] Allison, *supra* note 254.
[257] *supra* note 95.
[258] Прес-конференција организирана после јавното започнување на реформата за заштита на податоци во 2012 година. За повеќе информации, види: European Commission - Press release, *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses*, 2012, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46 (last visited 1 November 2019].
[259] *supra* note 4.

2018 година и правото на преносливост на податоци беше ново право, кое се воведува во новиот закон.

Правото на преносливост на податоци, според GDPR, бара од деловните субјекти (контролори на податоци) да обезбедат дека можат да ги предадат, односно да ги пренесат личните податоци обезбедени од самиот субјект на податоци.[260] Во преамбулата на GDPR се укажува дека правото на преносливост на податоци не се ограничува само за социјални мрежи и медиуми, но исто така се применува и за преместување во облак (Cloud computing), веб-услуги, паметни телефони и други системи за автоматска обработка на податоци. Правото на преносливост на податоци се однесува на широк спектар на области како што се: социјални медиуми, машини за пребарување, е-пошта, онлајн продавници, и др.[261]

Правото на преносливост на податоци е содржано во член 20 на GDPR и може да се смета како проширување на правото на пристап[262] на субјектот на податоците, кое се регулира со одредбите на член 15 на GDPR.

## 3. Дефиниција и елементи на правото на преносливост на податоци

Врз основа на некои извори што дискутираат за преносливоста на податоците, може да се претпостави дека правото на преносливост е концепт со јасно значење. На пример, член 29 Работната група[263] објаснува дека во контекст на GDPR, преносливоста е едноставно право за примање на лични податоци и пренесување на истите од еден давател на услуги на друг. Преносливоста на податоците ги прави податоците мобилни-да можат да се однесат таму каде што е најкорисно и им дава поголема контрола на субјектите на податоци врз своите лични информации. Преносливоста на податоците им овозможува на

[260] Во овој труд се користат поими како „поединец“ , „потрошувач“, „корисник“ и „субјект на податоци“, кои наизменично се однесуваат на субјектот на податоците.
[261] Diker Vanberg and Ünver, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?', *European Journal of Law and Technology* (2017) , at p.2.
[262] Право на пристап значи дека субјектите на податоците имаат право да добијат податоци за тоа дали нивните лични податоци се обработуваат, каде и за која цел. За повеќе информцаии види: член 20 на Општата регулатива за заштита на лични податоци , *supra* note 4.
[263] *Article 29 Data Protection Working Party Guidelines on the Right to Data Portability*, 2017, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

поединците да ги добијат своите податоци и повторно да ги користат за свои сопствени цели, преку различни услуги. Поединците имаат можност да ги преместат, копираат или пренесат своите лични податоци од една информатичка околина во друга, на еден лесен и безбеден начин.[264]

Имено, преносливоста на податоци ги има овие карактеристики:[265]

- Го проширува она што може да се направи со лични податоци;
- Им овозможува на поединците поголема контрола врз нивните лични податоци;
- Го охрабрува и го олеснува пристапот до податоци и носи иновација во користењето на податоците;
- Носи нови деловни модели и иновативни услуги со поголем проток и пристап на податоци; и
- Ги намалува бариерите за влегување или проширување на одредени услуги, во ситуации кога податоците претставуваат важен придонес за конкурентите (за да можат да обезбедат споредливи продукти).

Правото на преносливост на податоци има два елементи:

(1) Според член 20(1) на GDPR, поединците чии лични податоци се обработуваат електронски и во структуриран корисен формат, имаат право да добијат копија на тие податоци за понатамошна употреба.

(2) Член 20(2) понатаму го предвидува правото на поединците да ги пренесуваат нивните лични податоци од еден контролор до друг.

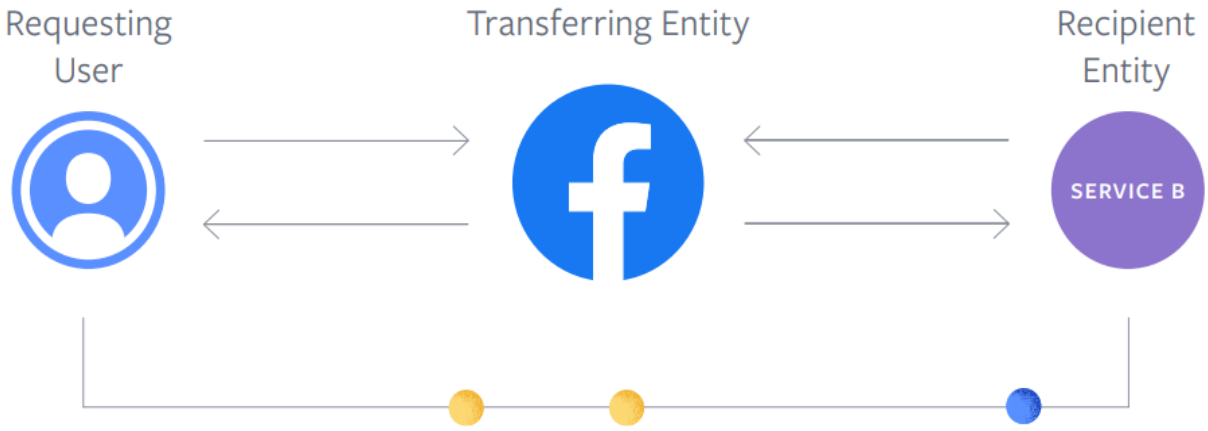
Правото на преносливост важи само кога обработката на податоците е основана според согласноста на корисникот на услугата или со договор, и трансферот на податоци

[264] *United Kingdom ("UK") Information Commissioner's Office – Guide to General Data Protection Regulation (GDPR) /Individuals Rights / Right to Data Portability*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/ (last visited 4 December 2019].

[265] *Discussion Paper on Data Portability: Personal Data Protection Commission In Collaboration with Competition and Consumer Commission of Singapore*, 2019, available at https://www.cccs.gov.sg/resources/publications/occasional-research-papers/pdpc-cccs-data-portability (last visited 4 December 2019].

општо вклучува три странки: корисниците на електронските услуги кои го прават барањето, субјектот кој ги пренесува податоците и примачот на податоците.[266]

Од техничка перспектива, преносот на податоци почнува кога лицето (барател) го упатува субјектот кој пренесува (пренесувач) да ги извезува неговите или нејзините податоци (како што се гледа на слика 2).[267] Субјектот за пренесување ги испраќа бараните податоци или на лицето кое го поднесува барањето, односно субјектот на податоци, или директно до примателот. Штом податоците се споделуваат со примателот, корисникот потоа може да комуницира преку таа услуга.




**Слика 2. Пренос на податоци.**

Според горенаведеното, правото на преносливост се состои од две посебни права на субјектот на податоци:

(1) Прво, постои правото на субјектот на податоците да прими лични податоци.

(2) Второ, постои правото на субјектот на податоците да ги пренесе своите лични податоци на друг управувач (контролор).

[266] Постојат различни технички уреди за остварување на овие трансфери, а во моментов истражувачите развиваат модели кои им овозможуваат на поединците да управуваат со своите податоци и да одлучат каде ќе ги чуваат истите. На пример, системите за управување со лични информации (на англиски: personal information management systems "PIMS") им овозможуваат на поединците да ги чуваат нивните податоци или локално или преку складирање во облак. За повеќе информации, види: Egan, 'Data Portability and Privacy', (2019) , available at https://fbnewsroomus.files.wordpress.com/2019/09/data-portability-privacy-white-paper.pdf.

[267] *Ibid.*, at p.8.

Овие права се одвоени, што значи дека субјектот на податоците може да избере или да ги прими сам своите лични податоци, или може да бара директно пренесување на друг контролор.

Со оглед на тоа што поголемиот дел на личните податоци се обработуваат по електронски пат, се чини дека член 20 на GDPR има широка применливост, па затоа може да донесе значителни придобивки за поединците.

## 3.1 Право на примање на лични податоци

Целта на правото на примање на податоци е зајакнување на контролата на субјектите на податоци врз нивните лични податоци.[268] Согласно член 20(1) на GDPR, поединците чии лични податоци се обработуваат електронски и во структуриран корисен формат, имаат право да добијат копија на тие податоци за понатамошна употреба. Со ова право, субјектот на податоци може да чува лични податоци во неговиот сопствен уред за лични цели и понатамошна употреба. Во овој контекст, правото на преносливост на податоци се сфаќа како продолжување на правото на пристап.[269]

Додека правото на пристап им овозможува на поединците да бараат од контролорот да им достави копија на личните податоци кои се во процес на обработка,[270] правото на преносливост им дава на поединците право да ги примаат своите податоци во структуриран корисен формат.[271] Правото на пристап е широко право кое има за цел да ги информира субјектите на податоци за тоа што се случува со нивните лични податоци. Информациите што можат да се добијат според правото на преносливост се потесни, бидејќи тие се ограничени на лични податоци обезбедени од страна на субјектот на податоците, а не на пример од податоци обезбедени од страна на трети лица.

[268] *supra* note 4, at recital 68.
[269] Bapat, 'The New Right to Data Portability', *Privacy and Data Protection* (2013) , at p.2.
[270] *supra* note 4, at article 15 (3).
[271] *Ibid.*, at article 20 (1).

## 3.2 Право на пренесување на лични податоци

Преку остварување на своето право на преносливост, субјектот на податоци има право да бара пренесување на своите лични податоци директно од еден контролор на друг, ако тоа е технички изводливо.[272]

Додека правото на пристап и правото на примање на податоци му овозможува на субјектот на податоци да ги чува своите податоци во сопствен приватен уред, правото на пренесување обезбедува личните податоци на одредениот субјект на податоци да можат да се користат повторно. Ова им дава на субјектите на податоци сопственост врз нивните лични податоци, бидејќи со нивно барање личните податоци можат да се пренесат директно од еден контролор на друг. Сепак, член 20 на GDPR предвидува ограничување за остварување на ова право, т.е. пренесувањето треба да биде технички изводливо. Поради ова, контролорите на податоци се охрабруваат да развиваат интероперабилни формати кои овозможуваат преносливост на податоци (рецитал 68, GDPR). Во оваа смисла, законот не создава обврска за контролорите да имаат технички компатибилни системи, но тие се охрабруваат да развиваат интероперабилни системи кои ќе овозможат преносливост на податоци.

Техничките барања за спроведување на правото на преносливост на податоци можат да бидат многу високи, бидејќи *de facto* треба да се воспостави техничка мерка што го олеснува трансферот на податоци, која се чини дека е во спротивност со барањето од рецитал 68 на GDPR.[273]

Трансферот на податоци може да биде од три вида (види слика 3):[274]

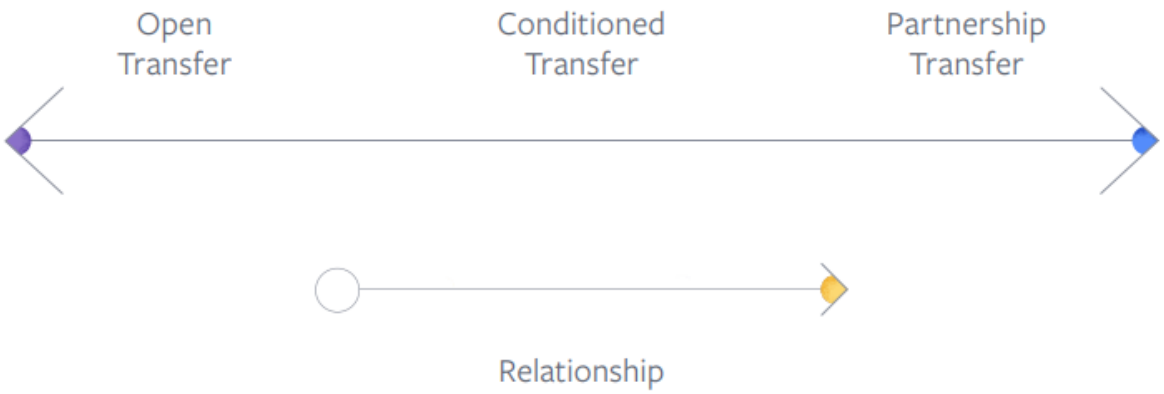
(1) Отворен трансфер – корисниците, односно барателите за пренесување на податоци можат да ги добијат своите податоци и да ги пренесуваат до кој било ентитет (примател) без никаква контрола или ограничување (освен оние предвидени со закон). Во овој модел, или корисникот може да го изврши пренесот на податоците преку свој уред (на пример со опцијата “download your data” Facebook им дозволува

[272] *Ibid.*, at article 20 (2).
[273] Engels, 'Data Portability among Online Platforms', *Internet Policy Review* (2016) , at p.4.
[274] Egan, *supra* note 266, at p.9.

на корисниците да преземаат дадотека што ги содржи сите нивни податоци)[275], или тоа може да се направи преку субјектот што пренесува (контролорот) кој може да прави директен трансфер. Освен техничката врска со цел овозможување на трансфер, субјектот кој го прави трансферот и примачот на податоци немаат никакви односи меѓу себе.[276]

(2) Условен трансфер – субјектите на податоци можат да ги добијат своите податоци и да ги пренесат на било кој примател кој ги исполнува условите наметнати од страна на пренесувачот. Односот помеѓу пренесувачот и примателот на податоците постои само додека трае пренесувањето на податоците. Овој вид на трансфер се смета како директно пренесување помеѓу даватели на услуги.[277]

(3) Трансфер во партнерство – субјектот на податоци може да ги добие своите податоци и да ги пренесува на одреден примател со кој пренесувачот има постојана врска во однос на такви трансфери, и каде постојат услови за тоа како примателот може да ги користи податоците добиени од преносот. Во овој вид на трансфер постојат односи меѓу пренесувачот и примателот на податоците за одредени цели (на пример интегрирање на една од карактеристиките на еден ентитет во прозводите на другиот ентитет).[278]




**Слика 3. Видови на пренос на податоци.**

[275] L. Feiner, *Facebook Addresses Antitrust Concerns with New Tool That Lets You Transfer Photos to Google*, 2019, available at https://www.cnbc.com/2019/12/02/facebook-releases-new-data-portability-tool-for-photos.html (last visited 4 December 2019].
[276] Egan, *supra* note 266, at p.9.
[277] *Ibid.*
[278] *Ibid.*, at p.10.

## 4. Интероперабилност и преносливост на податоци

Научниците истакнуваат дека преносот на податоци не треба да се меша со интероперабилноста, која оди подалеку од преносливост на податоци.[279]

Интероперабилноста се дефинира како можност на различни организации да комуницираат меѓусебно за корисни и заеднички цели, вклучително и споделување на информации и знаења помеѓу нив, преку деловни процеси кои тие ги подржуваат, и преку средства за размена на податоци помеѓу нивни соодветни ИКТ системи.[280] Во контекст на социјални мрежи на пример, интероперабилноста ќе им овозможи на корисниците на Интернет да се поврзат едни со други без оглед на нивната припадност на социјални мрежи, што значи дека еден корисник на Facebook може да објавува порака директно на нечија страница на Google +.[281] За разлика од тоа, според правото на преносливост на податоци, еден корисник на Facebook има право да бара од Facebook да го пренесе неговиот или нејзиниот профил (контакти, фотографии, видеа, итн.) директно на Google +, наместо сам да ги преземе сите информации содржани на Facebook и повторно да ги внесува на Google +.[282] Со други зборови, корисниците на различни електронски платформи и услуги не треба да почнуваат од нула кога менуваат платформи. На пример, Facebook ги охрабрува своите корисници да ги преземат своите списоци со контакти од Gmail, а потоа да ги достават на Facebook (со цел да изградат свој профил на Facebook).[283] Различен пример од социјалните мрежи би бил трансферот на документи или датотеки кои имаат лични иформации (на пр. слики) што корисникот ги поставил за чување во услуга во облак. Во овој контекст, правото на преносливост на податоци ќе им овозможи на корисниците да ги пренесат директно овие информации во друга конкурентна услуга во

[279] Engels, *supra* note 273, at p.4.
[280] Article 2 of Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) OJ L 260, 03.10.2009, p. 20
[281] Graef, 'Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union', *Telecommunications Policy* (2015) , at p.2.
[282] *Ibid.*, at p.8.
[283] B. Cyphers and D. O'Brien, *Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine*, 2018, Electronic Frontier Foundation, available at https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine (last visited 11 September 2019].

облак, без да имаат потреба да ги преземат податоците, да ги зачуваат во свој сопствен уред и пак да ги постават на нова платформа.[284]

## 5. Какви податоци можат да се пренесуваат?

Примарната цел на правото на преносливост е да им дава контрола на субјектот на податоците врз своите лични информации. Но, за какви податоци поточно се зборува? Јасно е дека луѓето треба да имаат можност да ги пренесат своите податоци кои тие ги објавуваат на различни платформи (на пример: објавување на фотографии на социјални мрежи), меѓутоа не е сосема јасно кои други податоци треба да бидат вклучени. Дали можат да се пренесуваат информации кои давателот на услугата ги прима додека корисниците ги користат таквите услуги, како што е историјата на пребарување, податоци за локација, дневна активност, и др.? А што со информациите генерирани од давателот на услугата врз основа на тоа што корисниците поставуваат во Интернет, како заклучоци што се користат за персонализирање на музика, настани и реклами, и др.?

Одредбите на GDPR наведуваат дека треба да има ограничувања на правото на преносливост за одредени податоци. Согласно член 20 (1) на GDPR, субјектот на податоци има право да прима лични податоци што тој или таа му ги доставил на контролорот. Член 29 Работната група (упатства за правото на преносливост на податоци, 2017 год.) предлага луѓето да можат да пренесат лични податоци кои тие активно им ги обезбедуваат на давателот на услугата или кои давателот на услугата ги забележува за нив додека тие ја користат одредената услуга, но не и податоците што давателот на услугата ги подразбира (врз основа на тоа како корисниците ја користат услугата).[285]

Според Работната група, следниве категории се сметаат како податоци обезбедени од страна на субјектот на податоци:[286]

- Податоци активно и свесно обезбедени од субјектот на податоци (на пример: е-пошта, адреса, корисничко име, возраст, итн.)

[284] Graef, *supra* note 281, at p.8.
[285] *supra* note 263.
[286] *Ibid.*, at p.10.

- Податоци кои давателот на услугата ги забележува за субјектот на податоци поради употреба на услугата или уредот. На пример, овие податоци можат да вклучуваат историја за пребарување на едно лице, податоци за сообраќај и податоци за локација.

Спротивно на овие податоци, заклучоците или податоците што давателот на услугата ги подразбира за одредената личност врз основа на тоа како тој или таа ја користи услугата, не се објект на правото на преносливост на податоци (на пример, податоци кој произлегуваат од извештајот во врска со здравјето на корисникот). И покрај тоа што таквите податоци можат да бидат дел од профилот на една личност што го чува контролорот, и истите се изведени од анализа на податоците кои биле обезбедени од страна на субјектот на податоци, тие нема да се сметаат како податоци обезбедни од субјектот на податоци, во контекст на став 1, член 20 на GDPR, и затоа не се објект на правото на преносливост на податоци.

## 6. Техничка изводливост на трансфер на податоци

Субјектот на податоци има право да бара пренесување на своите лични податоци директно од еден контролор на друг, ако тоа е технички изводливо (член 20 (2), GDPR). Според ова, значителен предизвик за спроведувањето на правото на преносливост на податоци претставува „техничката изводливост“ која се бара за пренесување на податоци преку различни платформи.

Тоа што технички е изводливо за еден контролор на податоци може да биде технички неизводливо за друг контролор на податоци.[287] Формулирањето на член 20 (2) на GDPR им остава место на контролорите да тврдат дека одредениот трансфер е технички неизводлив. Како резултат на тоа, пренесувањето на податоци може да биде игнорирано од контролорите на податоци.

Во своите упатства издадени во април 2017 год., член 29 Работната група нуди вредно појаснување во врска со поимот „техничка изводливост“. Работната група

[287] Diker Vanberg, 'The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?', *Journal of Internet Law* (2018) , at p.6.

наведува дека кога нема формати кои заеднички се употребуваат во одредена индустрија или одреден контекст, контролорите на податоци треба да обезбедат лични податоци користејќи најчесто користени отворени формати (на пример: XML, JSON, CSV) заедно со корисни метаподатоци на најдобро можно ниво на грануларност, додека се одржува високо ниво на апстракција.[288]

Што се однесува до „техничка изводливост", Работната група смета дека директниот пренос од еден контролор на податоци на друг контролор може да се случи кога е можна безбедна комуникација меѓу два системи, и кога системот за примање е во техничка состојба да ги прими дојдовните податоци.[289] Ова се смета како отстранување на пречки и инвестирање во нова функционалност во случај кога постоечките системи не го подржуваат трансферот контролор на контролор.[290]

Во однос на директната преносливост контролор на контролор, се чини дека Работната група се потпира на два механизма за мотивирање на директниот трансфер:

(1) Преку вршење на притисок врз субјектот на податоци – овластувајќи ги субјектите на податоци да бараат објаснување зошто контролорите на податоци не можат да понудат директен трансфер од еден контролор на друг;[291]

(2) Преку административен товар - може да се очекува од субјектот на податоци да поднесе повторувачки барања во однос на различни системи.[292]

Дали ќе биде ефикасен притисокот од субјектите на податоци за обезбедување на директен трансфер од контролор до контролор, останува да се види. Ќе биде интересно да се види дали контролорите ќе смислат начин да ја избегнат преносливоста на податоците со тоа што ќе тврдат дека трансферот не може да се оствари поради техничка неизводливост, кога всушност трансферот може да се направи.

[288] *supra* note 263, at p.18.
[289] *Ibid.*, at p.16.
[290] Diker Vanberg, *supra* note 287, at p.7.
[291] *supra* note 263, at p.16.
[292] *Ibid.*, at p.15.

## 7. Преносливост на податоци како право на потрошувачите

Правото на преносливост на податоци има за цел да ја подобри потрошувачката моќ на поединците. Идејата е во тоа што, вооружени со копија на нивните електронски лични податоци и можност да бараат пренесување на нивните лични податоци од еден до друг давател на услуга, поединците имаат поголема слобода на избор на даватели на услуги, и како резултат на тоа, им е многу полесно да ги менуваат давателите на услугите. Слободата на избор на потрошувачите доведува до поголема конкуренција помеѓу давателите на услугите и на крај обезбедува подобра вредност на парите.[293] Со други зборови, индивидуалниот потрошувач одлучува дали неговите/нејзините податоци се отворени за други организации, и кои организации треба да ги примат тие податоци. Во оваа смисла, правото на преносливост на податоци им дава на поединците право на информативно самоопределување.[294] Контролата врз податоци складирани во бази на податоци им дава слобода на физичките лица не само да го изберат давателот на услугата, но исто така им обезбедува зајакнување на правата за заштита на нивните лични податоци, бидејќи законодавецот е заинтересиран да ги отстрани ризиците што можат да се појават при таквиот трансфер на податоци.[295]

Со примена на нивното право на преносливост на податоци потрошувачите исто така можат да остварат финансиски придобивки. Така на пример, кога една личност има избор да одлучи да ги отстрани своите лични информации од една компанија која нуди „лоши понуди“ и да ги пренесе на друга компанија која има “подобри понуди, субјектот на податоци може да врши позитивен притисок врз давателите на услуги за да обезбедат конкурентни и подобри услуги или производи.[296]

[293] Bapat, *supra* note 269, at p.3.
[294] Zanfir, 'The Right to Data Portability in the Context of the EU Data Protection Reform', *International Data Privacy Law* (2012) , at p.4.
[295] *Ibid.*
[296] *supra* note 254, at p.10-11.

# 8. Преносливост на податоци: заедничка порта кон фер конкуренција и заштита на приватност

Правото на преносливост на податоци беше дизајнирано за намалување на тешкотиите на поединците да имаат контрола врз нивните лични податоци.

Развојот на Интернетот и технолошките промени ни овозможија да ги зачуваме нашите информации во облаци, така што пристапот е лесен и брз.[297] Можноста за извоз на сите податоци во облаци има една заедничка точка: создавање на огромни количини на податоци.

Овие количини на податоци, особено кога се комбинираат, можат да се сметаат како продолжение на нечија личност во дигиталниот свет, создавајќи дигитален идентитет за таа личност.[298] Од оваа гледна точка, забранувањето на пренесување на своите податоци од еден до друг давател на услуга може да се смета како повреда на човековите права.[299] Во овој контекст, корисниците на податоци градат свој профил на Интернет, и истиот треба да може да биде пренесен од една веб-станица на друга, така што тие не мора да почнат од нула ако одлучат да ја променат дигиталната платформа. Ова може да се илустрира со примерот кој го дава професор Picker: „Еден продавач на eBay има долготрајна репутација која ја изградил внимателно. Ако поединецот одлучи да создаде нов профил, тој повторно ќе биде почетник  и купувачите можеби нема да сакаат да купуваат од него. Но за оваа ситуација има решение: направете го идентитетот на eBay и репутацијата преносливи. Ако јас сум добар продавач во eBay, јас треба да бидам исто толку добар и на другите сајтови“.[300]

[297] Пресметувањето во облак е модел кој му обезбедува на крајниот корисник пристап до споделени ресурси како на пример единици за пресметки, скадирање податоци, бази на податоци и апликации како и сервиси по потреба, без да има потреба да ги купи или поседува. Овие сервиси се обезбедени и менаџирани од страна на обезбедувачот на сервиси, притоа намалувајќи ја потребата за менаџмент од страна на крајниот корисник. Основни карактеристики на облакот вклучуваат: само-сервисирање на барање на корисникот, мрежен пристап, поширок мрежен пристап, повлекување на ресурси, брза еластичност и мерни сервиси. За повеќе информации, види : Ѓ. Доревски, „Пресметување во облак и миграција на апликации - анализа и споредба“ (2017) Универзитет „Св. Климент Охридски“ - Битола, available at http://www.fikt.uklo.edu.mk/assets/uploads/2017/11/Dorevski-Gjoko-17-09-magisterski-trud.pdf.

[298] Zanfir, *supra* note 294, at p.3.

[299] *Ibid.*

[300] Picker, 'Competition and Privacy in Web 2.0 and the Cloud', *John M. Olin Law & Economics Working Paper No. 414* (2008) , at p.8.

Така, поимите „идентитет“ и „репутација“ се неспорно поврзани со личноста. На веб-страници како што е eBay, овие концепти влијаат врз угледот на таа личност. Според ова, развојот на правото на преносливост на податоци може да се поврзе со слободниот развој на идентитетот на еден човек во електронските комуникации, и крајната цел на ова право може да се смета како слободен развој на човечката личност. Средствата за постигнување на оваа цел се технички процеси кои се директно поврзани со заштитата на информативната приватност и фер конкуренција.[301]

## 9. Преносливост, обработка во облак (Cloud computing) и конкуренција

Креаторите на политиката за преносливост на податоци која е принцип кој дозволува земање на податоците од една услуга и преместување во друга услуга, се согласуваат дека правото на преносливост може да помогне во промовирање на онлајн конкуренција и ја поттикнува појавата на нови услуги. Експерти за конкуренција и заштита на податоци се согласуваат дека иако се појавуваат сложени проблеми, преносливоста им помага на луѓето да ги контролираат своите податоци и им олеснува да изберат меѓу различни даватели на електронски услуги.[302]

Преносливоста на податоците се идентификува како една од главните предизвици со кои се соочуваат услугите во облак (англиски Cloud computing) во нивниот развој како дигитален пазар.

За да се разбере поврзаноста на правото на преносливост на податоци со обработката во облак, најпрво треба да се дефинира обработката во облак.

Пресметување во облакот или англиски, Cloud computing е преместување засновано на Интернет, каде повеќе поврзани опслужувачи овозможуваат ресурси, софтвер, и податоци за компјутерите и други уреди кои имаат дадено барање до нив, што многу наликува на мрежата за електрична енергија. Овој начин на пресметување, најчесто ги користи веб-базираните алатки или апликации, кои на корисниците им даваат достапност до ресурси, програми и слично, преку прелистувачите, исто како тие да се инсталирани локално на нивните сопствени сметачи. Деталите се преземаат од корисниците и тие веќе

[301] Zanfir, *supra* note 294, at p.3.
[302] Egan, *supra* note 266, at p.3.

не мора да се експерти или да имаат контрола на технологијата која се наоѓа „во облакот“. Фундаменталниот концепт на пресметувањето во облак е дека пресметувањето и податоците кои се потребни за него не се на некое специфицирано место, па дури не е задолжително сите елементи да се на исто место (опслужувач). Генерално, корисниците на облачното пресметување не ја поседуваат физичката инфраструктура, туку најмуваат услуги од некој провајдер со што ефикасно се намалуваат нивните трошоци. Тие користат ресурси како сервис, а плаќаат само за ресурсите кои ги користат.[303]

Службите кои ги нудат апликациите кои се користат за процесирање на облакот нудат софтвер како сервис преку Интернет, со што се елиминира потребата од инсталации и извршување на апликации на компјутерите на корисниците, со што пак се намалува потребата од поддршка и одржување. Според Наумовски и Рашковски, Cloud технлогијата се дефинира како техничко уредување согласно кое корисниците ги чуваат своите податоци на оддалечени сервиси, под контрола на други софтверски апликации.[304] Главните карактеристики на пресметувањето во облак се состојат од:[305]

- Пристап и менаџирање на комерцијален софтвер преку мрежа.
- Активностите се контролираат од централна локација наместо кај секој корисник, со што се овозможува корисниците да пристапат кон апликации на оддалеченост преку Веб-от.
- Доставувањето на апликациите е типично еден на многу врски, а не еден на еден врска, и вклучува архитектурални, оценувачки, партнерски и менаџерски карактеристики.
- Централизирано обновување, што ја намалува потребата од преземање на надоградувања.

Пресметувањето во облак има многу предности за ИТ организациите, кои се презентираат во табела 4.[306]

[303] Технологијата во фокус: пресметување во облакот (2017), available at : womenwin.mk/mk/news/технологијата-во-фокус-пресметување/, (last visited 2 December 2019).
[304] Г. Наумовски and Д. Рашковски, *„Право и информатичка технологија“* (2019), at 159.
[305] Технологијата во фокус: пресметување во облакот (2017), available at : womenwin.mk/mk/news/технологијата-во-фокус-пресметување/, (last visited 2 December 2019).
[306] Доревски, *supra* note 297, at p.95.

**Табела 4. Предности на пресметувањето во облак.**

| Предности | Опис и карактеристики |
|---|---|
| **Намалени трошоци** | -намалени трошоци за хардвер и софтвер<br>-претпријатието плаќа месечна претплата за точен број корисници на кои им е потребна апликацијата |
| **Сигурност** | -разни даватели на услуги во облак нудат повеќе видови сигурност<br>-веб базираните системи во реалноста се еднакво или повеќе сигурни и имаат еднаква или подобра интерна контрола од локално базираните системи |
| **Одговор во работењето** | -додавањето нов софтвер е едноставно<br>-претпријатието може многу брзо да пристапи до ресурсите доколку дојде до проширување на капацитетот на работата |
| **Едноставна администрација** | -веб пребарувачот е сè што е потребно за да се пристапи од книговодството<br>-сите корисници ја имаат истата верзија на софтвер<br>-нуди back up во реално време што резултира со намален број на изгубени податоци |
| **Глобален пристап** | Вработени, партнери и клиенти можат да пристапат и да ги ажурираат податоците каде и да се наоѓаат |
| **Можност за тестирање пред купување** | -многу апликации се достапни во облак и обично може бесплатно да се тестираат<br>-ова им овозможува на компаниите да проверат дали апликацијата ќе одговара на нивните потреби |

Извор : Ѓоко Доревски, „Пресметување во облак и миграција на апликации - анализа и споредба“ (магистерски труд), Универзитет „Св. Климент Охридски“ – Битола, Факултет за Информатички и комуникациски технологии.

Cloud технологијата има потенцијал да го трансформира компјутерот во еден модел базиран на услуга, каде обезбедувачите на облаци градат облачни системи и поголемиот дел од корисниците стануваат „потрошувачи“ на таквите услуги. Во една динамична

компјутерска индустрија, обезбедувачите на облаци, односно давателите на услуги во облаци сè повеќе и повеќе стануваат одговорни за осигурувањето дека индивидуалните компоненти на хардверот и софтверот работат заедно за да ја обезбедат услугата ветена на клиентот. Во контекст на оваа фундаментална промена, владите треба да инвестираат релативно помалку ресурси за „интероперабилноста на системите“, бидејќи товарот за работа на хардверот и софтверот оди на обезбедувачите на облаци наместо на потрошувачот.[307]

Додека интероперабилноста на системите станува примарен домен на обезбедувачот на облак, проблемите околу интероперабилноста на податоците сè уште остануваат важни, а можеби дури и критични, бидејќи владини податоци остануваат содржани во системите обезбедени преку обезбедувачите на облаци. Прашањето на преносливост на податоци во облак е важно за владите, затоа што тие се заинтересирани да се осигурат дека клиентите можат да се префрлат од еден на друг давател на услуга во облак, без да имаат неразумни трошоци за префрлување. Општо, кога клиентот го менува давателот на услуга во облак, разумно е да се претпостави дека ќе има одредена сума на трошоци за префрлување. Сепак, од перспективата на преносливост во облак, важно е податоците да можат да се разменуваат помеѓу обезбедувачи на облаци, бидејќи без можност за пренесување на податоци, префрлувањето од еден на друг давател на услуга во облак станува невозможно.[308]

Во овој контекст, преносливоста на податоци има влијание врз конкуренцијата, особено во јавни облаци, затоа што постои ризик клиентот да биде заклучен со добавувачот. Со други зборови, обезбедувачите на облаци можат да создадат големи трошоци за префрлување, на пример преку ограничување на преносливост на податоци на клиентите до конкурентните услуги.[309] Оттука, потенцијалните ограничувања на преносливост на податоци ги спречуваат потрошувачите да користат комплементарни услуги во облак (Cloud services) и да ги трансферираат своите податоци од еден до друг давател на услуга. Според ова, ако потенцијалните клиенти сметаат дека ризикот за

[307] Ahmed, 'Data Portability: Key to Cloud Portability', *SSRN Electronic Journal* (2010) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1712565 , at p.2.
[308] *Ibid.*
[309] Sluijs, Larouche and Sauter, 'Cloud Computing in the EU Policy Sphere Interoperability, Vertical Integration and the Internal Market', *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2012) , at p.15.

префрлување е многу висок, тие целосно ќе се воздржат од купување на услуги во облак.[310]

Трошоците за префрлување се поттикнуваат од трошоци за кординација. Без преносливост на податоци, тие не можат да се пренесат на друга платформа и информациите кои еднаш биле споделени, т.е. податоци кои корисникот директно или индиректно ги „вложил“ како што се пораки, фотографии, углед и историја на пребарување, остануваат во оригиналната платформа. Поради ова, корисникот најверојатно ќе остане со платформата во која првично ги доставил своите податоци, иако друга платформа можеби е многу привлечна за него. Ова може да нанесе штета врз конкуренцијата, затоа што конкурентните платформи би немале стимул да иновираат и да нудат подобри услуги, знаејќи дека корисниците сепак ќе останат во сегашната платформа.[311]

Трендот на пресметување во облак не доаѓа без никакви проблеми. Заштитата на податоците и безбедноста на податоците се номинирани како главни правни проблеми поврзани со пресметувањето во облак.[312] На пример, безбедносни фирми како NSO Group тврдат дека можат да влегуваат во серверите на облак и да имаат пристап до податоци за локација, архивирани слики или пораки на таргетирани субјекти, со што предизвикуваат сомнеж дали компаниите можат да чуваат безбедни одредени лични информации, корпоративни тајни, класифицирани владини материјали, и сл. Освен тоа, дури и ако серверите во облак останат технички безбедни, владите можат да ги принудат компаниите да откриваат одредени податоци (како што се комуникација преку е-пошта или текстуални пораки) што се одржуваат во облакот.[313]

Може да се замисли дека зголемувањето на правото на преносливост на податоци во услугите во облак ќе ја намали приватноста и заштитата на податоци. Меѓутоа, Zanfir смета дека ситуацијата не е таква. Според неа, треба да се обезбедат дополнителни заштитни мерки за обработените податоци во облак, но не да се ограничува

[310] *Ibid.*
[311] Engels, *supra* note 273, at p.5.
[312] P. Balboni, K. Mccorry and W. D. Snead, *Cloud Computing. Benefits, Risks and Recommendations for Information Security*, 2009, European Networks and Information Security Agency (ENISA), available at https://www.pdpjournals.com/docs/88049.pdf (last visited 1 November 2019]; Наумовски and Рашковски, *supra* note 304, at p.159-180.
[313] S. Feldstein, *The Global Expansion of AI Surveillance* (2019), at p.23.

преносливоста, бидејќи преку обезбедување на преносливост на податоци, поединците уживаат зајакнување на нивното право на 'информативно самоопределување'.[314]

Во оваа смисла, правото на преносливост на податоци треба да се поврзе со правото на приватност и правото на заштита на лични податоци. Така, за да имаат вистинска контрола врз своите податоци складирани во бази на податоци, и да имаат слобода да го изберат давателот на услуга што ги чува и обработува нивните податоци, поединците имаат право на информативно самоопределување. Законодавецот треба да ги зајакне одредбите за заштита на податоци за да се отстранат ризиците кои можат да се појават при трансфер на податоци (во контекст на правото на преносливост на податоци).[315]

## 10. Практични размислувања за преносливоста на податоците во облак

Податоците во облак можат да се категоризираат во следниве категории:[316]

1) Податоци за корисникот: тие се податоци кои корисникот ги внесува во услугата во облак, како што е: е-пошта, имиња на клиенти, лозинки, контакти, трансакции, итн.
2) Придружни податоци: метаподатоци или други такви податоци кои се поврзани со податоците на корисникот. Пример на такви податоци може да вклучуваат логови на е-пошта, индекси, итн. Овие податоци им помагаат на давателите на услуги во облак за обезбедување на подобри услуги и можат да бидат врзани за одреден клиент.
3) Податоци за системот: како што се логови на системи, контроли, итн., кои услугите во облак ги користат за обезбедување на ефикасна услуга за нивните клиенти. Овие податоци помагаат во работењето на системот, но не се поврзани директно со податоците за корисникот.

[314] Zanfir, *supra* note 294, at p.4.
[315] *Ibid.*
[316] Ahmed, *supra* note 307, at p.10.

Услугите во облак треба да бидат изградени на таков начин што ќе овозможат издвојување на податоците за корисникот и податоците за системот, за да се овозможи лесно извлекување, односно пренесување на податоците за корисникот. Корисниците често вложуваат многу време во создавањето и организирањето на нивните податоци, како што е организирање на е-пошта и документи, албуми на фотографии, библиотеки, итн. Способноста за пренесување на податоците за корисниците без можност за извоз на придружни податоци може да доведе до неразумни трошоци за корисниците.[317]

## 10.1 Сопственост на податоци во облак

Основен концепт во контекст на преносливоста на податоците е сопственоста. Некои компоненти на услугата во облак како што се: хардвер, софтвер, дизајн на услугата и др. се на одговорност на давателот на услугата во облак.[318] Меѓутоа, кога станува збор за лични податоци, луѓето би кажале дека сè уште имаат сопственост врз нивните податоци складирани во една услуга во облак. Додека тие можат да бидат во право во одредена смисла, тоа не е секогаш така. На пример, да го разгледаме Facebook, кој многу луѓе го користат како складирање во облак за да ги зачуваат своите фотографии. Според договорот за крајниот корисник на Facebook, компанијата ги чува податоците онолку колку што е потребно, што може да биде различно од тоа што го сакаат корисниците. Ова подразбира дека корисниците ја губат сопственоста на податоците.[319]

Според Dan Gray, вистинската сопственост на податоците во облак зависи од природата на податоците и местото каде тие се создадени. Тој наведува дека има два вида на податоци што се чуваат во облакот. Првата категорија се податоци што ги создава корисникот пред да ги постави во облак, а другата категорија се податоци кои се создадени од самата платформа во облак. Податоците кои се создаваат пред испраќање во облак можат да бидат регулирани со соодветни закони за авторски права во зависност од

[317] *Ibid.*
[318] *Ibid.*
[319] D. Porter, *Data Ownership in the Cloud – How Does It Affect You?*, 2016, available at https://www.getfilecloud.com/blog/2016/11/data-ownership-in-the-cloud-how-does-it-affect-you/#.Xek8eZNKjIU (last visited 5 December 2019].

серверот во облак, додека податоците што се генерираат после складирање во облак имаат сосема нова и комплицирана димензија на сопственост.[320]

Во принцип, сопственоста на податоците во облак е комплицирано прашање.,определено од политиките на владите и компаниите, и не може секогаш да се задржи. Во зависност од политиките на давателот на услугата во облак и категоризирањето на податоците, на корисникот може да му се даде целосна сопственост врз неговите податоци. Меѓутоа, ако тоа не се случи, може да дојде до нарушување на правата на приватност и заштита на личните податоци. Поради ова клиентите на услугите во облак треба да обрнат големо внимание на договорот што го потпишуваат со давателот на услугата во облак и законите според кои провајдерот работи.[321]

## 10.2 Приватност и безбедност на податоците

Постојат различни деловни модели за даватели на услуги во облак. Некои даватели на услуги во облак се потпираат и зависат од приходи засновани на претплата, додека другите се потпираат на бизнис модели базирани на рекламирање, кои можат да имаат ефект во трошоците на услугата, така што на корисниците им се нуди пониска цена во размена на употребата на нивните податоци за комерцијални цели. Владите треба да се осигурат дека корисниците ги разбираат овие размени пред да донесат одлука за користење на одредена услуга во облак.[322]

Во врска со обработката на податоците во облак и користењето на таквите информации за комерцијални цели, научниците тврдат дека ова може да резултира со злоупотреба на приватноста на податоците. Така на пример, во нивната книга „Право и информатичка технологија“ Гоце Наумовски и Драги Рашковски истакнуваат дека употребата на Cloud технологјата (особено кога станува збор за прекугранични „облаци“) е поврзана со голем број на комплексни прашања за приватност, како што се:[323]

[320] D. Gray, *Data Ownership In The Cloud*, 2014, available at https://dataconomy.com/2014/03/data-ownership-in-the-cloud/ (last visited 5 December 2019].
[321] Porter, *supra* note 319.
[322] Ahmed, *supra* note 307, at p.12.
[323] Наумовски and Рашковски, *supra* note 304, at p.161.

- Прашањата поврзани со операторите на прекуграничните Cloud технологии (како што е, на пример, Google); и
- Прашањата поврзани со корисниците на прекуграничните Cloud технологии (како што е, на пример, банката која ги користи овие технологии за информација за клиентот).

Правните прашања со кои се соочуваат Cloud операторите и корисниците, произлегуваат од фактот дека личните податоци се пренесуваат преку територијални граници, каде што се применува одредена регулатива за приватност, која се разликува од една организација до друга, а кои се јавуваат како актери во трансакција. Има и случаи кога Cloud операторот при прекуграничниот пренос на податоци ја задржува контролата над овие податоци и не ја пренесува на трети лица.[324] Во овој контекст, владите треба да обезбедат поддршка и заштитни мерки, за да се избегнат прашањата на приватност и безбедност на податоци обработени во облак. Давателите на услуги во облак исто така треба да обезбедат транспарентни услови во однос на приватноста на податоците, особено за употребата на податоците за комерцијални цели.[325]

Специфични заштитни мерки треба да се применуваат за чувствителни информации поврзани со национална безбедност, за да не се изложат владите на ризик. Безбедносните барања на услугата во облак ќе зависат од чувствителноста на податоците. Владите треба јасно да ги дефинираат и да ги категоризираат безбедносните барања околу нивните податоци, и да се осигураат дека давателот на услугата во облак е запознат со овие класификации и користи транспарентни сертификати, како и други режими кои ги исполнуваат барањата за безбедност.[326]

[324] *Ibid.*, at 161–162.
[325] Ahmed, *supra* note 307, at p.12.
[326] *Ibid.*

## 11. Потенцијални ефекти на преносливоста на податоците врз пазарот

Од економска перспектива, дискусиите за влијанието на преносливоста на податоците[327] се фокусираат на два аспекта:

(1) Намалување на цената на трансферот на податоци; и

(2) Можност за комбинирање на податоци од различни извори. Како резултат на тоа, можат да се обележат некои ефекти, како што се:[328]

- Ефекти врз конкуренцијата на пазарот - што произлегува од потенцијално пониски трошоци за префрлување и бариери за проширување на одредена услуга, каде што барањата за преносливост им овозможуваат на потрошувачите да ги менуваат давателите на услуги; ова им овозможува на компаниите (постоечки или нови) кои се потпираат на податоци како важен придонес, да конкурираат соодветно и ефикасно на одреден пазар на услуги. Во овој контекст, клучен ефект на преносливоста на податоците е тоа што може да ги намали бариерите за влез или проширување на одредени услуги, бидејќи различни компании кои немаат свои клиенти, можат да добијат податоци со пониска цена. Влијанието за намалување на овие бариери е особено важно во ситуации кога податоците претставуваат важен (па дури и суштински) елемент (input) и организациите не можат да стекнат податоци по никоја цена. Според тоа, ако поединците нема да се повикаат на своето право на преносливост на податоци и не го користат својот избор за префрлување во нови организации, можноста на новите компании да имаат корист од овие преноси се намалува.
- Надворешни придобивки – што произлегуваат од зголемената употреба на податоци; преносливоста води кон обезбедување на огромна количина на податоци од страна на поединци и организации, а тоа може да носи вредност што не се рефлектира (експлицитно) во придобивките добиени од самите поединци. Во овој контекст, кога една личност ги споделува своите податоци со една организација, тој/таа за возврат добиваат

[327] Постојат тензии помеѓу потенцијалните придобивки на преносливоста на податоците и аспектите за имплементација на ова право. На пример, прашањата за пониски трошоци за префрлување ако обемот на правото на преносливост опфаќа само ограничен опсег на податоци. Спротивно на тоа, едно сеопфатно право на преносливост на податоци може да резултира во поголеми трошоци за компаниите кои го спроведуваат таквото право. За повеќе информации, види: *supra* note 254, at p.8.

[328] *Ibid.*, at p.9-10.

одредена услуга или одреден производ. Меѓутоа, компанијата може да ги користи податоците на поединецот за подобрување на своите производи и услуги, или за развивање на нови услуги и производи. Овие придобивки не се однесуваат само на субјектот на податоци-личноста која ги дава своите податоци, туку голем број на потрошувачи со исти или слични карактеристики со субјектот на податоци исто така имаат корист од новите подобрени услуги и производи.

- Повисока продуктивност – како резултат на комбинирање на податоци од различни извори, со што се намалуваат трошоците за производство на производи и услуги. Преносливоста на податоците го проширува пристапот на една организација до податоци, бидејќи добивањето на податоци станува поевтино. На организациско ниво, секој процес на производство што се потпира на податоци ќе има подобри резултати. Истражувачите исто така кажуваат дека организациите кои се ориентирани кон податоци имаат 5-6 % повисока продуктивност од она што би се очекувало со оглед на нивните инвестиции и употреба на информатичка технологија.[329]

- Иновација – што е резултат на комбинирање на податоци на нови начини преку различни организации и индустрии. Повеќе видови на податоци, односно пристап до повеќе извори на податоци исто така значи дека организациите можат да обезбедат подобар увид за однесувањето на потрошувачите. Во оваа смисла, организациите се подобро позиционирани за развој и подобрување на различни производи, прилагодени на желбите на нивните клиенти. Како резултат на ова, трошоците за развој на производи можат да се намалат, затоа што компаниите имаат подобра можност да ги разберат нивните клиенти за она што тие сакаат. Заштедените финансиски средства можат да се пренесат на други дополнителни услуги (на пример, реклами) кои ќе бидат поевтини, бидејќи компаниите имаат можност да ги таргетираат своите стратегии за маркетинг кон релевантни потрошувачи.

[329] Brynjolfsson, Hitt and Kim, 'Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance?', (2011) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486 , at p.5.

| Исход | Ефекти на правото на преносливост |
|---|---|
| **Префрлување** | -Преносливоста на податоци го олеснува преместувањето на податоците. Ова ги намалува трошоците за префрлување на потрошувачите (субјекти на податоци)[330] |
| **Конкуренција** | -Намалувањето на трошоците за префрлување им овозможува на потрошувачите да се префрлат кај давателот на услуга кој има подобра понуда. Ова може да ја подобри конкуренцијата и да ги намали потенцијалните бариери за влез и проширување во одредена сфера.[331] |
| **Иновација** | -Преносливоста на податоците може да има влијание во иновација, особено на соседни пазари каде организациите нудат комплементарни производи и/или услуги.[332] |

## 12. Преносливост, импликации за приватност и правни проблеми

Кога станува збор за правни аспекти, преносливоста на податоци претставува прашање за приватност и безбедност на податоците. Кога податоците се пренесуваат од еден контролор на друг, податоците можат да завршат во погрешни раце, ако пристапот му е даден на погрешна личност.[333] Така на пример, кога податоците се преносливи, една измама на идентитет може да се претвори во долготрајна злоупотреба на личните податоци, бидејќи хакерот може лесно да го пренесе својот лажен идентитет на различни платформи. Оваа ситуација е особено алармантна во случај на слаба автентикација.[334]

Член 29 Работната група не нуди сосема јасност во однос на стандардите за безбедност кои се очекува да се применуваат од страна на контролорите. Одговорноста за безбедност на податоци паѓа врз тековниот контролор на податоци и укажува дека

[330] *supra* note 254, at p.12.
[331] *Ibid.*
[332] *Ibid.*, at p.13.
[333] *Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security*, 2000, available at https://govinfo.library.unt.edu/acoas/papers/finalreport.htm (last visited 28 November 2019].
[334] Engels, *supra* note 273, at p.4.

мерките за намалување на ризикот на злоупотреба на податоци можат да вклучат користење на дополнителни информации за автентикација, како што е на пример OTP (one-time-pasword), суспендирање или замрзнување на преносот ако има сомневање дека профилот е компромитиран; во случај на директен пренос од еден контролор на друг треба да се користи автентикација базирана на токен.[335]

Според горенаведеното, за да се намали ризикот за пристап на одредени податоци од трети (неовластени) лица, контролорите треба да користат техники кои соодветно ги автентицираат потрошувачите – т.е., техники кои обезбедуваат доволен доказ дека одредената личност е овластена да има пристап до личните податоци. Бидејќи сè повеќе и повеќе од нашите лични информации се чуваат на Интернет, потребата за добра автентикација преку Интернет станува сè посилна, а нови решенија продолжуваат да пристигнуваат на пазарот.[336]

Друг правен проблем што се предизвикува од преносливоста на податоците е фактот што повеќе личности можат да бараат контрола врз одредени информации. Од овој аспект, пренесувањето на овие информации може да ги повреди правата на имот на третите лица. Правото на преносливост на податоци е исто така тешко да се применува во случаи кои се однесуваат на повеќе субјекти на податоци кои не се согласуваат за трансферот на податоците. На пример, може да се појави случај кога повеќе луѓе се на една фотографија: ако еден корисник пренесува информации за втор корисник, ова може да ги повреди правата на приватност на вториот корисник.[337] Во овој контекст, се поставува прашањето: Што се случува кога едно лице сака да пренесе податоци што се поврзани со друго лице? Што ако, на пример, лицето А сака да ги премести своите фотографии од една услуга во друга, но на тие фотографии е вклучено лицето Б? Кои се правата на лицето Б за контрола на своите лични информации во ова сценарио? Што ако луѓето сакаат да ги извезуваат нивните списоци со адреси на е-пошта (на пример од Gmail на Outlook), содржините на своите телефонски контакти или списоци на родендени во друга услуга? Дали споделувањето на овие податоци со нова услуга ги нарушува правата на приватност на лицата на кои се однесуваат информациите? Како што овие примери

[335] *supra* note 263.
[336] *supra* note 301.
[337] Engels, *supra* note 273, at p.4.

илустрираат, понекогаш е тешко да се разграничи чии податоци треба да бидат пренесени согласно правото на преносливост на податоци.

Коментаторите на овие прашања честопати ги опишуваат податоците на трети лица кои се однесуваат на преносливоста на податоците на одредено лице, како „социјален график“ – карта за врски помеѓу еден корисник и други корисници на иста услуга.[338] Некои застапници на правото на преносливост на податоци тврдат дека услугите кои ние ги користиме во денешно време мора да им овозможат на луѓето да ги пренесат не само своите податоци, туку и податоците за нивниот социјален график.[339]

Став 4 на член 20 (GDPR) наведува дека правото на преносливост на податоци не треба да има негативно влијание врз правата и слободите на другите. Меѓутоа упатствата на Работната група јасно укажуваат дека дури и ако преносливоста на одредени податоци влијае врз правата на приватност на трети страни, тоа не претставува пречка за пренесување на друг контролор. Предложеното решение за справување со потенцијалните недостатоци е двострано:

(1) Прво, операциите за обработка на податоци иницирани од субјектот на податоци, во контекст на лична активност што има потенцијално влијание врз трети страни, остануваат под негова одговорност, до степен до кој таквата обработка не се одлучува (на било кој начин) од контролорот на податоците.[340] Со други зборови, според упатствата од 2017 година за правото на преносливост на податоци, ако податоците се однесуваат на лицето што го поднесува барањето за пренос, а исто така и на трети лица, одговорноста паѓа врз лицето кое го прави барањето. Ова значи дека субјектот на податоците треба да се осигури дека правата за заштита на лични податоци на трети лица нема да бидат оштетени. Така на пример, ако една личност бара пренесување на податоци од неговата банкарска сметка, која освен податоци за имателот на сметката исто така содржи лични податоци во врска со трансакции на трети лица (на пример, ако тие пренесувале пари до имателот на сметката), правата и слободите на овие лица веројатно нема негативно да влијаат врз пренесувањето на информациите до имателот на сметката - под услов сите податоци да се користат за иста цел (т.е., една адреса за контакт да се

[338] Egan, *supra* note 266, at p.12.
[339] *Ibid.*
[340] *supra* note 263, at p.11.

користи само од субјектот на податоци или како увид за трансакциската сметка на субјектот на податоци).[341]

(2) Второ, правата и слободите на трети страни нема да бидат почитувани, ако контролорот на податоци ги користи личните податоци за други цели,[342] (на пример, ако контролорот ги користи личните податоци на трети лица за цели на маркетинг).

Покрај тоа, како што Grimmelmann истакнува, луѓето можат лесно да ги избегнуваат ограничувањата за приватноста поставени од една платформа со пренесување на податоците на друга платформа која нема такви ограничувања. На пример, секој што има пристап до преносливи информации на социјална мрежа А, сега е овластен да ги пренесува овие информации на социјалната мрежа Б. Во овој процес, тие можат да ги отстранат информациите за кои се применуваат ограничувања (било какви: правни, технички или социјални) на социјалната мрежа А.[343]

Бидејќи податоците на социјалните мрежи стануваат сè повеќе преносливи, истите стануваат помалку безбедни, и со тоа помалку приватни. Додека придобивките на правото на преносливост се јасни, за да се изградат алатки за преносливост на кои луѓето им веруваат и можат да ги користат ефективно, треба да се развијат јасни правила за тоа кои видови на податоци треба да бидат пренесени и кој е одговорен за заштита на таквите податоци кога тие се движат кон различни даватели на услуги.

## 13. Како да се заштити приватноста додека се овозможува преносливоста?

Во горенаведената анализа на правото на преносливост на податоци се вклучуваат прашања во врска со околностите пред луѓето да решат да ги пренесат своите лични податоци, како што се: кои видови на податоци можат да бидат пренесени, за каков вид на трансфер се работи, чии податоци можат да се пренесат, итн. Откако ќе ги дознаеме одговорите на овие прашања, следно што треба да прашаме е како може да се обезбеди преносливоста без да се повредат правата на приватност и заштита на лични податоци?!

[341] *Ibid.*
[342] *Ibid.*
[343] Grimmelmann, 'Saving Facebook', *Iowa Law Review* (2009) , at p.1194.

Законот обезбедува мала заштита во однос на овие трансфери. Засегнатите страни изразија загриженост во врска со ризиците за приватност и безбедност на податоци при остварување на правото на преносливост на податоци на една личност, и за недостаток на јасност од креаторите на политиките и регулаторите за тоа што се очекува од субјектите кои пренесуваат лични податоци.[344]

Како прво, безбедноста на информациите е критично загрижувачка. Пренесените податоци можат да содржат исклучително чувствителни информации за едно лице, и компаниите треба да бидат јасни за потенцијалните ризици пред корисниците да ги пренесат своите податоци на друг давател на услуги. Корисниците не треба да бидат охрабрени да споделуваат информации со недоверливи трети страни, а податоците секогаш треба да бидат заштитени со максимална безбедност на нивната нова локација.[345] За да се зајакне контролата на субјектот на податоците врз своите лични информации, корисниците треба да можат да веруваат дека за време на трансферот и после трансферот, нивните податоци ќе се управуваат со максимална одговорност.

Со оглед на тоа што преносливоста има за цел да им помогне на луѓето да имаат контрола врз своите податоци, субјектите што пренесуваат (контролори) треба да се фокусираат на осигурувањето дека субјектите на податоци имаат достапни информации за преносот на нивните податоци. Ова значи дека субјектите на податоци треба да имаат информации за давателот на услуата на кој сакаат да ги пренесат нивните податоци. За какви информации точно се зборува, како ќе се стават на располагање и од кого, се прашања кои не се целосно и соодветно третирани од креаторите на политиките, регулаторите или други засегнати страни.[346]

---

[344] Види на пример: K. Bankston, E. Null and R. Schulman, *Comments of New America's Open Technology Institute, In the Matter of Competition and Consumer Protection in The 21st Century: The Intersection Between Privacy, Big Data, and Competition*, 2018, Federal Trade Commission, available at https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0034-154926.pdf (last visited 8 November 2019]. („Најголемиот број на електронски услуги сега дозволуваат да ги преземеш твоите информации на социјални мрежи, но што се случува со коментарите на другите луѓе во тие објавувања или вашите коментари и ознаки во фотографиите и објавите на другите луѓе?...Ова се само некои од примерите на нерешената тензија помеѓу моето право на преносливост и правото на приватност на моите пријатели, и таа тензија не е никогаш поголема отколку кога станува збор за преносливост на информации за вашите контакти на социјални мрежи").

[345] G. Gebhart, B. Cyphers and K. Opsahl, *What We Mean When We Say "Data Portability"*, 2018, Electronic Frontier Foundation, available at https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability (last visited 18 September 2019].

[346] Egan, *supra* note 266, at p.13.

Во својата проценка на преносливост, Работната група објаснува дека иако луѓето се одговорни за идентификување на мерките за обезбедување на нивните податоци, субјектот кој го прави трансферот треба да го направи носителот на податоци „свесен“ за мерките, за да му овозможи на личноста да преземе соодветни чекори.[347] Еден документ на Комисијата за заштита на лични податоци на Сингапур сугерира дека контролорите кои ги пренесуваат личните податоци треба да одат подалеку; тие треба да обезбедат информации за тоа како ќе се користат податоците на корисникот; природата на новиот производ или услуга што корисникот ја стекнува; углед и практики за заштита на податоците кои ги применува новиот контролор.[348]

Второ, не е секогаш јасно кои податоци корисникот има право да ги пренесува. Некои барања за преносливост на податоци можат да вклучат податоци поврзани со трети лица (освен податоците на барателот, односно субјектот на податоци). Како што се дискутираше погоре, прашањата за тоа дали овие податоци воопшто треба да се пренесат, се тешки за одговарање. Ако тие податоци се пренесуваат, давателите на услуги ќе треба да сносат одговорност за заштита на интересите и правата на приватност на овие лица. Некои засегнати страни имаат предложено механизми за согласност кои ќе им дозволат на физичките лица да си дадат меѓусебна дозвола (согласност) за извезување на своите податоци од една до друга услуга, на пример, корисникот А да може да му овозможи на корисникот Б да ги сподели податоците на корисникот А со одреден контролор. Со други зборови, еден давател на услуга ќе може да ги праша пријателите на поединецот, чии лични податоци се пренесуваат, а исто така вклучуваат податоци на трети лица, да ја дадат нивната специфична согласност за споделување на нивните информации кога субјектот на податоци се повикува на своето право на преносливост на податоци. Според ова, компаниите ќе имаат можност да извезуваат списоци на пријатели и други форми на лични податоци на одредено лице, кои исто така се однесуваат на информации на трети лица.[349]

[347] *supra* note 263, at p.19.
[348] *supra* note 255.
[349] Gebhart, Cyphers and Opsahl, *supra* note 345.

## 14. Прашања за спроведување на правото на преносливост на податоци во пракса

Основната цел на правото на преносливост на податоци е да ги овласти потрошувачите да бараат копија на нивните електронски податоци, да бараат пренесување на нивните лични податоци на друг давател на услуга, и да се префрлуваат на други даватели на електронски услуги.[350] Оттука, целта на правото на преносливост на податоци се поклопува со целите на други области на правото, на пример: законот за конкуренција, законот за заштита на потрошувачите и слично.[351]

Слично како и другите права на субјектот на податоците во GDPR, преносливоста на податоците е право кое може да се повикува од субјектот на податоците и не може да се потпира на други странки, како што се мали и средни бизниси. На пример, еден мал бизнис не може да бара преносливост на податоци од банката со која има соработка, но поединецот може. Ова предизвикува теоретски проблеми за правото на преносливост во однос на правното спроведување на ова право.[352]

Освен тоа, не е јасно дали корисниците воопшто ќе го користат правото на преносливост на податоци. За да бидеме сигурни дека субјектите на податоци ќе се повикуваат на ова право, најпрво треба да се увериме дека поединците се информирани за тоа што подразбира правото на преносливост на податоци. Поради ова, како што Diker Vanberg истакнува, член 29 Работната група треба да има контакт со националните агенции за заштита на податоци на одредени земји за да се увери дека владите на тие земји направиле потребни инвестиции за едукација на јавноста за нивните права. Како минимум, националните агенции за заштита на податоци треба да обезбедат информации на нивните веб-страници на едноставен и разбирлив јазик, кои објаснуваат како корисниците можат да пристапат до контролорот на податоци ако сакаат да бараат трансфер на своите лични информации, и кои ги информираат корисниците како да направат и поднесат жалба доколку контролорот на податоци одбива да го направи преносот. Поднесувањето на жалба треба да биде лесно, и субјектите на податоци не треба

[350] Bapat, *supra* note 269.
[351] Diker Vanberg, *supra* note 287, at p.11.
[352] *Ibid.*

да имаат значителни трошоци и ризици, бидејќи тоа може да ги обесхрабрува во остварувањето на своите права.[353]

[353] *Ibid.*, at p.12.

# ТРЕТ ДЕЛ – НАДЗОР КАКО ФОРМА НА СОЦИЈАЛНА КОНТРОЛА

Во 21-виот век механизмите за надзор се наоѓаат насекаде. Глобалниот систем за позиционирање (GPS) им покажува на родителите каде се наоѓа нивното дете, софтверите собираат информации што луѓето ги објавуваат на социјалните мрежи, компаниите за осигурување ги снимаат разговорите на нивните клиенти поради „обезбедување на квалитет“, и според броевите за следење може да се следи движењето на секој производ што се купува електронски.

Овие технологии се користат за зголемување на ефикасноста, безбедноста и одговорноста на услугите, меѓутоа истовремено водат кон многу прашања поврзани со приватноста и заштитата на личните податоци. Треба да се истакне дека надзорот не е нужно лоша работа; предизвик е да се најде рамнотежа помеѓу промоцијата на економските вредности и заштитата на приватноста. Од една страна, надзорот носи транспарентност во нашиот личен и професионален живот, меѓутоа истовремено ја намалува нашата приватност.

Без приватност, не само што станува потешко да се формираат вредни социјални односи – односи базирани на ексклузивност, интимност и споделување на лични информации, но исто така да се задржат различни социјални улоги и идентитети. Приватноста заслужува да биде заштитена, како право, бидејќи е клучен елемент за живеење и исполнување на различни улоги во нашиот секојдневен живот: да играме улога на пријател, колега, родител или граѓанин, без да има повреди на овие идентитети без наша согласност. Ова има значителна важност, бидејќи ако се праша еден граѓанин „зошто е важна приватноста“, просечната личност на улица најверојатно нема да се жали за поими како идентитет и автономија, и може да има потешкотии да објасни зошто приватноста заслужува воопшто да биде заштитена.[354] Земајќи во предвид дека во денешно време технологијата се развива со огромни чекори, многу е важно да се еманципира јавноста за можните импликации на користењето на технологијата.

[354] Goold, *supra* note 44, at p.4.

Практиката на масовно собирање на податоци во врска со индивидуалното однесување на Интернет е важен феномен во областа на електронските услуги. Тоа има фундаментално влијание врз тоа како компаниите, луѓето и приватноста се поврзани меѓусебно едни со други, од една страна, и тоа влијае на способноста на поединците да градат свои идентитети, од друга страна.

Како што правниот научник Jerry Kang забележува: „Собирањето на податоци во сајбер просторот произведува детални податоци, компјутерски обработливи, индексирани на поединецот и трајни. Комбинирајте го ова со фактот дека сајбер просторот прави собирање и анализа на податоци експоненцијално поевтино отколку во реалниот простор, и го имаме она што Roger Clarke го има идентификувано како оригинална закана од "dataveillance".[355] Dataveillance (скратена форма на Data Surveillance), како што експертот за информатичка технологија Roger Clarke ја дефинира, претставува „систематска употреба на системи на лични податоци за истрага или следење на активности или комуникации на едно или повеќе лица".[356]

Според Colin Bennet, терминот "dataveillance" е креиран за да се опишат практиките за надзор кои го олеснија масовното собирање и складирање на огромни количини на лични податоци.[357] Според ова, dataveillance е нова форма за надзор, каде што наблудувањето не се прави преку камера, туку преку собирање на факти и податоци. Во овој процес се наблудуваат онлајн активностите на одредени лица, преку алгоритмичко проучување на нивните електронски активности.

Општо земено, може да се каже дека практиките за наблудување се однесуваат на еден процес или систем, каде што податоците собирани за одредена цел се користат за последователно друга, ненамерна цел. Овој процес обично вклучува три елементи: [358]

1) Вакум на политика;

2) Незадоволна побарувачка за одредена функција; и

3) Тајна апликација.

---

[355] Kang, 'Information Privacy in Cyberspace Transactions', *Stanford Law Review* (1998) , at p.1261.

[356] R. Clarke, *Dataveillance and Information Privacy*, available at http://www.rogerclarke.com/DV/ (last visited 6 December 2019].

[357] Bennett, 'The Public Surveillance of Personal Data: A Cross-National Analysis', in D. Lyon and E. Zureik (eds.), *Computers, Surveillance, and Privacy* (1996).

[358] S. Venier and E. Mordini, Competitiveness and Innovation Framework Programme: ICT Policy Support Programme (ICT PSP), 2011, p.19.

Од политичка перспектива, надзорот претставува сериозно нарушување на јавната доверба и ја уништува довербата на луѓето кон технологијата. Загриженоста за приватноста и заштитата на податоците се меѓу најдискутираните аспекти на распоредувањето на техниките за надзор.

# ГЛАВА ПРВА: НАДЗОР ВО ТЕХНОЛОШКИОТ СВЕТ: ИМПЛИКАЦИИ ЗА ПРИВАТНОСТА НА ПОЕДИНЦИТЕ

## 1. Растот на информатичката технологија и технологијата за надзор

Истражувањето за надзор претставува една интердисциплинарна иницијатива за подобро разбирање на современите начини на кои личните податоци се собираат, пренесуваат, и се користат како средство за влијание и управување со луѓето и населението.[359] Во денешно време, надзорот сè повеќе се користи како техника за истражување и подразбира различен modus operandi: надзор на однесувањето, комуникациски надзор, локација и следење, надзор на телото, надзор на ставот, и сл. Постојаното обновување на техничките уреди и дигитализацијата на општеството резултира со постојано нов modus operandi. Преку мобилните уреди надзорот станува глобален феномен.[360]

Кога станува збор за надзор, има бројни дефиниции. Од класичен поглед во кривичната постапка, надзорот се дефинира како електронско следење: „Електронскиот мониторинг е општ термин кој се однесува на форми на надзор со кои се следи локацијата, движењето и специфични однесувања на лицата во рамките на процесот на кривичната правда.“[361]

Меѓутоа, во денешно време, технологијата за надзор не се користи само за откривање, туку и за спречување на криминалот. Новата технологија ги достигнува овие цели со спроведување на специфични практики за наблудување, како што е профилирање,

[359] Lyon, 'Editorial. Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix', *Surveillance & Society* (2002) , at pp.1-7.
[360] Vervaele, 'Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?', in S. Gutwirth, R. Leenes and P. De Hert (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (2014) , at p.116.
[361] Council of Europe, European Committee on Crime Problems (CDPC), Council for Penological Cooperation (PCCP), Scope and Definitions—Electronic Monitoring, PC-CP (2012) 7 rev 2.

dataveillance (скратена форма на Data Surveillance-надзор на податоци)[362] и биометрија. Во едно проактивно и предвидливо општество, секој човек се смета за потенцијален таргет на системите за надзор.[363] Ентузијастите на информатичкото општество прогласуваат една ера на совршена комуникација, каде што „информациите постојат на сите места, во секое време“[364] Достапноста на овие информации може да доведе до губење на приватноста на поединците. На пример, Poster пишува дека детализирани бази на податоци за дневните активности на поединците кои ги водат кредитни компании, продавници, банки, болници, компании за здравствено осигурување, полициски агенции, државни агенции, општини, итн., ги надминуваат законодавните мерки за заштита на приватност.[365] Gumpert и Drucker сметаат дека безбедноста која се постигнува со техники за надзор може да биде во спротивставени интереси со правата на приватност на еден човек.[366]

## 2. Надзор во 21-виот век: паметен надзор

Надзорот во дигиталниот свет е во процес на длабоки промени. Поранешните различни системи за наблудување се конвергираат и се комбинираат.[367] Во денешно време, технологијата за надзор е далеку од аудио и видео снимките. Неодамнешните видови на податоци вклучуваат голем број на податоци кои се однесуваат на однесувањето на луѓето, нивната локација, содржината на е-пошта, итн. Собирањето и обработката на податоци станува покомплексен и автоматизиран процес. Анализата и автоматизацијата на

[362] Dataveillance значи систематска употреба на системи за обработка на лични податоци при тестирање или следење на однесувањето или комуникациите на едно или повеќе лица. За повеќе информации, види:Clarke, 'Information Technology and Dataveillance', *Communications of the ACM* (1988).
[363] Galetta, 'New Surveillance, New Penology and New Resistance: Towards the Criminalisation of Resistance?', in S. Gutwirth, R. Leenes and P. De Hert (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (2014) , at p.107.
[364] Hiranandani, 'Privacy and Security in the Digital Age: Contemporary Challenges and Future Directions', *The International Journal of Human Rights* (2010) , at p.1093.
[365] M. Poster, *The Mode of Information: Poststructuralism and Social Context* (1st ed., 1990).
[366] Gumpert and Drucker, 'Public Boundaries:Privacy and Surveillance in a Technological World', *Communication Quarterly* (2001) , at pp.115-129.
[367] Haggerty and Ericson, 'The Surveillant Assemblage', *British Journal of Sociology* (2000) , at pp.605-622.

податоците може да се прави со помош на техники за профилирање, која се овозможува со податочно рударство.[368]

Langheinrich et al. го анализираат надзорот во модерната ера, кој го нарекуваат паметен надзор и веруваат дека брзата еволуција на паметниот надзор ќе биде водена од пет главни трендови:[369]

1. Квалитативно проширување на податоците што можат да се соберат;
2. Квантитативно зголемување на изворите на овие податоци, како резултат на автоматизација;
3. Повеќе и подобри алатки за анализирање и обработка;
4. Зголемувањето на техниките за надзор како секојдневни алатки; и
5. Конвергенција на системите за надзор.

Како што се појавуваат нови типови извори на податоци, количината на постојните извори на податоци постојано се проширува – заради намалување на трошоците за хардвери за надзор. Камерите стануваат подобри и поевтини, додека сите видеа во живо можат да се чуваат на Интернет и да се пренесат наоколу. Усвојувањето на технологијата за препознавање на лице им овозможува на јавните и приватните субјекти веднаш да го проверат идентитетот на секој што поминува покрај една CCTV камера. До 2020 година, во Кина се предвидува да има една камера на секои две лица.[370] Аеродромите користат скенери за целото тело;[371] додека отпечатоците од прсти, како и скенирање на лицето стануваат сè почести.[372]

[368] Hildebrandt, 'Profiling: From Data to Knowledge', *DuD: Datenschutz Und Datensicherheit* (2006).

[369] Langheinrich et al., 'Quo Vadis Smart Surveillance? How Smart Technologies Combine and Challenge Democratic Oversight', in S. Gutwirth, R. Leenes and P. De Hert (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (2014) , at p.151-152.

[370] P. Bischoff, *The World's Most-Surveilled Cities*, 2019, available at https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ (last visited 3 November 2019].

[371] Скенери за цело тело се користат за откривање на предмети што се во телото на една личност без остварување на физички контакт. Овие скенери, за разлика од металните детектори, можат да детектираат и неметални предмети. За повеќе информации, види: Airport Full Body Scanner Market by Technology (Millimeter Radio-Wave Scanner and Backscatter X-Ray Scanner) and by Airport (Class A, Class B, Class C, Class D, Class E, and Class G): Global Industry Perspective, Comprehensive Analysis, and Forecast, 2018—2025, available at: https://www.zionmarketresearch.com/report/airport-full-body-scanner-market (last visited 7 November 2019).

[372] K. Yamanouchi, *Fingerprints, Facial Scans Becoming More Commonplace at Airports*, available at https://www.thestar.com.my/tech/tech-news/2018/04/12/fingerprints-facial-scans-becoming-more-commonplace-at-airports (last visited 9 November 2019].

Индија ја има една од најголемите светски биометриски бази на податоци,[373] која содржи отпечатоци од прсти и скенирање на ирис на секој од нејзините 1,2 милијарди жители, и Европската Унија сака наскоро да го направи истото. Додека индискиот систем беше промовиран како начин за создавање на финансиска можност преку банкарство и олеснување на пристап до јавните услуги за сиромашните Индијци, истовремено спречување измама и перење на пари; планот на Европската Унија, кој првпат беше предложен во 2016 година, е да се создаде една консолидирана база на податоци[374] која ќе служи како начин за подобро следење на терористите, криминалците и неовластените имигранти.[375]

Новите карактеристики на нови технологии за надзор укажуваат дека собирањето и обработката на податоците се автоматизираат. Од овој аспект, паметниот надзор го проширува концептот на dataveillance, што беше дефинирано од Roger Clarke во 1988 година.[376] Кога Clarke го измисли терминот во 1988 година, главните извори на податоци беа финансиски трансакции (употреба на кредитни картички, повлекување на пари од банкомати, електронски трансфери) и службени записи (судски налози, криминални досиеја, отпечатоци од прсти). Според новите случувања, овие извори се проширија и вклучуваат нови технологии, како што се:[377]

- Употреба на мобилни телефони;
- Користење на Интернет и оставање на дигитални траги, вклучувајќи колачиња, спам и шпионски софтвер;
- Автопати што бараат идентификација на патниците;

[373] N. Sharma, *India's among the World's Top Three Surveillance States*, 2019, Quartz India, available at https://qz.com/india/1728927/indias-among-the-worlds-top-three-surveillance-states/ (last visited 7 December 2019].

[374] Заедничкото складиште за идентитет (Common Identity Repository) ќе консолидира биометриски податоци за скоро сите посетители и мигранти во Европска Унија, како и за некои граѓани на Европска Унија – поврзувајќи ги постојните бази на податоци за криминал, азил и миграција и интегрирање на нови бази на податоци.

[375] G. Dobush, *The EU Wants to Build One of the World's Largest Biometric Databases. What Could Possibly Go Wrong?*, 2019, available at https://fortune.com/2019/05/01/eu-biometric-database-india/ (last visited 19 August 2019].

[376] Dataveillance, според експертот за информатичка технологија Roger Clarke претставува „систематско следење на дејствијата или комуникациите на луѓето преку примена на информатичка технологија". Види: Clarke, *supra* note 362.

[377] Clarke, 'Dataveillance - 15 Years On', *Wellington: Privacy Issues Forum* (2003) , available at http://www.rogerclarke.com/DV/DVNZ03.html.

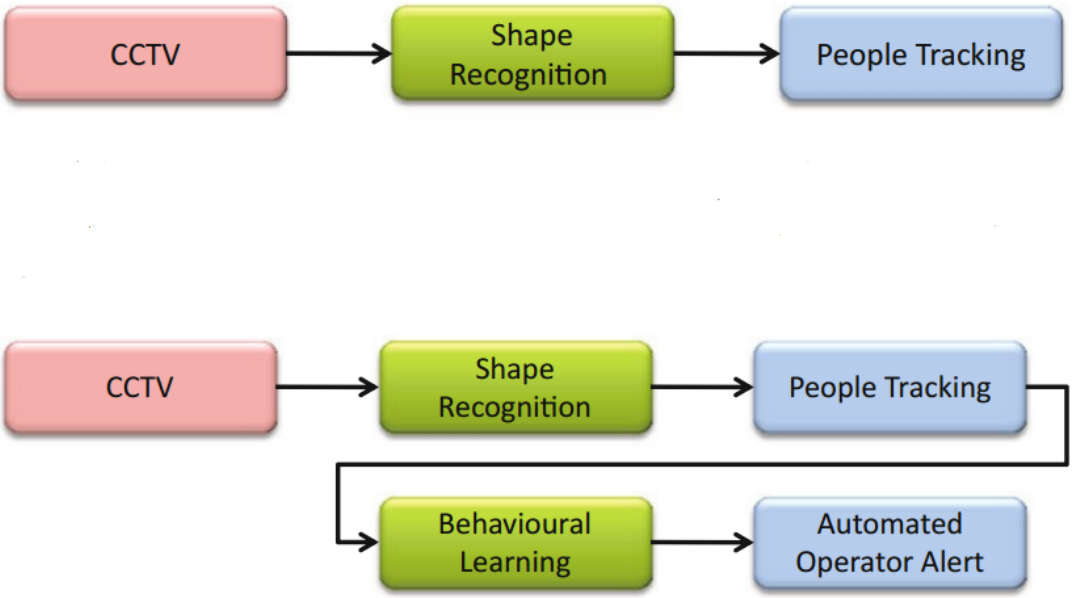
- Управување со дигитални права;
- Предлог за изразување на телефонски броеви како Интернет адреси;
- Идентификација заснована на чипови;
- Дигитални потписи;
- Локација и следење на лица;
- Биометрија;
- Екстракција, складирање и употреба на генетски податоци;

Како последица на тоа, додека во минатото надзорот бил ограничен на користење на безбедносни апликации управувани од институционални актери, денеска речиси секој има достапност до уреди за надзор. Поради ова, надзорот станува вообичаен, една рутина која многу лесно може да се изврши од безбројни актери, бидејќи алатките за надзор стануваат достапни и евтини (на пример, во денешно време речиси секој човек има мобилен телефон, а многу луѓе исто така имаат можност да купат камери, дронови, итн.).

Вистинската моќ на идните паметни системи за надзор лежи во комбинацијата на сите овие можности за прибирање и обработка на лични податоци во поврзани алатки за надзор, каде што излезот (output) од еден систем претставува влез (input) во друг систем (како што е илустрирано на слика 3.)[378]

Еден извор на податоци (на пример, CCTV камера) е влез за единечна фаза на обработка на податоци – во овој случај, тоа е алатка која автоматски детектира човечки форми (на пример ставена на еден паркинг). На крај, оваа алатка (во овој случај CCTV камера) му овозможува на системот да ги следи луѓето во одредениот паркинг, водејќи статистика за нивното движење во текот на времето. Откако системот може да ги следи луѓето на видео, може да се користи алгоритам за учење според кој ќе се класифицира човечкото однесување во „нормална“ и „сомнителна“ состојба, со што операторот може да прими автоматски сигнали секогаш кога ќе има потенцијална кражба на паркингот.

[378] Langheinrich et al., *supra* note 369, at p.153.




**Слика 3. Едноставен пример за паметен надзор**.

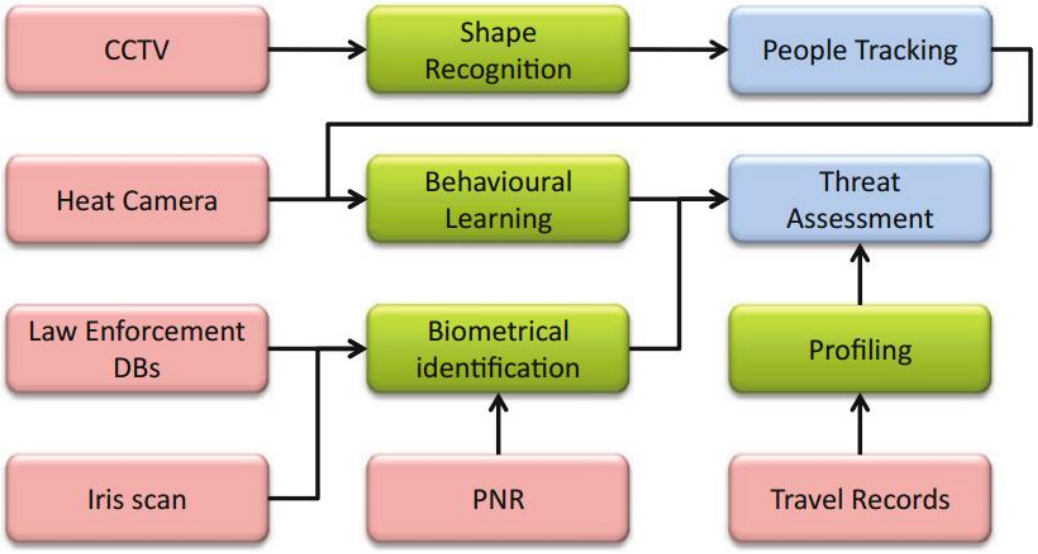
## 2.1 Дефинирање на паметен надзор

Системите за паметен надзор се оние системи кои се способни да извлечат специфични информации од други заробени или постоечки информации (на пример дигитални слики, електронски записи за патување и сл.) со цел да генерираат детализирани описи на настани кои на крај можат да се користат за донесување на автоматски или полуавтоматски решенија.[379]

За подобро разбирање на паметниот надзор, треба да разликуваме три вида на операции на системите за паметен надзор, како што се: извори, алатки и функции (или со други зборови: собирање на податоци, обработка на податоци и употреба на податоци). Во наједноставен случај, еден или повеќе извори обезбедуваат податоци за една алатка, за таа да може да изврши одредена функција (види слика 3). Во обработката на едно дигитално видео, препознавањето на човечки форми овозможува да се детектираат луѓе кои се движат низ сликата, и според ова операторот има можност да одржува едноставна статистика за бројот на луѓето што го посетуваат одредениот паркинг.

[379] *Ibid.*, at p.155.

За посложена функција, се комбинираат повеќе алатки за мониторинг. Така, една алатка може да стане извор за друга алатка што во принцип води кон сложени системи за мониторинг. На пример, еден паметен систем за надзор на аеродромите може да комбинира не само движења на луѓето, туку и други физички сигнали (на пример телесна температура) во системот за алармирање за одредени однесувања. Овие информации можат да се приложат со други информации за патникот од други бази на податоци (на пример биометриска идентификација, записи за патување, итн.), според кои се обезбедува сеопфатно оценување на однесувањето на секој патник и според тоа се проценува дали одредени патници претставуваат закана или не (како што е прикажано на слика 4).[380]




**Слика 4. Проценување на однесувањето на еден патник на аеродром како пример за паметен надзор. Неколку независни системи за наблудување се користат за проценување дали еден патник претставува закана на аеродромот. Системот за учење (behavioural learning) според однесувањето на патникот е само еден од неколкуте придонеси за сеопфатна проценка на одредената закана.**

Системите за паметен надзор се разликуваат од претходните техники за надзор во тоа што овие системи ги надминуваат „обичните“ надзори. На пример, Gary Marx дава дефиниција за „нов надзор“ како употреба на нови технологии со кои се извлекуваат

[380] *Ibid*.

лични информации на поединци, и каде што поголем фокус се става на наблудувањето на населението, наместо следење на одредени лица.[381] Примерите вклучуваат видео и аудио надзор, движење, звук, биометриски уреди, ДНК-анализа, профилирање, податочно рударство, и др. Според Marx, новиот надзор е резултат на различни аспирации за социјална совршеност, кое се обидува да биде безбедно со „нула толеранција". Во оваа смисла, содржината на надзор се проширува на детални лични информации во обид за развивање на разни програми за социјална помош и интервенција, проценување, предвидување и превенција на ризични ситуации.[382] На најопшто ниво, современите тактики за надзор би вклучувале:[383]

- База на податоци за работодавците која ги наведува лицата кои имаат поднесено побарувања за надомест според која се споредуваат апликации за работа;
- Еден работодавач кој задолжително бара примерок на ДНК за вработените;
- Еден супервизор кој ја следи локацијата, е-поштата и телефонската комуникација на вработениот користејќи софтвер кој открива обрасци на употреба на компјутер;
- Паметни домови со паметни уреди кои можат да ги следат и да ги контролираат од далечина електричните уреди (на пример до го спуштат термостатот);
- Совпаѓање на компјутерите и податочно рударство;
- Една компанија за пребарување на Интернет која обезбедува списоци на пребарувани теми и IP адреси до влади и рекламни компании;
- Колачиња (cookies) кои го следат однесувањето на луѓето при користење на електронски комуникации;
- Еден конвенционален уред со термички сензори насочен кон едно лице или една куќа од дрон или сателит кој од далечина (илјадници километри далеку) може да прими термички фреквенции (вклучувајќи и мерење на телесна температура на патници кои заминуваат од меѓународни аеродроми за да се утврди дали тие носат некој грип или вирус).
- Видео монитори во продавници кои ги скенираат клиентите и ги споредуваат нивните слики со слики од база на податоци на лица сомнителни за кражба;

[381] Marx, 'What's New About the "New Surveillance"? Classifying for Change and Continuity', *Surveillance & Society* (2002) , at pp.9-29.
[382] G. T. Marx, *Windows into the Soul: Surveillance and Society in an Age of High Technology* (2016), at p.43.
[383] *Ibid.*, at p.54.

- Една скриена камера на банкомат;
- Анализа на косата за да се утврди употреба на лекови или дроги;
- Полиграф или технологија која ги следи физиолошките промени за да се утврди вистинитоста;
- Интелегентни системи за транспорт;
- Следење на локација преку сигнали на мобилни телефони.

За подобро разбирање на овој развој, треба да се разгледа актуелната технологија за надзор, па затоа во понатамошната анализа ќе се понуди краток преглед на некои од новите технологии за надгледување кои моментално се распоредуваат, како и видови на податоци што тие ги собираат и нивната закана за приватноста на физичките лица.

## 2.2 CCTV камери

Најчесто воведувањето на камери се прави со цел зголемување на безбедноста. На пример, во Скопје стотици камери вршат видео надзор и го снимаат секојдневниот живот на граѓаните. По наредба на јавниот обвинител, снимките се користат како доказ при нарушување на јавниот ред и мир (на пример санкционирање на несовесни возачи и сообраќајни прекршоци) и за разрешување на кривични дела (најчесто за сообраќајки со жртви или со тешко повредени лица).[384]

Меѓутоа не се ретки случаите кога видео надзорот се врши за контрола на одредени поединци, со цел да се следи нивниот живот или однесување. Во овој контекст, се појавуваат многу прашања кои се однесуваат на непримена на технички и организациски мерки за да се биде во согласност со прописите и принципите за заштита на личните податоци. На пример, Дирекцијата за заштита на лични податоци[385] на Република Северна Македонија наведува дека видео надзорот и следење преку мониторинг е во постојан пораст во земјата. Како што се шири следењето на луѓето преку видео надзор така се намалува слободата на движење и однесување на луѓето и нивната приватност. Посебно

[384] М. Митевска, *„Видео надзор само за безбедност, во спротивно нема приватност“*, 2019, Радио Слободна Европа, available at https://www.slobodnaevropa.mk/a/30297066.html (last visited 5 December 2019].
[385] Официјална веб-страница на Дирекцијата може да се најде тука: https://dzlp.mk/mk.

треба да се внимава на видео надзорот на работните места.[386] Граѓаните се заинтересирани да знаат кој снима, за што снима, кој ги чува тие информации, за колку време, и сл. Поради ова, за да се заштитат правата на приватност на физичките лица, Дирекцијата има поставено некои правила за видео надзор на кои треба да им се придржуваат одговорните лица, како што се:[387]

1. Одговорното лице за видео надзор мора да ги информира сите кои ќе влезат во полето на снимање (видео круг) дека просторот се снима. Известувањето мора да ги содржи следниве информации:
    - Дека се врши видео надзор;
    - Името, односно записот на контролорот (одговорното лице) кое го врши надзорот;
    - Информации за тоа каде и колку време се чуваат снимките од системот за видео надзор.
2. Одговорното лице (контролорот) треба да преземе соодветни технички и организациски мерки за да ги заштити личните податоци кои ги собира и да го спречи неавторизираниот пристап до податоците;
3. Камерата мора да се постави на таков агол кој ќе го опфати само она подрачје заради кое се поставува камерата;
4. Снимките не смеат да се користат за друга цел освен ако тоа е потребно во доказна постапка.

За да се зачува првичната функција на видео надзорот, односно да се штити безбедноста на граѓаните, државите треба да донесуваат законски одредби кои наметнуваат законска одговорност за сите лица и/или институции кои ги злоупотребуваат овие снимки и го санкционираат незаконското обработување на личните податоци собрани на овој начин.

[386] За повеќе информации, види: Република Северна Македонија, Дирекција за заштита на лични податоци „видео надзор“, available at: https://dzlp.mk/mk/temi_5 (last visited 5 December 2019).
[387] *Ibid.*

## 2.3 Технологијата за препознавање на лице (биометрика)

Биометриката претставува мерење и анализа на физичките карактеристики на луѓето. Бидејќи биометриските податоци се уникатни за секоја личност, тие често се користат за идентификување на поединците, правејќи ја биометриката една форма на идентификација и контрола – на пример, компјутерите можат да пребаруваат и чуваат такви податоци за неколку секунди, според кои се одлучува дали да се дозволи одредениот пристап или не.[388]

Биометријата е најновиот тренд во сајбер безбедноста.[389] Според едно истражување спроведено во 2018 година, технологија за биометриска автентикација се користи во 62% од компаниите, а 24% планираат да ја искористат во рок од две години.[390] На пример, иако технологијата за препознавање на лице е во голема мерка нерегулирана, некои авиокомпании почнаа да користат технологија за препознавање на лице наместо конвенционални билети за меѓународни летови.[391]

Како што се развива технологијата, користењето на биометриската технологија се менува од првенствено криминална идентификација, во еден широк спектар на секојдневни активности, како што е на пример отклучување на паметни телефони. Над 75% од потрошувачите користеле некаква биометриска технологија, почнувајќи од скенирање на отпечатоци и препознавање на лицето, до геометрија на рацете.[392]

Технологијата за препознавање на лице се смета за дел од биометриката која користи софтвер за мерење на биолошките податоци на поединците, слично на скенирањето на отпечатоци и системите за скенирање на очите/ирисот. Системите за препознавање на лице користат голем број на мерења и технологии за скенирање на лица, вклучувајќи термички слики, 3D мапирање на мапи, каталогизирање на уникатни

[388] S. Liu, *Biometric Technologies -Statistics & Facts*, 2019, Statista, available at https://www.statista.com/topics/4989/biometric-technologies/ (last visited 4 June 2019].
[389] N. Olsen, *Biometrics Laws and Privacy Policies*, 2019, PrivacyPolicies.Com, available at https://www.privacypolicies.com/blog/privacy-policy-biometrics-laws/ (last visited 7 July 2019].
[390] P. Tsai, *Data Snapshot: Biometrics in the Workplace Commonplace, but Are They Secure?*, 2018, Spiceworks, available at https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure (last visited 9 September 2019].
[391] G. A. Fowler, *Don't Smile for Surveillance: Why Airport Face Scans Are a Privacy Trap*, 2019, The Washington Post, available at https://www.washingtonpost.com/technology/2019/06/10/your-face-is-now-your-boarding-pass-thats-problem/ (last visited 13 December 2019].
[392] Liu, *supra* note 388.

карактеристики, анализа на геометриските пропорции на фацијалните карактеристики, мапирање на растојанието меѓу клучните карактеристики на лицето и текстурата. [393] За разлика од обичните CCTV камери, системите за препознавање на лицето можат да скенираат јасни карактеристики на лицето, според кои можат да се создадат детални биометриски карти на поединци без добивање на нивна согласност.[394].

Софтверот за препознавање на лице се користи на различни начини, но најчесто за цели на безбедност и за спроведување на законот. Честопати, камерите за надзор за препознавање на лице се мобилни. На пример, безбедносните органи во Малезија влегоа во партнерство со кинеската компанија за технологија Yitu, за да им обезбеди на офицерите софтвер за препознавање на лицето. Ова ќе им овозможи на безбедносните службеници да прават брзо споредување на сликите од обични камери со слики од централна база на податоци.[395] Аеродромите користат софтвер за препознавање на лице на неколку различни начини, како што се скенирање на лица на патници за да пребаруваат поединци осомничени за криминал или лица кои се на листата на набљудувани терористи, а исто така да ги споредувааат пасошките фотографии со слични лица за да го потврдат идентитетот. Спроведувачите на законот користат софтвер за препознавање на лицето за да ги идентификуваат и да ги уапсат луѓето кои вршат кривични дела. Неколку држави користат софтвер за препознавање на лицето за да ги спречат луѓето да добијат лажни лични карти или возачки дозволи. Некои странски влади дури користеа технологија за препознавање на лицето за да се борат против измама на гласачите.[396]

Меѓутоа, експертите детализираат неколку грижи поврзани со системите за препознавање на лицето. Најпрво, нема регулаторни механизми за регулирање на употребата на бази на податоци на слики (складишта што чуваат слики од камери за препознавање на лицето). Како ги користат владите овие информации, колку долго се чуваат и каде надлежните органи ги добиваат овие слики, може да се разликува според јурисдикцијата на одредени држави.[397] Второ, овие системи можат да се користат како

[393] Р. Мидрак, *Што е препознавање на лицето?*, 2019, EYewated, available at https://mk.eyewated.com/што е препознавање на лицето/ (last visited 15 December 2019].
[394] Feldstein, *supra* note 313, at p.18.
[395] Feldstein, 'The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression', *Journal of Democracy* (2019) , at p.40.
[396] Мидрак, *supra* note 393.
[397] Feldstein, *supra* note 313, at p.18.

механизми за надзор што може да има импликации врз приватноста на луѓето. Еден од примерите за овој масовен надзор е во Кина, која е опремена со најнапредната вештачка интелигенција во светот и софтвер за препознавање на лица. Кина веќе го вгради системот со повеќе од 170 милиони најсовремени камери за надзор. Само во септември минатата година Кина инсталираше повеќе од 20 милиони безбедносни камери во земјата. Целта на оваа најмодерна мрежа во светот е да идентификува кој било од вкупно 1,4 милијарди граѓани во рок од само 3 секунди.[398] Додека ИТ-професионалците сметаат дека технологијата е една од најсигурните форми на автентикација на располагање,[399] поединците се загрижени за нивната приватност, и биометриските податоци само го зголемуваат овој страв. Американската унија за граѓански слободи (ACLU)[400] смета дека ризикот е реален и сите ние треба да бидеме загрижени. Во еден блог во својата веб-страница, агенцијата пишува: „ФБИ во моментот собира податоци за нашите лица, ириси, обрасци на одење и гласови, дозволувајќи на владите секаде да нè идентификуваат, следат и набљудуваат. Поради тајноста на ФБИ, малку е познато за тоа како агенцијата ги плаќа своите активности за надзор со користење на технологија за препознавање на лице“.[401] Освен тоа, биометриските податоци можат да се злоупотребат од страна на поединци кои имаат лоши намери. Во еден граничен премин во Канада, федералните агенти изгубиле контрола над илјадници патнички фотографии. Хакерите украдоа фотографии на патници и нивни регистарски таблици.[402] Прекршувањето на овие податоци ги нагласува ризиците создадени со рутинско собирање на лични податоци на поединците и покажуваат како проширувањето на напорите за надзор можат да ја загрозат приватноста на поединците.

Граѓаните почнуваат да се борат против системите за препознавање на лице. На пример, демонстрантите во Хонк Конг ги покрија своите лица и го исклучија

[398] *Кина го гради најмоќниот систем за препознавање лице во светот*, 2019, Studenti.Mk, available at https://studenti.mk/kina go gradi najmokjniot sistem za prepoznavanje lice vo svetot/ (last visited 5 November 2019].
[399] Liu, *supra* note 388.
[400] За повеќе информации, посетете ја нивната веб-страница на www.aclu.org.
[401] K. Crockford, *The FBI Is Tracking Our Faces in Secret. We're Suing.*, 2019, ACLU, available at https://www.aclu.org/news/privacy-technology/the-fbi-is-tracking-our-faces-in-secret-were-suing/ (last visited 15 December 2019].
[402] T. B. Lee, *Feds Lose Control of Thousands of Traveler Photos in Data Breach*, 2019, ArsTechnica, available at https://arstechnica.com/tech-policy/2019/06/hackers-stole-thousands-of-border-crossing-photos-from-border-agency/ (last visited 15 December 2019].

препознавањето на лице на своите паметни телефони за да го спречат пристапот на органите на власта.[403]

Изгледа дека владите на некои држави го забележаа ризикот и се одлучија да го сменат нивниот пристап. Така на пример, во мај 2019 година, Сан Франциско стана првиот американски град кој го забранува користењето на технологијата за препознавање на лице од страна на локалните агенции и полиција, што е симболичен удар врз технологијата за надзор која се спроведува од страна на надлежни органи.[404] По примерот на Сан Франциско, повеќе градови велат не на користењето на системите за препознавање на лице.[405]

## 2.4 Беспилотни летала (дронови)

Дроновите претставуваат еден вид на надзор кој претставува голема загриженост за приватноста на луѓето. Дронот може да следи секого, во секој момент, и во овој контекст дроновите имаат негативно влијание врз приватноста на однесувањето на физичките лица. Потенцијалното користење на дронот за тајно снимање и надзор значи дека поединците треба да се обидат да имаат соодветно однесување во секој момент. За да се заштитат од негативните ефекти и упади, тие мора да претпостават дека се следат во секое време, па затоа мора да се обидат соодветно да го прилагодат своето однесување.

Употребата на дронови ја нарушува приватноста на податоците и сликите на една личност, бидејќи може да генерира слики на поединци, понекогаш и тајно. Ова значи дека принципите за заштита на личните податоци, како што се транспарентност, согласност и право на пристап можат да бидат повредени, бидејќи поединците честопати немаат идеја дека се предмет на надзор во секој даден момент. Една посебна група која може да биде

[403] P. Mozur, *In Hong Kong Protests, Faces Become Weapons*, 2019, New York Times, available at https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html (last visited 10 December 2019].
[404] D. Harwell, *San Francisco Becomes First City in U.S. to Ban Facial-Recognition Software*, 2019, The Washington Post, available at https://www.washingtonpost.com/technology/2019/05/14/san-francisco-becomes-first-city-us-ban-facial-recognition-software/ (last visited 10 December 2019].
[405] R. Metz, *Beyond San Francisco, More Cities Are Saying No to Facial Recognition*, 2019, CNN Business, available at https://edition.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html (last visited 10 December 2019].

непропорционално погодена од распоредувањето на беспилотните летала во цивилниот воздушен простор се познатите личности кои се постојано мета на папараци или медиуми.[406]

Употребата на беспилотните летала исто така ја нарушува приватноста на локацијата и просторот, бидејќи овие уреди можат да снимаат слики на една личност во возило на јавен простор, а со тоа може да се следи локацијата на луѓето во одреден временски период и да се откријат нивните движења низ јавниот простор. Покрај тоа, дроновите можат да откријат исто така информации за приватни простори, како што е дворот, а во некои случаи (кога дронот лета многу ниско), дури можат да пренесуваат слики од активности кои се случуваат во внатрешниот простор на домот на една личност. Така, за поединците кои претпоставуваат дека нивните активности не се следат бидејќи се случуваат во домот или во рамките на приватната сопственост, честопати се загрозува нивниот приватен живот, без нивно знаење. Фактот дека овој надзор може да биде таен, го прави собирањето на овие информации особено проблематично.[407]

## 3. Технологии за надзор и импликации за приватноста

Секој граѓанин/потрошувач остава електронски траги како цена на користење на електронски услуги. Овие траги овозможуваат сеопфатен надзор на нашите физички движења и комуникациско однесување. Овие траги овозможуваат изградба на многу софистицирани лични профили. Иако оправданоста за инсталирање на системи за надзор има силен јавен интерес, т.е., за сигурност и безбедност на општеството, надзорот предизвикува етички прашања, прашања за приватност и заштита на лични податоци. Сите технологии претежно имаат двојна употреба,[408] со тоа што можат да се користат за подобрување на социјалниот и економскиот развој, и истовремено можат да се користат за

[406] Finn, Wright and Friedewald, *supra* note 36, at p.16.
[407] *Ibid.*
[408] Терминот „двојна употреба“ ќе се користи во текот на овој труд со кој се опишуваат технологии што произлегоа од индустријата за решавање на комерцијални проблеми, но завршија со ненамерни безбедносни употреби или импликации.

злонамерни цели. Поради ова постои потреба да се дефинираат границите помеѓу приватната и јавната сфера.

Четири од најголемите проблеми за кои што се водат разговорите околу податоците и етичкиот аспект на механизмите за надзор се:[409]

- Приватност – граѓаните се соочуваат со широко распространети закани за нивната приватност. Додека огромни количини на податоци се собираат на паметни телефони, агенциите за спроведување на законот низ целиот свет користат технологија за препознавање на лицето. Продавниците сакаат да ги категоризираат купувачите со технологија за препознавање на лице, и да ги споредуваат информациите со нивните кредитни картички, често без согласност на клиентите.[410] Како што застапници за приватност напишаа во една изјава: „За минимум, луѓето треба да имаат можност да одат по јавни улици без страв дека компаниите за кои тие никогаш не слушнале, го следат секое нивно движење и ги идентификуваат истите по име.“[411]
- Недостаток на транспарентност – алгоритмите засновани на Вештачка интелигенција[412] честопати се чуваат во тајност или се толку сложени што дури и нивните творци не можат да објаснат точно како работат. Поради ова поединците и широката јавност имаат свои сомнежи во користењето на интелигентни системи и технологии. На пример, ако одлуката за вработување се донесува врз основа на податоците од овие сложени алгоритми, се поставува прашањето: Дали одлуките можат да се донесат според „тајни“ критериуми? Каква улога треба да има владата во обезбедувањето на транспарентност?
- Пристрасност и дискриминација – некои судски системи почнале да користат алгоритми за да го проценат потенцијалниот ризик на обвинетите за кривични дела,

[409] N. Dalmia and D. Schatsky, *The Rise of Data and AI Ethics Managing the Ethical Complexities of the Age of Big Data*, 2019, Deloitte Insights, available at https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2020/government-data-ai-ethics.html (last visited 11 August 2019].

[410] C. Farivar, *Retailers Want to Be Able to Scan Your Face without Your Permission*, 2015, ArsTechnica, available at https://arstechnica.com/information-technology/2015/06/retailers-want-to-be-able-to-scan-your-face-without-your-permission/ (last visited 18 July 2019].

[411] *supra* note 153.

[412] Вештачка интелигенција (ВИ) е интелигенција претставена од машини и софтвер и е гранка од компјутерската наука која развива машини и софтвер со интелигенција. Под поимот „интелигентен агент“ се подразбира систем способен за перцепирање на околината и преземање на активности без човечка интервенција.

па дури почнале да ги користат овие податоци за утврдување на казната. Во оваа смисла, клучниот фактор е основниот сет на податоци. На пример, ако овие податоци историски опфаќале одреден пол, раса или националност, тогаш резултатите би биле пристрасни против лицата надвор од тие групи.

- Недостаток на управување и одговорност – едно од клучните прашања во дебатата околу заштита на податоците и етичкиот аспект на користењето на механизмите за надзор е: Кој е одговорен кога се појавуваат неетички практики? Кој е надлежен орган што го овластува собирањето, чувањето и уништувањето на податоците?

## 4. Заштита на податоци во една неизвесна средина

Во оваа ера на дигитална револуција, и сè додека владите на одредени држави не донесат свои национални регулативи и додека нема еден меѓународен механизам за заштита на личните податоци, секогаш ќе има несигурност и неизвесност околу заштитата и меѓународниот проток на податоците. Меѓутоа, научниците сметаат дека без оглед на тоа што ќе донесе иднината, организациите треба да бидат подготвени за секоја ситуација, за да не се наруши нивниот бизнис. На пример, Bart Vandekerckhove смета дека организациите кои усвојуваат еден стратегиски пристап (третирајќи ги личните податоци како предност), ќе можат да одржат една конкурентна позиција во одредена индустрија. Во оваа смисла, тој предлага некои опции, како што се:[413]

- Компаниите треба да имаат информации за протокот на податоци. Тие треба да ги следат и да ги разбираат сите начини на кои податоците се пренесуваат од една држава на друга, вклучително и каде точно податоците завршуваат. Организациите исто така треба да следат кои податоци содржат лични информации и која технологија се користи за нивно пренесување.
- Компаниите треба да создадат договорни одбрани. Како прв чекор, клучно е да се знае кој ги прима податоците што течат меѓу земјите. Оттаму, организациите треба

[413] B. Vandekerckhove, *Protecting Data Flow in Shifting Privacy Regulations*, 2019, Security Boulevard, available at https://securityboulevard.com/2019/06/protecting-data-flow-in-shifting-privacy-regulations/ (last visited 14 December 2019].

да развијат договори со овие приматели во однос на размената на податоци што ќе ги задржат потенцијалните регулаторни промени. Ако податоците остануваат во една организација, но течат на глобално ниво, исто така треба да се испитаат корпоративните правила. Во овој контекст, организациите треба редовно да ги ажурираат корпоративните политики за приватност и заштита на лични податоци.

- Компаниите треба да постават внатрешни правила. Така на пример, ако податоците се споделуваат во рамките на самата организација, тогаш треба да се анализираат обврзувачките корпоративни правила за прекугранични проток на информации.

# 5. Заклучок

Може да се заклучи дека сегашните и новите технологии стануваат интегрирани, автоматизирани и се поприсутни системи за надзор, кои според научниците се нарекуваат паметен надзор. Додека современиот надзор вклучува различни технологии и се користи за различни цели, покрај националната безбедност, некои луѓе се загрижени за загуба на нивната лична автономија.

Овој надзор влезе во нашиот живот без најава и стана дел од нашите социо-политички односи. Нема сомнеж дека некои механизми за надзор носат социјални придобивки, но исто така нема сомнение дека оние што ги контролираат овие системи за надзор имаат голема моќ во своите раце. Поголемиот надзор неизбежно носи поголема бирократија и поголема институционална моќ. Тоа не е само проширување на државната моќ, туку исто така претставува проширување на корпоративната моќ, особено на некои големи корпорации како што се Google и Facebook, која истовремено носи зголемена закана за малициозни дејствија за поединците.

Гледајќи го начинот на кој технологиите за наблудување се користат, брзите чекори со кои се развиваат, и гледајќи во блиска иднина, може да се заклучи дека надзорот навистина станува се поприсутен во нашиот живот, не само преку Интернет, туку и во физичкиот свет. Способноста на системите за наблудување да нè следат што правиме, со кој седиме и каде одиме, во поголема мера ги нарушува бариерите помеѓу јавната и приватната сфера на нашиот живот.

# ГЛАВА ВТОРА: НОВА ТЕХНОЛОГИЈА, НОВИ ЗАКАНИ И ПРЕДИЗВИЦИ ЗА НОВО РЕГУЛИРАЊЕ

## 1. Нова технологија, стари правила

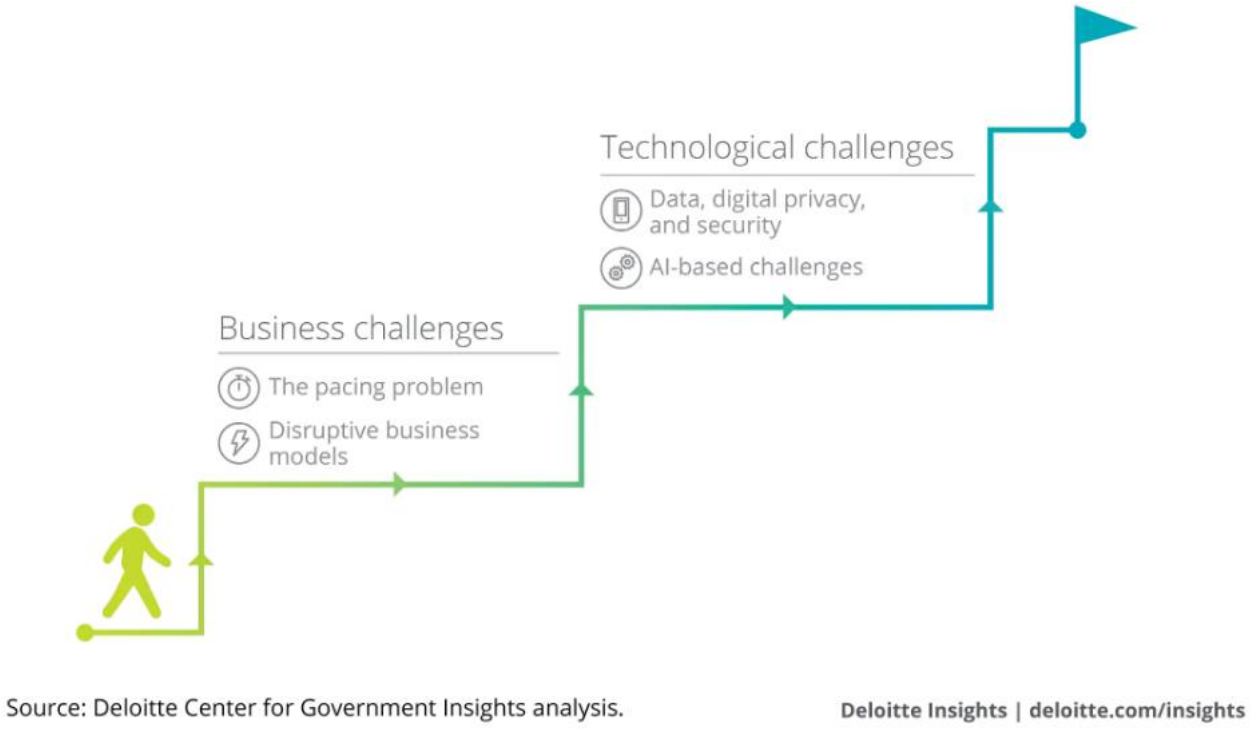
Технолошкиот развој се поттикнува од дигиталната револуција што започна пред повеќе од четири децении. Овие иновации се насочени кон собирање, обработка и анализирање на огромни количини на податоци кои имаат импликации во безброј области на истражување и развој. Овие достигнувања ветуваат значајни социјални и економски придобивки, зголемена ефикасност и зголемена продуктивност во повеќе сектори, но исто така постои загриженост дека овие технологии претставуваат нови можности за напаѓачите да се мешаат во приватниот живот на поединците, односно да ги злоупотребуваат нивните лични информации. Додека развојот на нови технологии продолжува со брзи чекори, за жал не може да се каже истото за една сеопфатна анализа на социјалните и етичките последици од таквата технологија. На меѓународно ниво, не само што недостасуваат комисии за приватност и информации, туку недостасуваат и национални агенции кои се занимаваат со влијанието на новите технологии. Па затоа, што треба да прават регулаторите?

За еден технолог, дронот е брилијантен производ кој овозможува подобра услуга за клиентите. За национална или лична безбедност, дронот претставува софтвер за таргетирање што носи безбројни закани. Регулаторите не можат едноставно да ја забранат технологијата, бидејќи комерцијалната корист е премногу голема. Можеби регулаторите едноставно не можат да го контролираат протокот на технологијата, затоа што таа е веќе надвор во дивината. Повеќе креатори, повеќе индустрии, повеќе намени, сето тоа значи дека секоја дадена технологија има потенцијал да допре многу регулатори. Ако пак го земаме дронот на пример; во САД овие летала можат да имаат потреба за регулаторни механизми почнувајќи од Федералната управа за авијација (FAA), бидејќи тие летаат низ воздушен простор, Министерство за транспорт, бидејќи тие летат по јавни патишта, Оддел за домашна безбедност па дури и од граничната контрола, ако тие ги

преминуваат границите и многу други. Предизвикот е што сите овие различни регулатори имаат различни перспективи и цели кои го утврдуваат пристапот на овие институции кон регулирање на технологијата.[414]

Сепак, регулаторите не можат да останат пасивни, со оглед на потенцијалната штета што може да ја нанесе развојот и примената на новите технологии за надзор. Бидејќи новите технологии водат кон нови услуги и деловни модели, владите мораат брзо да создаваат, модифицираат и спроведуваат соодветни регулативи. Главното прашање е: како да се заштитат граѓаните и националната безбедност на една држава, за да не се задуши иновацијата?

Истражувачите идентификуваат различни предизвици кои новите технологии ги претставуваат за традиционалните регулаторни модели и општо ги делат во две групи: деловни и техолошки (види слика 5).[415]




**Слика 5. Предизвици за традиционалното регулирање.**

[414] H. Ennis et al., *National Security and Technology Regulation: Government Regulations for Emerging Technology* (2019), available at https://www2.deloitte.com/us/en/insights/industry/public-sector/national-security-technology-regulation.html (last visited 12 September 2019], at p.5-8.

[415] W. D. Eggers, M. Turley and P. Kishnani, *The Future of Regulation: Principles for Regulating Emerging Technologies* (2018), available at https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html (last visited 5 November 2019], at p.3.

## 1.1 Деловни предизвици

- Проблемот на брзиот развој на технологијата – можат ли регулаторите да бидат во чекор со променливата технологија?[416] На пример, регулаторите на беспилотните летала се борат да останат во чекор со брзорастечката технологија.[417] Постоечките регулаторни структури честопати не се прилагодени на променливите општествени и економски околности, а регулаторните агенции генерално не сакаат да преземат големи ризици. Затоа, адаптацијата на нови технологии се соочи со значителни пречки.[418]
- Проблематични деловни модели – со постојана технолошка промена, различни деловни модели често ги надминуваат традиционалните граници во индустријата. Бидејќи производите и услугите се развиваат, тие можат да се префрлат од една регулаторна категорија во друга.[419]

## 1.2 Технолошки предизвици

- Податоци, дигитална приватност и безбедност – зголемената употреба на паметни телефони, поврзани уреди и сензори создадоа огромни дигитални траги во животот на потрошувачите. Од регулаторна перспектива, важно прашање е: кој ги поседува сите овие податоци, корисникот или давателот на услугата што ги чува? Ако давателот на услугата ги поседува информациите, каква обврска има да ги чува и заштити? И до кој степен може да ги споделува овие податоци со трети страни? На пример, дали може еден производител на автомобили да им бара поголема цена на сопствениците на автомобили кои одбиваат да ги споделат своите лични податоци, а помала цена на оние кои ќе прифатат да ги споделат нивните

[416] G. Stern, *Can Regulators Keep Up with Fintech?*, 2017, available at https://insights.som.yale.edu/insights/can-regulators-keep-up-with-fintech (last visited 7 September 2019].
[417] A. Pasztor and R. Wall, *Drone Regulators Struggle to Keep Up With the Rapidly Growing Technology*, 2016, Wall Street Journal, available at https://www.wsj.com/articles/drone-regulators-struggle-to-keep-up-with-the-rapidly-growing-technology-1468202371 (last visited 5 November 2019].
[418] Eggers, Turley and Kishnani, *supra* note 415.
[419] *Ibid.*

информации?[420] Без еден глобален договор или законска рамка за заштита на податоци, регулаторите низ целиот свет земаат различни позиции за овие проблеми, без разлика на тоа што протокот на лични податоци и користењето на електронските услуги нема граници, поради тоа што Интернетот е глобална платформа. 21 проценти од државите немаат закони за заштита на податоците.[421] Оние што имаат, честопати имаат спротивставени закони.[422] Тоа се случува и помеѓу Европската Унија и Соединетите Американски Држави.[423] Така на пример, Општата регулатива за заштита на лични податоци (GDPR)[424] на Европската Унија обезбедува строги контроли за прекуграничниот пренос на податоци и на граѓаните им дава право „да бидат заборавени“. Според една анкета, 82 проценти од Европејците велат дека планираат да ги користат своите нови права, односно да ги ограничат или бришат своите податоци.[425] Спротивно на тоа, Соединетите Американски Држави се одлучија за поинаков пристап кон заштитата на податоците. Наместо формулирање на сеопфатна регулатива, како што е GDPR во Европската Унија, тие спроведуваат закони и регулативи за специфични сектори и се фокусираат на државни закони.[426]

[420] *Ibid.*

[421] *United Nations Conference on Trade and Development 'Data Protection and Privacy Legislation Worldwide'*, available at https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (last visited 7 November 2019].

[422] На пример, некои закони ги исклучуваат малите бизниси (на пример, Австралија и Канада). Други вообичаени исклучоци се однесуваат на: 1) видови на субјекти на податоци (на пример, само за деца, а не на вработени); 2) чувствителност на податоци (на пример само на чувствителни податоци како што се медицински или финансиски записи); 3) извори на податоци (на пример, се ограничуваат на податоци собрани само од Интернет или податоци собрани офлајн); 4) податоци од одреден сектор (на пример, исклучоци поврзани со приватниот и јавниот сектор или закони кои се ограничени за специфични сектори, како што е здравство). За повеќе информации, види: *United Nations Conference on Trade and Development, "Data Protection Regulations and International Data Flows: Implications for Trade and Development"*, 2016, available at https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf (last visited 10 December 2019].

[423] A. Coos, *EU vs US: How Do Their Data Privacy Regulations Square Off?*, 2018, Endpoint Protector, available at https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/ (last visited 7 December 2019].

[424] *supra* note 4.

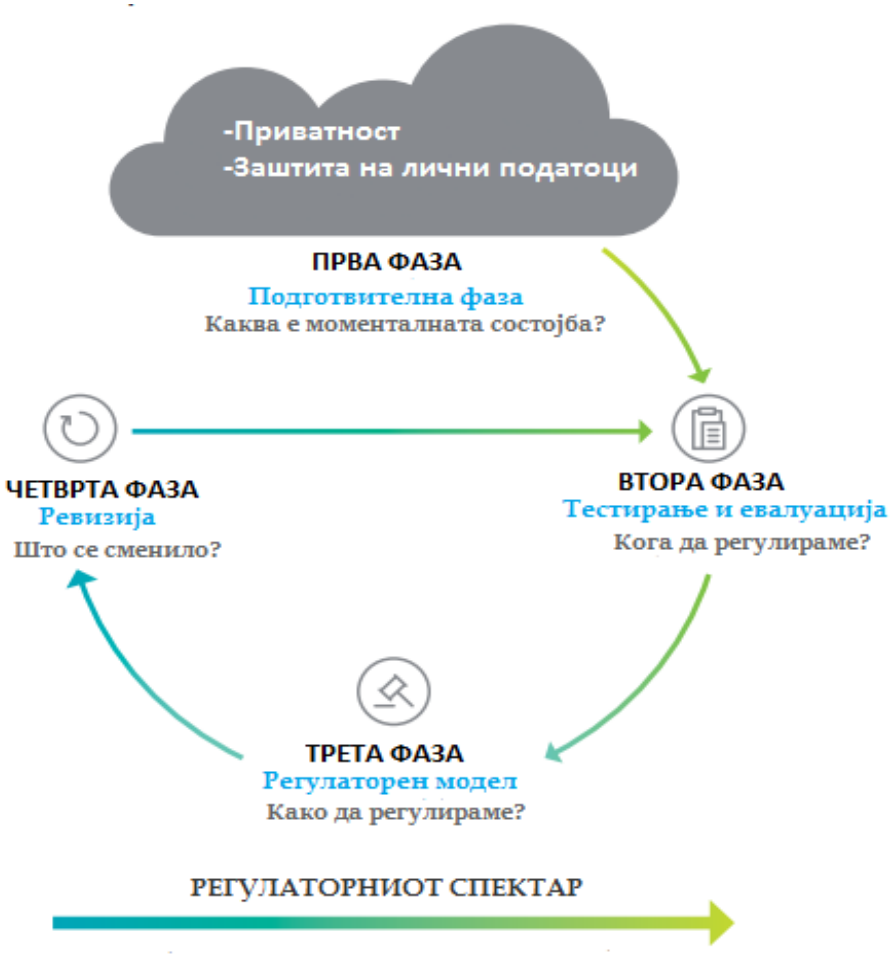
[425] *GDPR: Show Me the Data*, 2017, Pega, available at https://www.pega.com/gdpr-survey (last visited 7 December 2019].

[426] Coos, *supra* note 423.

## 2. Четири основни прашања за нов регулаторен пристап

Додека креаторите на политики и закони се справат со регулаторни предизвици што ги поставуваат дигиталните технологии, истражувачите сметаат дека четири основни прашања се клучни за решавање (види слика 6):[427]

- Каква е моменталната состојба на регулирање во областа?
- Кога е вистинското време за регулирање?
- Кој е вистинскиот пристап кон регулативата?
- Што се сменило откако беа донесени регулативите?




**Слика 6. Четири основни прашања.**

Извор: Deloitte insigths | deloitte.com/insights

1. Каква е моменталната состојба на регулирање во областа?

[427] Eggers, Turley and Kishnani, *supra* note 415.

Првиот чекор во подготвителната фаза треба да вклучува детален преглед и разбирање на релевантните постоечки регулативи, во потрага по оние што можат да ја блокираат иновацијата, се застарени или се дупликати. Според моменталната состојба, регулаторите треба да се повикуваат на целиот екосистем на регулација што може да се примени: од вертикална услуга или секторско регулирање (на пример, за моторни возила); кон конвергентна регулатива каде се вклучуваат повеќе сектори.[428] Честопати ваквиот преглед не е направен многу години. Според една анализа од 2017 година, се утврдува дека многу федерални регулативи во САД никогаш не биле ажурирани.[429] Ретроспективниот преглед ги принудува регулаторите да проценат дали алтернативите за регулирање или прилагодување на тековните правила можат соодветно да го решат одредениот проблем.[430]

2. Кога е вистинското време за регулирање?

   Традиционално, регулаторите конципираат нови правила и закони како одговор на развојот на пазарот или новото законодавство. Следно, тие поминуваат месеци или години изготвувајќи правила кои му се презентираат на општеството за јавно коментирање. Конечно, регулаторите ги прегледуваат овие коментари (може да има десет илјади, па дури и милиони од нив) и соодветно го променуваат предложениот нацрт (драфт).[431] Проблемот со овој процес е тоа што регулаторите често не знаат како бизнисите и потрошувачите ќе реагираат на новите закони и, другиот проблем е тоа што откако се донесува еден закон и влегува во сила, ретко истиот се разгледува.[432] За да се реши овој проблем, истражувачите сугерираат да се премине од „регулирај и заборави“ кон еден прилагодлив и одговорен пристап,[433] на пример преку механизми за меки закони, кои не се директно спроведливи.[434]

[428] *Ibid.*, at p.9.
[429] D. Byler, B. Flores and J. Lewris, *Using Advanced Analytics to Drive Regulatory Reform: Understanding Presidential Orders on Regulation Reform* (2017), at p.4.
[430] M. C. Peacock, S. E. Miller and D. R. Pérez, *A Proposed Framework for Evidence-Based Regulation* (2018), at pp.3-26.
[431] Eggers, Turley and Kishnani, *supra* note 415, at p.11.
[432] C. Brummer and D. Gorfine, *Fintech: Building a 21st Century Regulator's Toolkit* (2014), at pp.1-14.
[433] Eggers, Turley and Kishnani, *supra* note 415, at p.11.
[434] Merchant and Allenbey, 'Soft Law: New Tools for Governing Emerging Technologies', *Bulletin of the Atomic Scientists* (2017), at pp.108-114.

3. Кој е вистинскиот пристап кон регулативата?

   Креаторите на политики и закони имаат различни причини за донесување на одредени закони, но генерално, тие се обидуваат да ги заштитат граѓаните и да ја промовираат иновацијата. Која од овие причини е најважна во дадена ситуација ќе влијае како да одговориме на следново прашање: Кој е најдобриот регулаторен модел што треба да се користи? Во однос на тоа, постои широк спектар на потенцијални пристапи. На пример, регулаторите можат да се одлучат за строги закони, vice verca, или воопшто да не донесат никаква регулатива.[435]

4. Што се сменило откако беа донесени регулативите?

   Со оглед на брзиот развој на технологијата и новите бизнис модели, за да останат соодветни и релевантни, законите кои се применуваат во денешно време најверојатно ќе треба да бидат ревидирани во текот на следната деценија.

## 3. Нови законски правила: иднина на регулативата

Како што се гледа од претходната анализа, не е лесна работа да се регулираат новите технологии во информатичкото општество, а во исто време да се зачуваат интересите на граѓаните од една страна, и напредокот на иновацијата од друга страна. За да не се спречи економскиот раст, треба да биде отворена размената на идеи помеѓу индустријата, академиците и независните истражувачи.

Додека тековните процеси обично не дозволуваат флексибилност за оптимално управување со новите технологии, академиците сметаат дека со нови регулаторни правила може да се надминат овие предизвици и ефикасно да се контролираат потенцијалните закани од новите технологии, без да се наруши иновацијата. Според Ennis et al., на пример, владата треба да работи со информирани регулатори и производители на технологија и истовремено треба да размисли за изнаоѓање на нови начини за регулирање

[435] Eggers, Turley and Kishnani, *supra* note 415, at p.9.

на технологијата. Овие нови алатки и начини на регулирање ги сумираат како „иднина на регулативата“.[436]

Иднината на регулативата нуди нови алатки и пристапи кои можат да помогнат во решавањето на секој од предизвиците што се создаваат од новите технологии кои се користат за комерцијални цели (види слика 7).[437]


[436] Ennis et al., *supra* note 414, at p.10.
[437] *Ibid.*, at p.11.


**Слика 7. Иднина на регулатива нуди нови пристапи за решавање на предизвиците кои се предизвикуваат од нови технологии**.

Извор: Deloitte insigths | deloitte.com/insights

## 4. Движење напред

За да се одредат соодветни принципи и регулаторни механизми за заштита на личните податоци од заканите на технологијата, креаторите на политиките за приватност и заштита на лични податоци треба да имаат повеќе од едно заедничко разбирање за тоа како се развива технологијата, како се дизајнира и како може да се користи; тие треба да ги познаваат принципите што ги применуваат различни заедници низ целиот свет, како и очекувањата на општеството и деловните институции. Во овој контекст, треба да се надмине артикулацијата на принципи за заштита на лични податоци и да има практична примена на законски правила, како и признавање на одредени предизвици и ограничувања.

Одговарањето на ризиците и предизвиците не може да се достигне само со истражување на нови структури, алатки и процеси за управување. Оваа задача бара длабоко разбирање на социјални, културни, економски и геополитички фактори, бидејќи само тогаш може да се разберат конфликтните прашања меѓу човештвото и технологијата. Поради ова, научниците идентификуваат некои предизвици, кои владите и креаторите на политики треба да ги адресираат. Kavanagh истакнува некои од нив, како што се:[438]

[438] C. Kavanagh, *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?* (2019), at p.3-5.

- Идентификување на клучните принципи и вредности – релевантните актери мора да ги применуваат принципите за заштита на лични податоци како што се: правичност, еднаквост, одговорност, транспарентност, и др., кои можат да имаат негативно влијание од користењето на одредени технологии. Оваа задача бара ново размислување за тоа како да се осигуриме дека одредени технологии (на пример, биотехнологија) нема да ги влошуваат постоечките социо-економски нееднаквости, и бара размислување како најдобро да се одговори на нови напади на личната приватност. Во овој контекст, Kavanagh смета дека одредени форми на истражување (на пример некои аспекти на биолошки инженеринг) можеби треба да се ограничат.
- Ефикасно ангажирање на засегнати страни – законодавци, регулатори, лидери на приватни бизниси, истражувачи и граѓани треба да бидат подготвени да одговорат ефективно и со одговорност на последиците на технолошкиот развој и потенцијалните ризици што тие ги претставуваат. Додека тековните експерименти за применување на нови правила за конкретни прашања се многу значителни, голем предизвик претставува примената на овие одговори за прекугранични протоци на податоци, што може да претставуваат социо-економски и безбедносни предизвици. Оваа задача бара примена на различни пристапи, поголема инвестиција за независно јавно истражување и вклучување на многу актери освен држави. Од витално значење преостанува утврдувањето на тоа кои прашања поврзани со технологијата треба да се гледаат од национална призма, односно да се решат дома, и кои проблеми бараат прекугранична соработка и координација.
- Проширување на постоечките платформи за мултилатерална соработка - треба да се појасни како различни актери (и не само држави) можат да го дадат својот придонес за зацврстување на националните норми и меѓународно право за заштита на приватност и лични податоци. Така на пример, различни групи на Обединетите Нации, како и други експерти или специјализирани работни групи кои се занимаваат со технологија (вклучително ИКТ, машинско учење, автономни интелигентни системи, биотехника и сл.) треба да го дадат својот напор за меѓународна безбедност.

- Соодветни регулативи – потребни се свежи пристапи кон политиката и регулативата за приватност. Развојот на технологијата веќе има предизвикано различни дискусии и фокусот се става на соодветен вид на регулатива. Има многу прашања околу тоа дали креаторите на политики треба да се одлучат за строги закони, меки иницијативи (на пример, упатства) кои не претставуваат обврзувачки одредби, или мерки за самоуправа од страна на приватни институции. Како што е наведено погоре, клучно прашање е: како ќе се осигурат законодавците дека одреденото регулаторно решение е соодветно за целите за кои се донесува?; и дали овие актери треба да имаат меѓународен пристап? Со оглед на меѓународниот проток на информациите, некоординирани национални правила најверојатно нема да бидат ефективни за одговарање на конкретните прашања.
- Зајакнување на транспарентност, надзор и одговорност – нови пристапи за регулаторни политики бараат поголема инвестиција во механизмите за транспарентност, надзор и одговорност. Според ова, треба да се утврди природата на националните тела за надзор, дали тие треба да бидат јавни или приватни. Ова исто така значи дека компаниите и организациите треба да прифатат поголема контрола. На пример, технолошките компании треба да го зголемат внатрешниот надзор и екстерното известување за нивните иницијативи за внатрешни правила, треба да обезбедат пристап до нивните податоци за јавно финансирани истражувачи, и пред сè, треба да бидат одговорни во сите етапи на синџирот на снабдување.[439]

[439] За повеќе информации за принципот на одговорност, види: Floridi and Cowls, 'A Unified Framework of Five Principles for AI in Society', *Harvard Data Science Review* (2019).

# ГЛАВА ТРЕТА: ПРОФИЛИРАЊЕ, ПОСТОЈАН ПРОБЛЕМ ЗА ЗАШТИТА НА ПОДАТОЦИТЕ И ПРИВАТНОСТА

## 1. Што претставува профилирањето?

Општо, профилирањето подразбира снимање и анализа на психолошките карактеристики и однесувањето на една личност или група на физички лица, со цел да се проценат или предвидат нивните способности во одредена сфера.

Профилирање е каква било форма на автоматска обработка на лични податоци кои ги вреднуваат личните аспекти поврзани со физичко лице, особено за анализирање или предвидување на аспекти во врска со изведбата на работата на субјектот на податоците, економската состојба, здравјето, личните преференци или интереси, сигурност или однесување, локација или движења, каде што создава правни последици во врска со субјектот на податоците.[440]

Автоматското профилирање вклучува:[441]

- Снимање на податоци;
- Чување на податоци (на начин што ги прави податоците достапни);
- Следење на податоци (снимање и складирање за одреден временски период, поврзувајќи ги податоците со истите субјекти на податоци);
- Идентификување на обрасците во податоците (со алгоритми преку базата на податоци);
- Мониторинг на податоци (проверка дали новите податоци се вклопуваат во шемата или произведуваат надворешни информации).

Профилирањето може да се однесува на една личност или на една група личности и односите меѓу нив. Може да се користи за опишување и анализирање на одредени ситуации, на пример да покажува што се случило во одредена ситуација. Ова не претставува нешто ново и проблематично. Овој вид на собирање и обработување на

[440] Тошкова, *supra* note 22, at p.55.
[441] За повеќе информации на автоматското профилирање види:Hildebrandt, *supra* note 368.

податоци се нарекува пребарување. Во тој случај, профилирањето дозволува структурирање на она што веќе е познато. Од друга страна, профилирањето може да се користи за приклучување на податоците на таков начин кој дозволува предвидување на однесувањето и желбите на одредени лица. Ваквата активност создава посебен вид на знаење, познато како откривање на знаење во бази на податоци.[442]

Профилите не претставуваат тековна состојба на одредена ситуација, туку тие се создаваат како резултат на обработка на лични податоци. Во оваа смисла, тие не ја опишуваат реалноста, туку се откриваат како резултат на анализа на податоци во одредени софтвери. Во апстрактно ниво, преку извлекување (екстракт) на употребливи податоци од базата на податоци, профилирањето доведува до идентификување на претходните однесувања на поединците во минатото, кои можат да се развијат во веројатни сознанија за поединците во сегашноста и иднината. На некој начин, нашиот поглед за сегашноста се обликува од тоа што пронаоѓањето во базата на податоци го нагласува. Поради тоа се смета дека профилирањето е продуктивен вид на знаење: има тенденција да ја создаде „реалноста" според она што се случило во минатото.[443]

Практиките за профилирање во дигиталната ера имаат многу форми. Тие создаваат загриженост за општеството, кое честопати се прикажува преку медиумите, а од таму прашањата стигнуваат до релевантните регулатори. Овие ентитети се во постојана борба за наоѓање на соодветна регулаторна реакција за комплицираните прашања претставени пред нив. Профилирањето претставува голем предизвик не само за општеството, туку и за политиката. Меѓутоа, штетата што ја предизвикува и начинот на кој истата треба да се реши, останува тешко да се конципираат.

Предизвиците на регулаторите и научниците кои се справуваат со овие проблеми може да се опишат на следниов начин:[444]

(а) Тие мора да генерираат една корисна таксономија за разбирање и решавање на потенцијалните проблеми;

[442] Gutwirth and Hildebrandt, 'Some Caveats on Profiling', in S. Gutwirth, Y. Poullet and P. de Hert (eds.), *Data Protection in a Profiled World* (2010) , at p.32.
[443] *Ibid.*
[444] Zarsky, 'Responding to the Inevitable Outcomes of Profiling: Recent Lessons from Consumer Financial Markets, and Beyond', in S. Gutwirth, Y. Poullet and P. De Hert (eds.), *Data Protection in a Profiled World* (2010) , at p.53.

(б) Тие мора да утврдат кои прашања би можеле да се решат со внатрешни механизми, и за кои прашања е потребна директна регулаторна контрола и интервенција; и

(ц) Конечно, и што е најважно, тие мора да формулираат или да препорачуваат регулаторни одговори за посебни прашања за кои сметаат дека се неопходни.

За подобро разбирање на профилирањето, штетата која ја нанесува и начинот за решавање, треба да се анализира информацијата која ќе се добие од профилирањето, односно употребите кои произлегуваат од обработката на личните податоци во базите на податоци. За да се постигне тоа, мора прво да го разбереме протокот на личните податоци.

## 2. Присуство на Интернет и споделување на информации

Се што ние споделуваме на Интернет, останува таму засекогаш. Информатичката технологија ги чува дигиталните траги трајно. Разговорите меѓу луѓето во реалниот живот се различни од тие во виртуелниот живот. На пример, ако јас кажувам нешто и слушателот не го запишува тоа што јас го кажувам, информацијата се губи, засекогаш. Ако полицијата нема алатки за прислушување на вашиот телефон денес, тие не можат да го вратат времето и да го снимат разговорот ако се сомневаат следниот месец за она што се случило денеска. Меѓутоа, не може да се каже истото за електронските преноси и комуникации, кои генерално се чуваат од давателите на услуги на Интернет, се архивираат од машини за пребарување и се документираат во колачиња *by default.*[445] Со други зборови, нашето присуство на Интернет кажува многу за нашиот живот и нашата личност.

Активностите на Интернет можат да се категоризираат под три широки наслови: комерцијални, информативни и комуникативни (социјални).[446]

[445] Tufekci, 'Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites', *Bulletin of Science, Technology & Society* (2008) , at p.20-21.
[446] Weiser, 'The Functions of Internet Use and Their Social and Psychological Consequences', *CyberPsychology & Behavior* (2001) , at pp.723-743.

Во анализата на динамиката на приватност, овие различни активности не треба да се третираат како недиференцирана група на слично однесување. Првите два вида на активности главно одговараат на инструментална употреба (на пример купување на билети за патување или гледање на времето). Од друга страна, социјалните активности се однесуваат на едно мрежно комуницирање. Луѓето комуницираат со своите социјални контакти преку повеќе механизми, како што се пораки, е-пошта и сл. Освен тоа, луѓето создаваат профили на само-презентирање, како што се лични веб-страници или профили на социјални мрежи. Сите овие виртуелни врски помеѓу поединците служат како канали за споделување на информаци. Според информациите кои поединците ги стават на Интернет, на пример, во своите профили на социјални мрежи, може да се даде една сеопфатна слика за тоа кои сме ние и кого го познаваме. Ова може да се илустрира според примерите кои ги дава Grimmelmann:[447]

- Објавите на sидот на социјалните медиуми можат да содржат информации за објавувачот (на пример еден контакт - пријател кој објавува на мојот sид, спомнува едно патување во Хрватска). Овие објави исто така можат да содржат информации за поединецот, на чиј sид се пишува или за обајцата (некој трет спомнува еден курс на кој ние бевме заедно на училиште).
- Ако јас те „боцнам" (poke) на Facebook, тоа значи дека јас сум на Интернет и размислувам за тебе.
- Изборот на еден e-mail над друг има значење дека другата личност разбира и претставува персонализирана порака.
- Ако јас објавам и означам една фотографија од тебе, тоа документира како ти изгледаш, каде и со кого си бил. Исто така документира дека јас те познавам тебе и некој може да заклучи дека јас бев фотографот.
- Секоја игра што ја играме онлајн дава одредени информации за нашата личност.
- Еден список на причини им кажува на другите кои принципи ти значат тебе.
- Одговарањето на различни квизови може да открие многу информации за знаењето, верувањата и преференците на една личност.

[447] Grimmelmann, *supra* note 343, at p.1150.

Во овој контекст, информациите пулсираат помеѓу масивни бази на податоци. Овие информации можат да бидат од голем интерес за трговски цели на различни компании, а понекогаш и на владата, која ги собира и анализира овие податоци.[448] Оваа индивидуална колекција на лични информации е конципирана како „дигитално досие", дефинирано како збирка на детални податоци за еден поединец, односно колекција на нашите дигитални траги на Интернет.[449]

## 2.1 Проблеми на дигиталните досиеја

Компјутерите и сајбер просторот значително ја зголемија нашата способност да собираме, чуваме и анализираме различни информации. Во денешно време, безброј компании одржуваат компјутеризирана евиденција за преференците, купувањата и активностите на нивните клиенти. Постојат голем број на записи со детали за потрошувачката моќ на еден поединец. Компаниите за кредитни картички одржуваат информации за купување со кредитни картички. Видео продавниците водат евиденција за нечие изнајмување на видеа. Онлајн платформи за купување, како што е Amazon.com, задржуваат записи од сите книги и други производи што некој ги купува. Има и стотици други компании за кои луѓето не се свесни, а кои исто така ги прибираат личните податоци на поединците.[450]

Сите информации кои се собираат од страна на давателите на електронските услуги се анализираат за да го предвидат однесувањето на потрошувачот. Преку разни аналитички техники, пазарот развива модели кои се однесуваат на желбите на поединците, за тоа какви производи ќе посакаат конкретни клиенти и како да ги натераат потрошувачите да консумираат одредени производи. Компаниите знаат како ние ги трошиме нашите пари, каква работа имаме, колку заработуваме, каде живееме, итн. Тие знаат за нашето етничко потекло, религија, политички погледи, здравствени проблеми, и слично. Според овие информации компаниите ги предвидуваат нашите желби. На пример,

[448] Tufekci, *supra* note 445, at p.21.
[449] D. J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (2004), New York University Press, at p.1-2.
[450] *Ibid.*, at p.3.

според нашето претходно однесување, тие знаат какви книги ќе купиме наскоро или какви видови филмови би сакале да гледаме.[451]

Овие информации можат да се користат од оние кои донесуваат важни одлуки за животот и кариерата на поединецот (на пример според овие информации една институција може да одлучи дали да му даде работа на одредено лице). Во многу случаи, поединецот нема да знае дека одлуката е базирана на вакви информации.

## 3. Краток вовед за протокот на лични информации

За поедноставно разбирање, профилирањето ќе се анализира преку три повторувачки процеси, во кои се вклучува фазата на собирање, анализирање и користење на личните податоци.

Според тоа собирање на лични податоци, во контекст на профилирањето, подразбира собирање на лични податоци од еден релевантен индивидуелен профил, кои се чуваат (се складираат) во база на податоци. Собирањето може да се направи од страна на контролорите директно од субјектите на податоците, со или без нивна согласност, или собирањето може да се направи преку трети страни.

Директното собирање на податоци се однесува на самооткриените информации од страна на физичките лица  т.е. информации за поединци откриени од самите нив.

За жал, општата јавност не ги разбира долготрајните последици  од таквите активности. Тоа може да доведе до сериозно загрозување на приватноста и угледот на едно лице, како резултат на информациите што се вртат надвор од контролата на нивните сопственици. Една стара латинска поговорка нагласува *verba volant scripta manent* што значи дека изговорените зборови летаат додека пишуваните зборови остануваат.[452] Слично на тоа, дигиталните информации лесно се копираат и репродуцираат. Сепак, корисниците на Интернетот продолжуваат да споделуваат приватни информации за нивниот живот,

[451] *Ibid.*, at p.4.
[452] Martin and del Alamo, 'Forget About Being Forgotten From the Right to Oblivion to the Right of Reply', in S. Gutwirth, R. Leenes and P. De Hert (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (2016) , at p.252.

верска или сексуална ориентација, политички коментари и мислења за секакви ситуации, верувајќи дека тие ќе останат приватни засекогаш.

Собирањето преку трети лица се однесува на информациите на едно лице кои се откриваат или се споделуваат од страна на трети лица. Најпознатиот пример на такво откривање на податоци претставува означување (tagging) на социјалните мрежи, како на пример на Facebook, каде едно лице може да идентификува (означи) други лица во својата фотографија или пост. Друг релевантен пример е карактеристиката „споменување на корисникот" што им овозможува на корисниците на Интернет да објават одреден текст и истиот да го поврзат со други лица, споменувајќи ги нивните имиња преку означување на нивните специфични ознаки (на пример, "@корисничко име").

Што се однесува до приватноста на субјектот на податоците, најтешка ситуација претставува случајот кога личните податоци се собираат директно од субјектот на податоците. Во овој случај, субјектот на податоците признал, односно дал согласност за собирање на неговите податоци, меѓутоа прашањето дали тој знаел за што се собрани податоците и за какви цели ќе се користат, останува проблематично и тешко за означување во правната наука и судската пракса.[453]

Собирањето проследува со анализа на податоците. Во оваа фаза, анализата се прави во база на податоци која вклучува профили на многу лица, во потрага по релевантни информации и знаења кои би биле корисни за одредени фирми и организации. Ова се реализира преку употреба на технологија за податочно рударство (англиси data mining), софтвери кои применуваат софистицирани алгоритми за откривање на скриени обрасци во податоците.[454]

Податочното рударство се реализира преку користење на статистички податоци, принципи за машинско учење (ML), вештачка интелигенција (AI) и огромни количини на податоци (често од бази на податоци). Податочното рударство има две основни цели: опис и предвидување. Прво, се опишуваат увидите и знаењата добиени од анализата на обрасците во податоците, второ, овие описи и препознатливи модели се користат за предвидување на идни модели.[455] Во многу случаи, анализата укажува на потенцијални

[453] Zarsky, *supra* note 444, at p.56.
[454] *Ibid.*
[455] Р. Л. Мидрак, *Што е Data Mining?*, EYewated, available at https://mk.eyewated.com/што-е-data-mining/ (last visited 15 December 2019].

придобивки кои не биле очигледни во моментот на собирањето. Со други зборови, во базата на податоци се генерираат нови знаења. Еве еден пример како тоа функционира во пракса: Ако сте поминале одредено време на Интернет за купување на книги за одредена тема, услугите за рударство кои работат зад сцената на таа веб-страница најавуваат опис на вашите пребарувања во врска со вашиот профил. Кога повторно се пријавувате две недели подоцна, службите за рударство на веб-сајтот ги користат описите на вашите претходни пребарувања за да ги предвидат вашите тековни интереси и да понудат персонализирани препораки за купување кои вклучуваат книги со исти теми за кои претходно сте пребарувале.[456]

Конечно, горенаведените две фази водат кон вистинската употреба на податоците, односно третата фаза која се однесува на добиените знаења од анализата на податоците – процес што може да доведе до различни придобивки за одредени странки. Сепак, овие придобивки се поврзани со голем број опасности за личните податоци и загрозување на приватноста на едно лице. Грешките кои можат да се појават во базата на податоци или во целокупниот процес на обработување на личните податоци можат да доведат до неправеден третман за субјектот на личните податоци. Како прво, информациите кои произлегуваат од анализата на податоците можат да бидат приватни, и како такви би можеле да доведат до загрозување на приватниот живот, желби и приватни активности на едно лице. Како второ, може да дојде до потенцијална злоупотреба на овие информации, па дури да се уцени субјектот на податоците. Најчесто, сите овие информации се користат од страна на одредени фирми и организации, за да можат да ги предвидат однесувањата на нивните консуматори. Во овој контекст, се појавува една голема нерамнотежа меѓу странките инволвирани во овој процес – фирмите „ги познаваат“ своите потрошувачи подобро отколку што тие се знаат себеси. На тој начин, информациите можат да се користат за дискриминација на таргет групи, додека се потпираат на различни фактори и стратегии – индикации за нивната куповна моќ, информации за нивните трошоци итн. Конечно, таквото знаење им овозможува на фирмите (особено во областа на маркетинг и рекламирање) да ги користат информациите за желбите на нивните таргет потрошувачи за неправедно манипулирање со нив. Според овие информации фирмите комуницираат со нивната таргет група (најчесто преку реклама), ја анализираат реакцијата на поединците и

[456] *Ibid.*

соодветно на тоа ја менуваат нивната идна употреба на податоци.[457] Сите овие проблеми бараат регулаторно дејствување.

## 4. Следење на однесување (профилирање на однесување)

Концептот на профилирање на однесување, исто така познат како „таргетирање“ се состои од собирање и анализирање на неколку настани, сите поврзани со една личност или еден ентитет, со цел да се добијат информации за наведениот субјект. Со други зборови, овој процес претставува трансформирање на податоци во знаење или информации.[458] Според Hildebrandt, профилирањето не се однесува на податоци, туку на знаење. Профилирањето, според неа, е друг термин за софистицирана шема за идентификување и овозможување на амбиентална интелигенција. Тоа нè соочува со нов вид на индуктивно знаење, изведено со помош на автоматски алгоритми.[459]

Профилирање на однесување вклучува собирање на податоци (снимање, чување и следење) и нивно пребарување за идентификување на обрасци (со помош на алгоритми за податочно рударство). Фазата на прибирање на податоци честопати се нарекува следење на однесување.[460] Еден пример за таргетирање или профилирање на однесување се дава од страна на Dwyer, како што е прикажано според Castelluccia. Таа зборува за сценариото каде еден клиент бара онлајн билет за New York. Тој бара летови, меѓутоа не прави никакво купување. Последователно, тој посетува една веб-страница која прикажува реклами, односно понуда на билети за New York. Според ова, иако нема собирање на информации за иденфикување, неговиот интерес за билети е веднаш забележан.[461] Освен ова, има безброј други примери кога луѓето се прашуваат како на пример Facebook или Instagram секогаш знае за што се тие заинтересирани и според тоа прикажуваат реклами во нивните newsfeed. Таквите платформи користат информации зачувани во вашите

[457] Zarsky, *supra* note 444, at p.56-57.
[458] Hildebrandt, *supra* note 368.
[459] *Ibid.*
[460] Castelluccia, 'Behavioural Tracking on the Internet: A Technical Perspective', in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?* (2012) , at p.21.
[461] *Ibid.*

активности зачувани во вашиот прелистувач[462] кој ги следи вашите активности, како што се колачиња, заедно со сопственото знаење за вашата претходна употреба на услугата на Facebook или Instagram за да ги предвидите производите или понудите за кои можеби сте заинтересирани.[463]

## 5. Мотивации: Зошто нè следат и профилираат?

Профилите се многу важни за многу компании во прилагодувањето на нивните услуги да одговараат за нивните клиенти, со цел да ги зголемат приходите. Јасна намера на таргетирање на однесувањето на поединците е да се следат корисниците во текот на времето и да се изградат профили на нивните интереси, карактеристики (како што е пол, возраст, етничка припадност, и др.), и трговски активности. На пример, компаниите користат таргетирање на однесувањето за да прикажуваат реклами кои тесно ги одразуваат интересите на корисниците или нивните потенцијални клиенти.[464]

Системот на онлајн рекламирање најчесто се состои од три главни субјекти : огласувачот, издавачот и мрежата на рекламирање. Огласот е еден ентитет, на пример производителот на автомобили или еден хотел, кој сака да рекламира производ или услуга. Издавачот е субјектот, како што е една компанија, која поседува една или повеќе веб-страници и прикажува реклами за свои финансиски цели. Конечно, мрежата на рекламирање е субјект кој собира реклами од огласувачите и ги става на страниците на издавачите. Ако корисникот кликнува на оглас, мрежата на рекламирање собира финансиски средства од соодветниот огласувач. Поради тоа има силен поттик за мрежата на рекламирање да генерира многу точни и целосни профили со цел да го зголеми профитот.[465] Така, веб-страниците на Е-трговија го користат профилирањето на однесување за да препорачаат производи кои најверојатно ќе бидат од интерес за

[462] Компјутерска програма што се користи за пристап до сајтови или информации во мрежа (како што е World Wide Web). Најпознати веб прелистувачи се: Google Chrome, Mozilla Firefox, Opera, и др. За повеќе информации, види С. Оргера, *Што е Веб Прелистувач?*, EYewated, available at https://mk.eyewated.com/што е веб прелистувач/ (last visited 15 December 2019].
[463] Мидрак, *supra* note 455.
[464] Castelluccia, *supra* note 460, at p.22.
[465] *Ibid.*, at p.21-22.

корисниците. На пример, Амазон им препорачува производи на корисниците на Интернет, засновани врз претходни индивидуални однесувања (персонализирани препораки), или врз досегашното однесување на слични корисници (социјална препорака), и секако, врз пребаруваните артикли (препорака за артикли).[466]

## 6. Профилирање и импликации за приватност и безбедност

Се чини дека дискурсот за опасностите или заканите соочени со понатамошниот развој на информатичкото општество е заклучен во дебатата за тоа како да се најде рамнотежа помеѓу приватноста и безбедноста. Да не заборавиме дека профилирањето и другите форми на обработка на личните податоци честопати се гледаат како позитивен пристап за еден побезбеден живот.

Како што Hildebrandt наведува во својата статија, граѓаните се убедени дека во време на меѓународен тероризам и транснационален организиран криминал е подобро и попаметно да дадат малку од нивната приватност за да бидат безбедни. Оваа размена доведе до поширoки перспективи за овие прашања, особено во однос на импликациите на профилирањето во демократијата и владеењето на правото. Најпрво дебатата е целосно фокусирана на податоци, меѓутоа како што Hildebrandt истакнува, многу од нив се тривијални и поголемиот дел од времето тие се процесираат од машини, и не од луѓе. Освен злоупотреба, постои мала причина да се плашиме од собирање и складирање на овие податоци.[467]

Меѓутоа, други научници нè предупредуваат за заканите на приватноста на личните информации кои произлегуваат како резултат на профилирање. Castelluccia тврди дека профилирањето создава сериозни грижи за приватноста, бидејќи им овозможува на некои компании или институции да соберат огромна количина на информации за нивните

[466] R. Macmanus, *A Guide to Recommender Systems*, 2009, available at https://readwrite.com/2009/01/26/recommender_systems/ (last visited 20 March 2019].
[467] Hildebrandt, *supra* note 368, at p.550.

клиенти и воопшто за корисниците на Интернет. Опасност е да се претвориме во едно општество каде сите наши физички активности се евидентираат и корелираат.[468]

Оваа закана е реална. Така на пример, владата на Кина изгледа дека има амбициозен план за искористување на моќта на податоците. Таканаречениот „Социјален кредитен систем“ (официјално наречен социјален кредитен рејтинг) утврден со еден план објавен во 2014 год. кој сè уште е во изградба и се очекува да биде целосно оперативен до 2020 година, има за цел да ги прошири системите за оценување на финансиските кредити – најчесто користени од финансиските институции во Соединетите Американски Држави. Планот е да се поврзат јавните и приватните податоци за финансиско и социјално однесување низ цела Кина, да се користат податоците за да се оцени однесувањето на поединците и компаниите, и според тоа да се казнуваат или да се наградат одредени лица за несоодветно, односно соодветно однесување.[469] Секој граѓанин во Кина ќе добие оцена што ќе биде јавно достапна. Оценувањето се однесува на социјалното однесување на поединците, како што се нивните навики за трошење, редовно плаќање на сметките, нивните социјални интеракции, итн., и според овие елементи се оценува дали една личност е доверлива (и ова ќе биде јавно рангирано).[470] За да се изведе тоа, кинеската влада има вклучено околу 200 милиони безбедносни камери низ цела Кина.[471] Дали е ова систем на социјална контрола? Социјалниот рејтинг во суштина става број на една личност и неговата вредност и целосно ја нарушува приватноста на корисниците. Сите форми на активности и интеракции (онлајн или на друг начин) ќе се оценуваат и ќе бидат достапни за другите лица. Така на пример, некој што ќе купи алкохол ќе се смета како неоговорен, а некој кој игра видеоигри десет часа на ден ќе се смета како неактивен. Според ова, овој систем може да создаде неточна и нецелосна слика за една личност. Проблемот останува во тоа што општественото прифатливо однесување ќе се дефинира од

[468] Castelluccia, *supra* note 460, at p.22.
[469] Chorzempa, Triolo and Sacks, 'China's Social Credit System: A Mark of Progress or a Threat to Privacy?', *Peterson Institute for International Economics* (2018) , available at https://www.piie.com/system/files/documents/pb18-14.pdf , at p.1.
[470] Т. Гроздановски, *Како ќе функционира оценувањето на жителите во Кина?*, 2017, available at https://www.fakulteti.mk/news/17-12-04/kako_kje_funkcionira_ocenuvanjeto_na_zhitelite_vo_kina (last visited 8 November 2019].
[471] Б. Арсовска, *Кина воведува застражувачки надзор на луѓето, животот ќе зависи од поени*, 2018, available at https://www.fakulteti.mk/news/21092018/kina-voveduva-zastrashuvachki-nadzor-na-lugjeto-zhivotot-kje-zavisi-od-poeni (last visited 8 November 2019].

страна на кинеската влада, која исто така најверојатно ќе има казнени мерки за личностите кои ќе ја нарушат оваа доверба.[472]

Во понатамошниот текст ќе се зборува за три најпопуларни Интернет услуги, како главни извори на информации што се користат за профилирање, како што се: веб-страници и социјални мрежи.

## 6.1 Веб-страници

Еден од главните извори на информации што се користат за профилирање доаѓа од следење од страна на веб-страниците, т.е., следење на корисниците низ различни посети или преку различни страници. Во собирањето на податоците се вклучува и редоследот на посетените страници и времето поминато во секоја од нив. Веб-следењето се врши преку регистрирање на адреса на Интернет протоколот (IP) на веб-страниците кои ги посетуваме, и преку користење на техники како што се колачиња (cookies).[473]

### 6.1.1 Колачиња (cookies)

Колачињата се парче текстови зачувани од страна на веб-страницата која ја посетуваме. Едно колаче се состои од еден или повеќе парчиња на информации поставени од страна на веб-серверот. Постојат два вида колачиња: привремени и постојани колачиња.

Привремените колачиња честопати се користат за складирање на информации кои се однесуваат на изборите на корисниците. Тие се поставени од давателот на услугата кога корисникот се најавува, и се бришат кога корисникот се одјавува.[474]

[472] Гроздановски, *supra* note 470.
[473] Види: McKinley, 'Cleaning Up After Cookies', *Technical Report, ISEC PARTNERS* (2008) , available at https://www.nccgroup.trust/us/our-research/cleaning-up-after-cookies/.
[474] Castelluccia, *supra* note 460, at p.23.

Постојаните колачиња најчесто се користат како токени за автентикација. Овие датотеки остануваат во пребарувањето на корисникот додека истите не се избришат експлицитно или истечат. Тие се испраќаат непроменети од страна на прелистувачот секој пат кога еден корисник ќе пристапи до таа веб-страница, па затоа можат да се користат од страна на веб-страниците за следење на нивните корисници.[475]

Со други зборови, колачињата се податоци кои ги користат веб-страниците за да ги идентификуваат своите корисници. Преку овие податоци веб-страната може да го идентификува корисникот следниот пат кога ќе ја посети страницата, па затоа не е потребно корисникот да се идентификува секогаш кога ќе влезе на истата веб-страна.[476] Постојаните колачиња предизвикуваат сериозни грижи за приватноста. Во понатамошниот текст терминот колаче ќе се однесува на постојаните колачиња.

Како што се наведува на веб-страната на Дирекцијата за заштита на лични податоци на Република Северна Македонија,[477] колачињата се мали текстуални документи кои можат да прибираат и чуваат податоци за:

- адресата на Интернет протоколот (IP) на компјутерот,
- фреквенцијата на посета на веб-страната,
- потреби на корисникот,
- корисничкото име и лозинката,
- список на производи кои биле купени на Интернет,
- посетените веб-страни,
- име и презиме и,
- алфанумеричките знаци поврзани со личните податоци на корисникот на компјутерот.

Колачињата им овозможуваат на веб-страниците да формираат профили за нивните корисници врз основа на податоците што претходно ги имаат дадено. Тоа најчесто се прави за рекламни цели.[478]

[475] *Ibid.*
[476] За повеќе информации може да ја посетите веб страницата на Дирекција за заштита на лични податоци на Република Северна Македонија, во https://dzlp.mk/mk/cookies.
[477] Види: https://dzlp.mk/mk/cookies.
[478] *Ibid.*

Некои страници, како што се оние на рекламните компании, користат колачиња од трета страна за да ги следат корисниците на повеќе веб-страници. Така на пример, една компанија за рекламирање може да следи еден корисник на сите веб-страници каде што компанијата за рекламирање има ставено реклами (слики или линкови). Знаењето на страниците што ги посетува одредениот корисник и дозволува на компанијата за рекламирање да ги таргетира корисниците и да дава реклами кои се базираат на интересите на корисникот.[479] Со други зборови, колачињата од трети страни се колачиња кои се поставуваат не од веб-страницата која ја посетуваме моментално, туку од некоја друга веб-страница. На пример, на една веб-страница која ја посетуваме има копче "Like", и во моментот кога ние притискаме на тоа копче, посетената веб-страна ќе складира колаче на кое подоцна може да се пристапи од страна на Facebook за да го идентификува посетителот и да види кои веб-страници ги посетил.

Колачињата обезбедуваат четири главни предности за развивачот на софтверот : тие можат да содржат податоци за сесии, како во шопинг количка; можат да се користат за чување на информации за најавување; можат да обезбедуваат персонализација; или тие можат да се користат за следење на активноста на корисникот.[480]

За да имаме една идеја за тоа колку веб-страниците се потпираат на податоците прибирани од колачиња, имам избрано некои од најпосетените веб-страници низ целиот свет и проверив колку колачиња од трети страни тие користат (види слика 8).

[479] Castelluccia, *supra* note 460, at p.24.
[480] McKinley, *supra* note 473, at p.2.


**Слика 8. Број на колачиња од трети страни за некои од најпосетените веб-страници од целиот свет.**

Извор на податоци: Cookiepedia.co.uk

Иако колачињата се неопходни за современиот Интернет,[481] дебатата за нивното влијание врз приватноста на веб-корисниците е секогаш присутна. На еден начин, колачињата им овозможуваат на веб-страниците да чуваат податоци за корисниците или нивната интеракција со страницата. Колачињата можат да се користат за чување на лични податоци – почнувајќи од името на едно лице, адреса на е-пошта па дури и информации за идентификување кои можат да содржат букви или броеви. Овие информации корисниците ги доставуваат преку регистрација, најавување или формулари за нарачки. Тоа исто така може да биде информација која е уникатно доделена за одреден корисник од страна на веб-страницата. Ситуацијата не е загрижувачка се додека тие информации се безбедни и

[481] Колачињата се употребуваат од страна на веб-страниците за да им помогнат на нивните корисници во навигацијата. Така на пример, cookiepedia.co.uk во својата политика за приватност покажува дека колачињата ги користи за да им помогне на корисниците при регистрација, најавување или да им даде можност да дадат мислење, односно повратни информации за услугата; да ја анализираат употребата на своите производи, услуги или апликации; да им помогне за своите промотивни и маркетинг напори (вклучувајќи рекламирање на оденесување). За повеќе информации, види: https://cookiepedia.co.uk/cookies-and-privacy-policy.

се чуваат само привремено; меѓутоа најчесто се случува спротивното, што значи дека постои ризик за злоупотреба.

За да се намали ризикот за заштита на лични податоци, пред да се дадат истите многу е важно да се прочита политиката на приватност на одредената веб-страна која се посетува, односно да се прочитаат правилата и условите (terms and conditions). Никогаш не треба да се даде согласност за прибирање и процесирање на лични податоци за некоја цел која не е јасна или поединецот не ја разбира. За да се ограничи пристапот до лични информации, исто така треба да се одбива давањето на личните податоци кои не се задолжителни. Секогаш треба да се означи или штиклира (opt-out) опцијата. Во случај на чувствителна трансакција (како на пример кај е-банкарството) треба да се користи кодирана веб врска.[482]

## 6.2 Социјални мрежи

Интернетот и социјалните медиуми им даваат на корисниците лесен начин за пренесување на информации и мислења. Овие платформи можат да се користат за најразлични цели и поединците можат да се најават на овие платформи од нивните персонални компјутери, мобилни телефони или други комуникациски уреди и да пренесуваат информации низ целиот свет за неколку секунди. Многу корисници можат да користат повеќе од еден социјален медиум (на пример Facebook, Instagram, Twitter, идр.)

Интернет-содржината (т.е., видеа, коментари, твитови, и сл.) заедно со врските преку Интернет (пријателства, коментари, следбеници, и сл.) можат да се користат од технологијата за анализа, која ја користи чувствителноста на овие информации за најразлични цели, вклучувајќи и профилирање, односно предвидување на однесување на одредени лица или групи на поединци.

Со софистицирани алатки за анализа се извлекуваат чувствителни податоци, лични информации како што се политички верувања, психосоцијални карактеристики, итн. за корисниците на социјалните медиуми и преку автоматски начин и преку индексирање на податоци, различни институции имаат можност да генерираат профили за масовни

[482] Види: https://dzlp.mk/mk/cookies.

корисници, врз основа на идентификација на обрасци. Во оваа смисла, корисниците на социјалните медиуми од „субјекти во комуникација“ се претвораат во „предмет на информација“, односно „предмет за надзор“.[483]

## 7. Придобивки и ризици на автоматското донесување на одлуки

Моќта на дигиталната технологија доаѓа од системите за надзор. Таканаречениот „надзорен капитализам“ претставува можност за собирање на податоци за клиенти и предвидување на нивното однесување, која стана главен сегмент за креирање на вредности во различни индустрии, како што е трговија на мало, финансии и медиуми.[484] Владите користат слични техники на дигитален надзор за национална безбедност и имаат амбиции да ја прошируваат употребата на техниките за дигитален надзор за подобрување на јавните услуги како што е здравјето и образованието.[485]

Иако системите за профилирање се дизајнирани за подобрување и заштита на нашиот живот, постојат причини да се верува дека овие системи имаат потенцијал за нанесување на штета. Утврдувањето дали потенцијалната штета ја надминува користа не е нешто што може да се направи со тековно испитување, бидејќи тоа се потпира на постојано испитување на влијанието врз населението.

Gutwirth и Hildebrandt ги сумираат заканите кои профилирањето може да ги нанесува, како што се:[486]

1. Надзор на индивидуално однесување, што претставува закана на приватноста во смисла на лична автономија;
2. Нееднаквост во моќта помеѓу оние што профилираат и оние кои се профилираат, што исто така претставува закана за приватноста како лична автономија;

[483] Mitrou et al., 'Social Media Profiling: A Panopticon or Omniopticon Tool?', (2014).
[484] Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization', *Journal of Information Technology* (2015) , available at http://dx.doi.org/10.1057/jit.2015.5 , at pp.75-89.
[485] Taylor, *supra* note 60, at p.77.
[486] Gutwirth and Hildebrandt, 'Some Caveats on Profiling', in S. Gutwirth, Y. Poullet and P. De Hert (eds.), *Data Protection in a Profiled World* (2010) , at p.34.

3. Донесување на погрешни одлуки како резултат на лажни информации, што претставува закана за правичност, бидејќи лицето е „осудено“ врз основа на неточни податоци;
4. Донесување на неправедни одлуки кои овозможуваат невидлива дискриминација;
5. Донесување на едностранни решенија за поединци, што претставува закана за лична автономија и правилен процес, додека таквите одлуки многу тешко можат да се оспорат.

# ГЛАВА ЧЕТВРТА: НАДЗОР ВО ЕРАТА НА СОЦИЈАЛНИТЕ МЕДИУМИ (SOCIAL NETWORK SERVICES), ВЛИЈАНИЕ ВРЗ ПРИВАТНОСТА НА ПОЕДИНЦИТЕ

## 1. Социјални медиуми: дефиниција и влијание врз поврзаноста меѓу луѓето

Grimmelmann истакнува дека социјалните медиуми се страници за социјална мрежа[487], поим кој покажува дека овие веб-страници се дизајнирани за да ги поврзуваат луѓето во „социјална мрежа“[488], структура која овозможува интеракции помеѓу луѓето. Наумовски и Рашковски ја издвојуваат дефиницијата според која социјалните медиуми претставуваат вид на виртуелна заедница фокусирана на создавање и одржување односи, и во однос на елементите кои ги сочинуваат социјалните медиуми, тие ги бројат следниве елементи:[489]

- Содржината – елемент кој им овозможува на поединците да бидат креатори на различни содржини и истите да бидат слободно и лесно/едноставно дистрибуирани.
- Соработка/колаборација – елемент кој овозможува раст на индивидуални дејствија, односно трансформирање во поголеми, колективни резултати.
- Заедница – елемент кој овозможува продолжена соработка во врска со една идеја, којашто може да се одвива од различни локации.
- Колективна интелигенција – елемент кој ги одредува социјалните медиуми како простор за поврзување на членовите на групата и стекнување на колективно искуство.

[487] Grimmelmann, *supra* note 343, at p.1142.
[488] Во понатамошниот текст терминот „социјални медиуми“ и „социјални мрежи“ се користат комплементарно.
[489] Наумовски and Рашковски, *supra* note 304, at p.280-281.

Според Boyd и Ellison,[490] социјалните медиуми се дефинираат како веб-базирани услуги кои им овозможуваат на поединците:

(1) Да имаат јавен или полу-јавен профил во ограничен систем;

(2) Да создадат список на пријатели со други корисници со кои имаат некаква врска; и

(3) Да го прегледаат својот список на пријатели и списокот на другите поединци, направени во рамките на истиот систем.

Овие три точки на дефиницијата одговараат на три важни аспекти на социјалните интеракции овозможени од таквите веб-страници. Првата точка, профили – го нагласува идентитетот на корисниците: корисниците создаваат еден профил што ги претставува; Втората точка, контакти – ги потенцира односите меѓу одредени корисници: поединците воспоставуваат врски едно на едно со други личности; Третата точка, прегледувањето на списокот на пријатели ја нагласува заедницата: корисниците земаат посебно место меѓу своите пријатели.[491]

Има различни мотивации за користење на социјални медиуми. Причините на луѓето за користење на социјални медиуми се водат од социјални фактори. Луѓето ги користеле компјутерите како средство за дружење и социјализирање долго време,[492] и нови форми на електронски услуги се прошируваат многу брзо кога им нудат на корисниците нешто привлечно.[493]

Grimmelmann објаснува дека има три вида на социјални фактори кои ги тераат луѓето да користат социјални медиуми, и секој фактор ги тера луѓето да споделуваат лични информации и секој фактор зависи од личните информации на другите корисници.

Според Grimmelmann, првиот социјален фактор е најлесно да се види: социјалната мрежа им дозволува на луѓето да градат свој профил таков каков што сакаат, односно да кажат кои се тие.[494] Goffman забележува дека дневните социјални интеракции се полни со

[490] Boyd and Ellison, 'Social Network Sites: Definition, History, and Scholarship', *Journal of Computer-Mediated Communication* (2007).
[491] Grimmelmann, *supra* note 343, at p.1143.
[492] Види: Rheingold, 'The Virtual Community: Homesteading on the Electronic Frontier', (2000). (Авторот дава детализирано искуство за неговите учества на почетокот на електронските комуникации).
[493] Види: M. Campbell-Kelly et al., *Computer: A History of the Information Machine* (3rd ed., 2013). (Опишувајќи го брзото усвојување на е-пошта во 1970-тите).
[494] Grimmelmann, *supra* note 343, at p.1152.

обиди да ги убедите другите да ги прифатат вашите тврдења за себе.[495] Во овој контекст, онлајн интеракциите се многу слични. Се што ние користиме на социјалните медиуми, почнувајќи од корисничкото име, влијае на тоа како другите нè гледаат нас.[496] Сите наши напори за да оставиме одреден впечаток врз другите, Goffman ги нарекува „управување со впечаток".[497] На социјалните медиуми тоа најчесто се прави преку избирање на слика на профил. Поради ова, многу корисници се трудат да ги прикажат најдобрите фотографии за самите себе, бидејќи профилите на Facebook им овозможуваат на корисниците да претстават „престиж, диференција, автентичност и театарска личност" користејќи заеднички културен јазик.[498] Така, профилите на социјалните мрежи претставуваат социјални артефакти: контролирани впечатоци за специфична публика, толку перформативни колку и информативни.[499] Тие се поврзани со идентитетот на една личност.

Вториот социјален фактор е дека социјалните медиуми и социјалното вмрежување им овозможува на корисниците да се спријателат со нови луѓе и да ги продлабочат врските со актуелните пријатели. Комуникациските технологии ги поврзувале луѓето уште пред Интернетот,[500] и многу автори ја забележуваат јачината на врските преку Интернет.[501] Во овој контекст, личното споделување на информации е основна компонента за интимност.[502] Социјалните мрежи се разбираат како услуги кои им овозможуваат на своите корисници различни начини за комуникација и споделување на содржини,

[495] E. Goffman, *The Presentation of Self in Everyday Life* (1st ed., 1959).
[496] P. Wallace, *The Psychology of the Internet* (1999), at pp.14-37. (Авторот зборува за тоа како корисниците на Интернет управуваат со нивните онлајн личности-како се среќаваме со луѓето со кои комуницираме преку Интерет).
[497] Goffman, *supra* note 495, at p.80.
[498] Liu, 'Social Network Profiles as Taste Performances', *Journal of Computer-Mediated Communication* (2008) , at ) 252–275. (Статијата проучува како различни интереси на едно лице изразени на социјалните мрежи, како што е музика, книги, филмови, телевизиски емисии, итн., можат да функционираат како експресивни елементи за изградба на вкусот и профилот на одредено лице).
[499] Grimmelmann, *supra* note 331, at p.1153; A. Williams, *Here I Am Taking My Own Picture*, 2006, New York Times, available at https://www.nytimes.com/2006/02/19/fashion/sundaystyles/here-i-am-taking-my-own-picture.html (last visited 6 December 2019]. (Williams цитира експерти кои го опишуваат „дигиталното автопортретирање" како „само-брендирање", „театарски").
[500] T. Standage, *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers* (2 (revised, 2014). (Авторот раскажува за тоа како телеграфот бил револуционарен напредок во комуникацијата, како го потресе светот и како доаѓањето на телеграфот беше многу слично на појавата на Интернетот еден век и половина подоцна).
[501] Види на пример: J. Dibbell, *My Tiny Life: Crime and Passion in a Virtual World* (1999). (Авторот ја опишува својата романса на Интернет).
[502] Strahilevitz, 'A Social Networks Theory of Privacy', *The University of Chicago Law Review* (2005) , at pp.919-988.

вклучувајќи размена на пораки, споделување на фотографии и видеа, коментирање, препорачување пријатели, итн. Употребата на вистински имиња (наместо корисничко име) и особено фотографии, укажува на директна интеракција, давајќи посилен психолошки впечаток. Тоа што ги прави социјалните мрежи уникатни не е фактот што тие им овозможуваат на поединците да се сретнат со странци, туку тоа што корисниците имаат можност да ги направат јавни своите социјални мрежи. Ова може да резултира во врски помеѓу поединци кои поинаку не би се сретнале,[503] но тоа не е често целта на социјалните мрежи. Во поголемите социјални мрежи корисниците не бараат „мрежно поврзување“ и запознавање на нови луѓе; наместо тоа, тие комуницираат со луѓе кои веќе се дел на нивната проширена социјална мрежа.[504]

Третиот социјален фактор е дека страницата за социјално вмрежување му дозволува на корисникот да заснова свој социјален статус. Основната желба е едноставна и стара: да се препознае како ценет член на заедницата.[505] Постојаната човечка желба да биде дел од посакуваните социјални групи ги тера луѓето да користат социјални мрежи. Поради ова, луѓето уживаат во користењето на социјалните мрежи, дури и ако тие немаат причина да ги користат таквите платформи, само поради фактот што нивните пријатели ги користат истите. Ова ја претставува желбата на луѓето да се вклопат во одредени ситуации. На пример, ако нашите пријатели се во трговски центар, ние ќе им се придружиме таму; ако тие се на Facebook, и ние ќе бидеме на Facebook.

Идентитетот, врската со пријателите и заедницата, и социјалниот статус се основни елементи на социјална интеракција, и поради тоа тие остануваат висока мотивирачка сила за користење на социјални медиуми.[506]

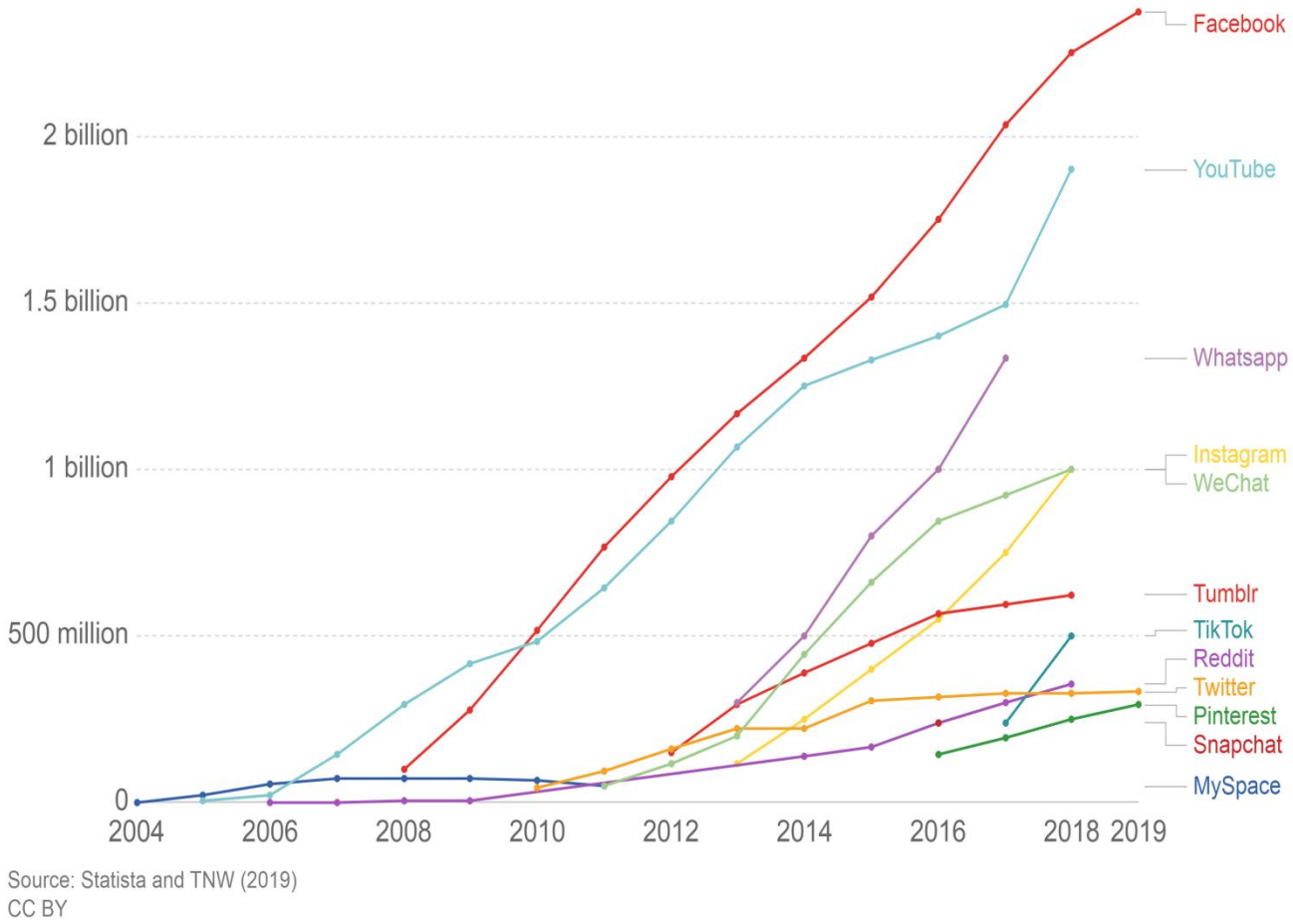
[503] Haythornthwaite, 'Social Networks and Internet Connectivity Effects', *Information, Communication & Society* (2005).
[504] Boyd and Ellison, *supra* note 490, at p.211.
[505] Grimmelmann, *supra* note 343, at p.1157.
[506] Maslow, 'A Theory of Human Motivation', *Psychological Review* (1943) , at pp.370-396. (Наведување и дискутирање за основните човекови потреби).

## 2. Социјални медиуми како „економија за надзор“

Социјалните медиуми го сменија светот. Брзото усвојување на овие технологии го изменија нашиот живот, почнувајќи од начинот на кој наоѓаме партнер, како пристапуваме до различни информации, како организираме и бараме политички промени, итн. Растот на платформите за социјални медиуми во текот на последната деценија се совпаѓа со појавата на таканаречената ера на „Големи податоци“ (Big Data).[507] Во 2019 година, Facebook, најголемата платформа за социјални медиуми има 2,4 милијарди корисници,[508] а другите социјални медиуми исто така постојано имаат зголемување на нивните корисници (види слика 9). Еден профил на одредено лице на Facebook содржи околу четириесет парчиња на лични информации, како што се: име, роденден, политички и религиозни погледи, контакт информации, пол, сексуален избор, омилени книги, филмови, итн.; едукација и вработување, фотографии, и слично.[509]

Социјалните сајтови на медиумите генерираат приходи со насочено рекламирање, врз основа на лични информации. Како такви, тие се заинтересирани да обезбедат колку е можно повеќе информации. Овие платформи содржат доверливи информации за нивните корисници, и поради ова корисниците се изложени на надворешни (внатрешни) напади. Со зголемената глобална употреба на социјалните медиуми, се појавија низа можности за злоупотреба на личните податоци на поединците, како што е кражба на идентитет, вршење на онлајн измами, и слично. Освен тоа, употребата на социјални медиуми може да открие информации за корисниците кои ќе бидат искористени од страна на криминалци. Така на пример, ако објавите еден статус на Facebook или Twitter дека сте надвор од државата, постои можноста вашиот дом да се соочи со кражба.[510]

[507] Во својата Статија, Tufekci покажува дека големи пакети на податоци, кои обично се нарекуваат Големи податоци (Big Data), се користат за проучување на многу феномени, вклучително и човечкото однесување. За повеќе информации, види: Tufekci, 'Big Questions for Social Media Big Data: Representativeness, Validity and Other Methodological Pitfalls', *Proceedings of the Eighth International AAAI Conference on Weblogs and Social Media* (2014) , available at https://www.aaai.org/ocs/index.php/ICWSM/ICWSM14/paper/view/8062/8151.
[508] E. Ortiz-Ospina, *The Rise of Social Media*, 2019, available at https://ourworldindata.org/rise-of-social-media (last visited 1 December 2019].
[509] Grimmelmann, *supra* note 343, at p.1149.
[510] Наумовски and Рашковски, *supra* note 304, at p.283-284.




**Слика 9. Број на луѓе кои имаат користено социјални медиуми во периодот : 2004-2019 година.**

Движечката сила за растот на социјалните медиуми и општо за сите дигитални медиуми е еден комплексен збир на системи за прибирање, следење и таргетирање, кои го следат однесувањето на индивидуалните корисници, како и нивните интеракции со пријатели и други луѓе. Така на пример, маркетингот, собирањето на податоци, и сите операции за следење и таргетирање на Facebook се особено прилагодени на клучните аспекти на развојот на адолесцентите. Овие техники се однесуваат на потребите на младите луѓе и ги користат нивните уникатни слабости. Адолесцентите се поранливи од таквите техники, поради емотивната нестабилност и нивната тенденција да дејствуваат импулсивно, па затоа овие техники се прилагодени на нивниот индивидуален профил и

обрасци на однесување (на пример има таргетирање на локација кога корисникот е близу до една точка за купување).[511]

Според Tufekci, Големите податоци на социјалните медиуми се сметаат како клучен увид во однесувањето на една личност, кој наведува дека појавата на големи податоци од социјалните медиуми имаа имликации за проучување на човечкото однесување слично како што е воведувањето на микроскопот или телескопот во областа на биологијата и астрономијата.[512]

## 3. Социјални медиуми и импликации за приватноста на податоците

Големите бази на податоци за човечката активност на социјалните медиуми привлекоа големо научно внимание. Поради единствената улога што ја играат социјалните медиуми во животот на корисниците, овие платформи можат да привлечат огромни количини на информации. Во моментов, развојот на Големи податоци (Big Data) се соочува со многу проблеми, и прашањата за приватност и безбедност се еден од клучните проблеми, бидејќи во денешно време секој потег што луѓето го прават на Интернет се евидентира, вклучувајќи ги и нивните навики за купување, контакт со пријатели, навики за читање, навики за пребарување, итн.

Безбедносните импликации на Големите податоци не претставуваат само закана за ограничување на личната приватност. Тие исто како сите информации, се соочуваат со големи ризици при складирање, обработка и пренос на лични податоци, па затоа е потребно да се обезбеди заштита на личните податоци на сите корисници. На пример, во нашите социјални активности, често се појавува случајот кога социјалните медиуми препорачуваат да се поврзуваме со луѓе кои можеби ние ги познаваме. Зошто се случува тоа? На пример, ако личноста А го знае Игор, а Игор ја знае Ана, може да се шпекулира дека личноста А можеби исто така ја знае Ана. Преку анализата на социјалните мрежи на два корисника, може да се добијат бројни информации за корисниците. Иако одредени корисници можат да ја исклучат функцијата за читање на социјалните мрежи, додека

[511] Montgomery, *supra* note 160, at p.1.
[512] Tufekci, *supra* note 507, at p.505.

поединците ги користат овие платформи, тие оставаат дигитални траги, како што се статуси, пораки, и др.[513]

Јасно е дека откривање на масовни лични информации на социјалните медиуми претставува сериозна закана за приватноста и идентитетот на корисниците на овие платформи. Како одговор на тоа, социјалните медиуми имаат поставено политики за приватност кои конкретно се однесуваат на колекцијата на лични информации. Тие обично содржат детали за личните информации кои се собираат, како ќе се користат личните податоци, на кого можат да бидат објавени, безбедносните мерки преземени за заштита на личните информации и дали веб-страницата користи технологии како што е на пример, колачиња, за следење на информациите или навиките на прелистување. Општо, политиките за приватност го појаснуваат видот на информации што се собираат и видот на обработка за кои корисникот дал согласност откако има поставени лични информации во таа услуга. Затоа, со оглед на тоа што профилите на социјалните медиуми содржат чувствителни информации, како што е адреса, место и датум на раѓање, и сл., корисниците треба да применуваат детално разгледување на политиката за приватност на одредениот сајт.

## 4. Facebook

Кога зборуваме за социјални медиуми, речиси е невозможно да не се вратиме неколкупати на Facebook, бидејќи во моментов, Facebook е најкористениот социјален медиум низ целиот свет.[514] Ова е најпопуларната страница за социјално вмрежување што служи како алатка за презентација. Корисниците на Facebook споделуваат информации за нивниот живот, објавуваат слики, видеа и други информации, така што стануваат „видливи“ за нивните вистински и потенцијални пријатели. Од една страна, Facebook им

[513] Zeng, *supra* note 67, at p.47.
[514] D. Chaffey, *Global Social Media Research Summary 2019*, 2019, Smart Insights, available at https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ (last visited 10 October 2019].

дозволува на корисниците да споделуваат лични информации на еден многу лесен начин. Од друга страна, Facebook претставува еден електронски систем за мониторинг.[515]

Andrejevic покажува како овие информации се користат како начин за наблудување и контрола, бидејќи секое парче на податоци може да се следи од страна на креаторите на Facebook или од хакери.[516] Покрај тоа, постојат специфични функции кои можат да се користат за цели за надзор, како што е на пример копчето "Like".[517] Профилирањето е вообичаена практика на Facebook, сметајќи дека корисниците сами си создаваат профили и ги прават достапни за системот.[518]

## 4.1 Копчето "Like": отпечатоци на социјалната мрежа

Според Facebook, копчето Like му дозволува на корисникот да сподели содржини со пријателите на Facebook.[519] Додека копчето Like претставува една алатка која им овозможува на членовите на Facebook да споделуваат свои интереси, таа исто така претставува грижа за приватноста на податоците. На пример, ако некој го притисне копчето 'Like' на Facebook, автоматски тоа наведува дека одреденото лице е заинтересирано за една веб-страница или елемент на веб-страница. За давателот на содржината, копчето Like на тој начин може да функционира како важна алатка за предвидување на однесувањето на поединците. Покрај тоа, копчето Like се користи и за испраќање на колачиња и за следење на корисниците на електронските услуги, без оглед на тоа дали едно лице го користи или не копчето Like. Така, иако еден корисник нема сметка на Facebook, може да се создаде збир на податоци во врска со индивидуалното

[515] Galetta, *supra* note 363, at p.109.
[516] M. Andrejevic, *ISpy: Surveillance and Power in the Interactive Era* (2007).
[517] Roosendaal, 'Facebook Tracks and Traces Everyone: Like This!', *Tilburg Law School Legal Studies Research Paper Series No. 03/2011* (2010) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563 , at pp.1-10.
[518] Galetta, *supra* note 363, at p.109.
[519] Facebook Developers, "Like Button for the Web" available at http://developers.facebook.com/docs/reference/plugins/like (last visited 15 December 2019).

однесување, базирано на неговите резултати на пребарување. Кога корисникот подоцна ќе создаде сметка, податоците можат да се поврзат со новиот воспоставен профил. [520]

## 4.2 Facebook: една машина за надзор

Секој ден, корисниците на Facebook испраќаат стотици милиони фотографии на социјалната мрежа. Ако тие не ја исклучиле опцијата за препознавање на лице, софтверот ги скенира тие фотографии во потрага по лица што ги препознава. Корисниците имаат можност да ги прифатат или одбијат препораките за тоа кој треба да биде обележан на одредената фотографија, и според тоа алгоритмите на Facebook се подобруваат. Предлозите за обележување (tag) му овозможуваат на Facebook да анализира дали пријателите на одредени корисници се наоѓаат на фотографиите поставени од корисникот. Кога една фотографија е поставена, технологијата ја скенира фотографијата за да открие дали има геометриски карактеристики (како што е растојанието помеѓу очите, носот и ушите), кои можат да се користат за да се идентификува лицето на еден човек. Технологијата потоа ги споредува овие информации со информации од базата на податоци на Facebook за да се утврди дали има совпаѓање, како што е прикажано на слика 10.[521]

[520] Roosendaal, 'We Are All Connected to Facebook...by Facebook!', in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?* (2012) , at p.4.

[521] C. Kwan, *US Court Rules Users Can Sue Facebook over Facial Recognition Technology*, 2019, ZDNet, available at https://www.zdnet.com/article/us-court-rules-users-can-sue-facebook-over-facial-recognition-technology/ (last visited 7 December 2019].


**Слика 10. Предлозите за обележување на Facebook.**

Извор: https://www.facebook.com/notes/facebook/making-photo-tagging-easier/467145887130/

Во *Patel против Facebook*,[522] една група корисници на Facebook од Илиноис тврдат дека Facebook го прекршил Законот за приватност на биометриските информации на Илиноис со користење на софтвер за препознавање на лице на фотографии без експлицитна согласност. Додека Facebook тврдеше дека корисниците немале вистинска повреда бидејќи мапирањето на нивните податоци за лицето не предизвикало да изгубат пари или да претрпат некоја економска повреда, судот донесе одлука дека употребата на технологија за препознавање на лицето без согласност ги напаѓа приватните права на поединците и конкретните интереси.[523] Адвокатот, кој ги претставуваше корисниците на Facebook, рече дека пресудата испраќа силна порака дека Facebook може да биде одговорен поради неуспех за заштита на личните податоци на луѓето. „Овие биометриски податоци се многу чувствителни. Тие се уникатни како отпечатоци од прсти“, рече

[522] *Patel v. Facebook, Inc., No. 18-15982 (9th Cir. 2019)-JD*, 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/18-15982/18-15982-2019-08-08.html.

[523] N. F. Wessler, *A Federal Court Sounds the Alarm on the Privacy Harms of Face Recognition Technology*, 2019, ACLU, available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/federal-court-sounds-alarm-privacy-harms-face/ (last visited 5 September 2019].

адвокатот Shawn Williams.[524] Одлуката е значаен напредок во борбата против заканите на технологиите за надзор, алармирајќи го потенцијалот на овие технологии сериозно да ја нарушат приватноста на луѓето.

Истражувачите на Facebook сугерираат дека компанијата ја има најголемата база на податоци за лицето досега, подржана од DeepFace, систем за длабоко учење за препознавање на лицето.[525] За разлика од Amazon, кој користи софтвер за препознавање на лице кој скенира бази на податоци обезбедени од клиенти, како агенции за спроведување на законот, системот на Facebook не користи надворешни податоци, бидејќи Facebook ги има сите податоци што ние сами ги испраќаме таму (слики од различни фази од нашиот живот, од различни агли, со различна облека и фризури, итн) секој ден. Facebook нè препознава нас, дури и ако ние никогаш не сме се обележале на нашите слики, има некој од нашите пријатели кои не имаат обележано во нивните фотографии.[526]

Кога размислуваме за тоа како една голема компанија како Facebook може да го користи своето богатство за социјален надзор, Siva Vaidhyanathan, автор на книгата "Antisocial Media" сугерира да размислуваме во однос на начинот на кој Facebook работи во социјалното вмрежување. „Еден глобален систем кој поврзува 2,2 милијарди луѓе низ стотици земји, му овозможува на секој корисник да објавува свои содржини, развива алгоритми кои фаворизираат преполнети содржини и зависи од рекламен систем кој насочува реклами користејќи интензивен надзор...не може да се очекува да испадне од доминантната позиција сама по себе", вели Vaidhyanathan.[527]

Главниот извршен директор на Facebook, Mark Zuckerberg вели дека Facebook не ги продава податоците на корисниците, нарекувајќи го тоа како обична заблуда што луѓето ја имаат за Facebook.[528] Дека тоа е точно, научниците истакнуваат со тоа што Facebook им дава можност на рекламните компании да стигнат до одредени луѓе врз основа на

[524] N. Iovino, *Ninth Circuit Advances $35 Billion Privacy Suit Against Facebook*, 2019, Courthouse News Service, available at https://www.courthousenews.com/ninth-circuit-advances-35-billion-privacy-suit-against-facebook/ (last visited 3 September 2019].
[525] A. Glaser, *Facebook's Face-ID Database Could Be the Biggest in the World. Yes, It Should Worry Us*, 2019, Slate, available at https://slate.com/technology/2019/07/facebook-facial-recognition-ice-bad.html (last visited 7 December 2019].
[526] *Ibid.*
[527] S. Vaidhyanathan, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (2018), at p.9.
[528] *Does Facebook Really Not Sell Your Data to Advertisers?*, 2018, Thejournal.Ie, available at https://www.thejournal.ie/mark-zuckerberg-facebook-sell-data-3957290-Apr2018/ (last visited 13 November 2019].

податоците што Facebook ги има за тие луѓе.[529] Во оваа смисла, Facebook не ги продава податоците на своите корисници директно на трети страни, но благодарение на податоците и информациите што ги има, Facebook во 2018 година надмина 55 милијарди американски долари приходи. Само приходите од рекламирање за четвртиот квартал на 2018 година достигнаа 16,64 милијарди американски долари, зголемени за 30% во однос на истиот период во 2017 година.[530] Но како се случува ова? Facebook ги користи податоците што корисниците ги обезбедуваат (на пример каде живеат, колку години имаат, итн.) и ги комбинира со географски информации од нивниот телефон за да ги прилагоди рекламите за одредена публика. Што е публиката поконкретизирана, повеќе пари за Facebook. Како го прави ова Facebook без да продава податоци? Рекламите избираат видови на корисници (таргет група) до кои сакаат да стигнат, а Facebook ги избира корисниците на кои ќе им се појават рекламите. Во овој случај, иако Facebook технички не продава податоци, тоа не значи дека податоците никогаш не ја остават социјалната мрежа.[531] Всушност, со скандалот за приватност на Кембриџ аналитика,[532] кој беше голем политички скандал во почетокот на 2018 година, беше откриено дека Кембриџ аналитика успеа до добие лични податоци на десетици милиони луѓе корисници на Facebook без нивна согласност, преку апликација која наводно била алатка за истражување, и ги користел овие информации за политички рекламни цели. Скандалот беше потсетник дека со години Facebook им дозволуваше на трети лица да користат тони податоци за корисниците на социјалната мрежа. Од друга страна, додека Facebook се обидува да се прошири како социјална мрежа, компанијата би можела да ги продава своите услуги за препознавање на лицето на авиокомпаниите, или на секоја институција која сака да го потврди идентитетот на своите клиенти со една брза фотографија.[533]

[529] Glaser, *supra* note 525.
[530] M. Frascona, *Facebook's Revenue Exceeded $55 Billion in 2018*, 2019, Newsfeed.Org, available at https://newsfeed.org/facebooks-revenue-exceeded-55-billion-in-2018/ (last visited 3 September 2019].
[531] *supra* note 528.
[532] N. Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, 2018, The New York Times, available at https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (last visited 3 September 2019].
[533] Glaser, *supra* note 525.

# Заклучок

Концептот за приватност претставува многу широк концепт кој се толкува и во правни и во филозофски текстови. Покрај огромната литература за приватност, овој поим честопати останува нејасен, бидејќи не постои единствена и унитарна перцепција за тоа како треба да се дефинира приватноста, и како треба да се оправда правото на приватност.

Правата на приватност не се апсолутни. Законите за приватност се донесени за да го регулираат пристапот од луѓето до информациите, а не да го забранат таквиот пристап.

Иако правото на заштита на личните податоци е уставна категорија и основно човеково право, практиката покажува дека поголемиот број на повреди на ова право се резултат на недоволно развиена јавна свест и непознавање на основните начела за заштита на лични податоци.

Во заштитата на личните податоци важна улога имаат правните мерки и закони, било тие од меѓународно или национално ниво. Правните инструменти можат да бидат корисни и ефективни само ако се способни да се прилагодат на актуелните социо-технолошки промени. Ова е еден од предизвиците со кои законодавците во Република Северна Македонија мора да се соочат кога станува збор за донесување, дополнување или промена на законите за заштита на податоците. Тоа ќе им помогне на корисниците на Интернетот целосно да уживаат во предностите на информатичката технологија, додека имаат контрола на нивната дигитална репрезентација, а во исто време овозможува и остварување на другите фундаментални човекови права, како што е слободата на изразување. Иако Република Северна Македонија сè уште не е земја членка на Европската Унија, Општата регулатива за заштита на личните податоци на Европската Унија претставува одлична можност за менување на „старомодниот“ закон за заштита на податоци со нови современи правила, кои ќе обезбедат поголема правна сигурност и ќе им дадат на граѓаните поголема моќ и контрола на нивните лични податоци.

# Библиографија


Ahmed, 'Data Portability: Key to Cloud Portability', *SSRN Electronic Journal* (2010) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1712565.

Allen A.L. and Rotenberg M., *Privacy Law and Society* (2016).

Allison K., *Social Networks May Find It Does Not Pay to Be Too Possessive*, 2008, available at https://www.ft.com/content/8b6351e4-c843-11dc-94a6-0000779fd2ac (last visited 1 January 2019].

Anderson M. and Jiang J., *Teens, Social Media & Technology*, 2018, available at https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/ (last visited 23 November 2019).

Andrade, 'Oblivion: The Right to Be Different from Oneself. Reproposing the Right to Be Forgotten', *Revista de Internet Derecho y Política* (2012) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033155.

Andrejevic M., *ISpy: Surveillance and Power in the Interactive Era* (2007).

Ausloos, 'The 'Right to Be Forgotten' - Worth Remembering?', 28 *Computer Law & Security Review* (2012) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1970392.

Balboni P., Mccorry K. and Snead W.D., *Cloud Computing. Benefits, Risks and Recommendations for Information Security*, 2009, European Networks and Information Security Agency (ENISA), available at https://www.pdpjournals.com/docs/88049.pdf (last visited 1 November 2019].

Bamberger K.A. and Mulligan D.K., *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (2015].

Bankston K., Null E. and Schulman R., *Comments of New America's Open Technology Institute, In the Matter of Competition and Consumer Protection in The 21st Century: The Intersection Between Privacy, Big Data, and Competition*, 2018, Federal Trade Commission, available at https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0034-154926.pdf (last visited 8 November 2019).

Bapat, 'The New Right to Data Portability', *Privacy and Data Protection* (2013).

Beasley L.B., *Did You Know GDPR Compliance Affects Your Data Collection for European and Some Non-European Residents?*, 2018, available at https://beasleydirect.com/gdpr-countries/ (last visited 4 December 2019].

Bennett, 'The Public Surveillance of Personal Data: A Cross-National Analysis', in D. Lyon and E. Zureik (eds.), *Computers, Surveillance, and Privacy* (1996).

Bernal, 'A Right to Delete?', 2 *European Journal of Law and Technology* (2011] , available at http://ejlt.org/article/view/75/144.

Bessant, 'Hard Wired for Risk: Neurological Science, “the Adolescent Brain,” and Developmental Theory', 11 *Journal of Youth Studies* (2008].

Bischoff P., *The World’s Most-Surveilled Cities*, 2019, available at https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ (last visited 3 November 2019).

Bolton, 'The Right to Be Forgotten: Forced Amnesia in a Technological Age', *John Marshall Journal of Computer and Information Law* (2015) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2513652.

Boyd and Ellison, 'Social Network Sites: Definition, History, and Scholarship', *Journal of Computer-Mediated Communication* (2007).

Brummer C. and Gorfine D., *Fintech: Building a 21st Century Regulator’s Toolkit* (2014).

Brynjolfsson, Hitt, and Kim, 'Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance?', (2011) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486.

Bygrave L.A., *Data Protection Law. Approaching Its Rationale, Logic and Limits* (2002).

Byler D., Flores B. and Lewris J., *Using Advanced Analytics to Drive Regulatory Reform: Understanding Presidential Orders on Regulation Reform* (2017).

Campbell-Kelly M. et al., *Computer: A History of the Information Machine* (3rd ed., 2013).

Castelluccia, 'Behavioural Tracking on the Internet: A Technical Perspective', in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?* (2012).

Chaffey D., *Global Social Media Research Summary 2019*, 2019, Smart Insights, available at https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ (last visited 10 October 2019].

Chorzempa, Triolo, and Sacks, 'China’s Social Credit System: A Mark of Progress or a Threat to Privacy?', *Peterson Institute for International Economics* (2018] , available at https://www.piie.com/system/files/documents/pb18-14.pdf.

Clarke, 'Dataveillance - 15 Years On', *Wellington: Privacy Issues Forum* (2003] , available at http://www.rogerclarke.com/DV/DVNZ03.html.

Clarke R., *Dataveillance and Information Privacy*, available at http://www.rogerclarke.com/DV/ (last visited 6 December 2019).

Clarke, 'Information Technology and Dataveillance', *Communications of the ACM* (1988).

Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms', *Computer Science* (1997).

Confessore N., *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, 2018, The New York Times, available at https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (last visited 3 September 2019].

Cook, Augusto, and Jakkula, 'Ambient Intelligence: Technologies, Applications, and Opportunities', *Pervasive and Mobile Computing* (2009].

Coos A., *EU vs US: How Do Their Data Privacy Regulations Square Off?*, 2018, Endpoint Protector, available at https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off/ (last visited 7 December 2019).

Crockford K., *The FBI Is Tracking Our Faces in Secret. We're Suing.*, 2019, ACLU, available at https://www.aclu.org/news/privacy-technology/the-fbi-is-tracking-our-faces-in-secret-were-suing/ (last visited 15 December 2019].

Cyphers B. and O'Brien D., *Facing Facebook: Data Portability and Interoperability Are Anti-Monopoly Medicine*, 2018, Electronic Frontier Foundation, available at https://www.eff.org/deeplinks/2018/07/facing-facebook-data-portability-and-interoperability-are-anti-monopoly-medicine (last visited 11 September 2019).

Dalmia N. and Schatsky D., *The Rise of Data and AI Ethics Managing the Ethical Complexities of the Age of Big Data*, 2019, Deloitte Insights, available at https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2020/government-data-ai-ethics.html (last visited 11 August 2019].

Davies, 'Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity', in P. E. Agre and M. Rotenberg (eds.), *Technology and Privacy: The New Landscape* (1997).

Diaz C., *Privacy Risk Scenario*, 2006, Future of Identity in the Information Society, available at https://www.esat.kuleuven.be/cosic/publications/article-834.pdf (last visited 25 November 2018).

Dibbell J., *My Tiny Life: Crime and Passion in a Virtual World* (1999).

Diker Vanberg, 'The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?', *Journal of Internet Law* (2018).

Diker Vanberg and Ünver, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?', *European Journal of Law and Technology* (2017).

Dobush G., *The EU Wants to Build One of the World's Largest Biometric Databases. What Could Possibly Go Wrong?*, 2019, available at https://fortune.com/2019/05/01/eu-biometric-database-india/ (last visited 19 August 2019].

Van Eecke and Truyens, 'Privacy and Social Networks', 26 *Computer Law and Security Review* (2010] , available at http://dx.doi.org/10.1016/j.clsr.2010.07.006.

Egan, 'Data Portability and Privacy', (2019] , available at https://fbnewsroomus.files.wordpress.com/2019/09/data-portability-privacy-white-paper.pdf.

Eggers W.D., Turley M. and Kishnani P., *The Future of Regulation: Principles for Regulating Emerging Technologies* (2018], available at https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html (last visited 5 November 2019).

Ehrenkranz M., *Sweden's First GDPR Fine Goes to a High School Piloting Facial Recognition Attendance*,

2019, available at https://gizmodo.com/swedens-first-gdpr-fine-goes-to-a-high-school-piloting-1837616893 (last visited 25 November 2019].

Engels, 'Data Portability among Online Platforms', *Internet Policy Review* (2016].

Ennis H. et al., *National Security and Technology Regulation: Government Regulations for Emerging Technology* (2019], available at https://www2.deloitte.com/us/en/insights/industry/public-sector/national-security-technology-regulation.html (last visited 12 September 2019).

Europe University Institute, Guide on Good Data Protection Practice in Research, 2019.

European Commission - Press release, *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses*, 2012, available at https://ec.europa.eu/commission/presscorner/detail/en/IP_12_46 (last visited 1 November 2019].

European Data Protection Supervisor (EDPS), *Opinion on the Communication: A Comprehensive Approach on Personal Data Protection in the European Union*, 2011, available at https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf (last visited 11 November 2019).

European Data Protection Supervisor (EDPS), *Opinion on the Data Protection Reform Package*, 2012, available at https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf (last visited 22 November 2019].

European Union Committee, *EU Data Protection Law: A 'Right to Be Forgotten'?* (2014], available at https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf.

Farivar C., *Retailers Want to Be Able to Scan Your Face without Your Permission*, 2015, ArsTechnica, available at https://arstechnica.com/information-technology/2015/06/retailers-want-to-be-able-to-scan-your-face-without-your-permission/ (last visited 18 July 2019).

Federal Trade Commission (FTC), *Complying with COPPA: Frequently Asked Questions*, 2017, available at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General Audience (last visited 20 November 2019].

Federal Trade Commission (FTC), *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing (Staff Report)* (2012], available at https://www.ftc.gov/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing.

Feiner L., *Facebook Addresses Antitrust Concerns with New Tool That Lets You Transfer Photos to Google*, 2019, available at https://www.cnbc.com/2019/12/02/facebook-releases-new-data-portability-tool-for-photos.html (last visited 4 December 2019).

Feldstein S., *The Global Expansion of AI Surveillance* (2019).

Feldstein, 'The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression', *Journal of Democracy* (2019).

Fingas J., *FTC Fines TikTok $5.7 Million over Child Privacy Violations*, 2019, available at https://www.engadget.com/2019/02/27/ftc-fines-tiktok-over-child-privacy/#:~:targetText=The creators of TikTok are,its lip-syncing video app. (last visited 25 November 2019].

Finn, , Wright, , Friedewald, 'Seven Types of Privacy', in S. Gutwirth et al. (eds.), *European Data Protection: Coming of Age* (2013).

Floridi and Cowls, 'A Unified Framework of Five Principles for AI in Society', *Harvard Data Science Review* (2019].

Fowler G.A., *Don't Smile for Surveillance: Why Airport Face Scans Are a Privacy Trap*, 2019, The Washington Post, available at https://www.washingtonpost.com/technology/2019/06/10/your-face-is-now-your-boarding-pass-thats-problem/ (last visited 13 December 2019).

Frascona M., *Facebook's Revenue Exceeded $55 Billion in 2018*, 2019, Newsfeed.Org, available at https://newsfeed.org/facebooks-revenue-exceeded-55-billion-in-2018/ (last visited 3 September 2019].

Galetta, 'New Surveillance, New Penology and New Resistance: Towards the Criminalisation of Resistance?', in S. Gutwirth, R. Leenes and P. De Hert (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (2014).

Gebhart G., Cyphers B. and Opsahl K., *What We Mean When We Say "Data Portability"*, 2018, Electronic Frontier Foundation, available at https://www.eff.org/deeplinks/2018/09/what-we-mean-when-we-say-data-portability (last visited 18 September 2019).

Glaser A., *Facebook's Face-ID Database Could Be the Biggest in the World. Yes, It Should Worry Us*, 2019, Slate, available at https://slate.com/technology/2019/07/facebook-facial-recognition-ice-bad.html (last visited 7 December 2019].

Goffman E., *The Presentation of Self in Everyday Life* (1st ed., 1959].

González Fuster G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (2014].

Goold, 'Surveillance and the Political Value of Privacy', *Amsterdam Law Forum* (2009] , available at http://amsterdamlawforum.org/article/view/88/152.

GPEN, *2015 GPEN Sweep – Children's Privacy*, 2015, available at https://www.garanteprivacy.it/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf (last visited 26 November 2019).

Graef, 'Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union', *Telecommunications Policy* (2015).

Graux, Ausloos, and Valcke, 'The Right to Be Forgotten in the Internet Era', *ICRI Research Paper No.11* (2012) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2174896.

Gray D., *Data Ownership In The Cloud*, 2014, available at https://dataconomy.com/2014/03/data-ownership-in-the-cloud/ (last visited 5 December 2019].

Grimmelmann, 'Saving Facebook', *Iowa Law Review* (2009].

Gstrein, 'The Right to Be Forgotten in the General Data Protection Regulation and the Aftermath of the "Google Spain" Judgment (C-131/12)', *PinG Privacy in Germany: Datenschutz Und Compliance* (2017] , available at https://www.pingdigital.de/ce/the-right-to-be-forgotten-in-the-general-data-

protection-regulation-and-the-aftermath-of-the-google-spain-judgment-c-131-12/detail.html.

Gumpert and Drucker, 'Public Boundaries:Privacy and Surveillance in a Technological World', *Communication Quarterly* (2001].

Gutwirth, , Hildebrandt, 'Some Caveats on Profiling', in S. Gutwirth, Y. Poullet and P. de Hert (eds.), *Data Protection in a Profiled World* (2010).

Gutwirth, , Hildebrandt, 'Some Caveats on Profiling', in S. Gutwirth, Y. Poullet and P. De Hert (eds.), *Data Protection in a Profiled World* (2010).

Haggerty and Ericson, 'The Surveillant Assemblage', *British Journal of Sociology* (2000].

Hartlev, 'The Concept of Privacy: An Analysis of the EU Directive on the Protection of Personal Data', in D. Beyleveld et al. (eds.), *The Data Protection Directive and Medical Research Across Europe* (2004).

Harwell D., *San Francisco Becomes First City in U.S. to Ban Facial-Recognition Software*, 2019, The Washington Post, available at https://www.washingtonpost.com/technology/2019/05/14/san-francisco-becomes-first-city-us-ban-facial-recognition-software/ (last visited 10 December 2019).

Haythornthwaite, 'Social Networks and Internet Connectivity Effects', *Information, Communication & Society* (2005).

De Hert, , Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action', in S. Gutwirth et al. (eds.), *Reinventing Data Protection?* 1 (2009).

Hildebrandt, 'Profiling: From Data to Knowledge', *DuD: Datenschutz Und Datensicherheit* (2006).

Hiranandani, 'Privacy and Security in the Digital Age: Contemporary Challenges and Future Directions', *The International Journal of Human Rights* (2010).

Hornung, 'A General Data Protection Regulation For Europe? Light And Shade In The Commission's Draft Of 25 January 2012', *SCRIPTed 64* (2012).

Hustinx, 'EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation', in M. Cremona (ed.), *New Technologies and EU Law* 1 (2017).

Iovino N., *Ninth Circuit Advances $35 Billion Privacy Suit Against Facebook*, 2019, Courthouse News Service, available at https://www.courthousenews.com/ninth-circuit-advances-35-billion-privacy-suit-against-facebook/ (last visited 3 September 2019].

Kang, 'Information Privacy in Cyberspace Transactions', *Stanford Law Review* (1998].

Kang et al., 'A Study for Security Scheme and the Right to Be Forgotten Based on Social Network Service for Smart-Phone Environment', *Communications in Computer and Information Science* (2011] , available at https://link.springer.com/chapter/10.1007/978-3-642-23141-4_33.

Kavanagh C., *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?* (2019].

Koops, 'Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice', *Tilburg Law School Legal Studies Research Paper Series No. 08/2012* (2011] ,

available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986719.

Kulk S. and Borgesius Zuiderveen F., *Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe* (2018], The Cambridge Handbook of Consumer Privacy.

Kuzevski I., *Personal Data Protection Vis-à-Vis Freedom of Expression and Information*, 2017, available at https://cloudprivacycheck.eu/latest-news/article/personal-data-protection-vis-a-vis-freedom-of-expression-and-information/ (last visited 5 January 2019).

Kwan C., *US Court Rules Users Can Sue Facebook over Facial Recognition Technology*, 2019, ZDNet, available at https://www.zdnet.com/article/us-court-rules-users-can-sue-facebook-over-facial-recognition-technology/ (last visited 7 December 2019].

Lagone, 'The Right to Be Forgotten: A Comparative Analysis', *SSRN Electronic Journal* (2012] , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229361.

Langheinrich, et al., 'Quo Vadis Smart Surveillance? How Smart Technologies Combine and Challenge Democratic Oversight', in S. Gutwirth, R. Leenes and P. De Hert (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (2014).

Lee T.B., *Feds Lose Control of Thousands of Traveler Photos in Data Breach*, 2019, ArsTechnica, available at https://arstechnica.com/tech-policy/2019/06/hackers-stole-thousands-of-border-crossing-photos-from-border-agency/ (last visited 15 December 2019).

Lehtonen, 'Genetic Information and the Data Protection Directive of the European Union', in D. Beyleveld et al. (eds.), *The Data Protection Directive and Medical Research Across Europe* (2004).

Levesque R.J.R., *Adolescents, Rapid Social Change, and the Law: The Transforming Nature of Protection* (2016).

Lievens and Verdoodt, 'Looking for Needles in a Haystack: Key Issues Affecting Children's Rights in the General Data Protection Regulation', 34 *Computer Law and Security Review* (2018) , available at https://doi.org/10.1016/j.clsr.2017.09.007.

Lindroos-Hovinheimo, 'Legal Subjectivity and the 'Right to Be Forgotten': A Rancie`rean Analysis of Google', 27 *Law Critique* (2016) , available at http://rdcu.be/koh1.

Liu, 'Social Network Profiles as Taste Performances', *Journal of Computer-Mediated Communication* (2008).

Liu S., *Biometric Technologies -Statistics & Facts*, 2019, Statista, available at https://www.statista.com/topics/4989/biometric-technologies/ (last visited 4 June 2019].

Livingstone S. et al., *Risks and Safety on the Internet: The Perspective of European Children: Full Findings and Policy Implications from the EU Kids Online Survey of 9-16 Year Olds and Their Parents in 25 Countries*, 2011, EU Kids Online Network, available at http://eprints.lse.ac.uk/33731/1/Risks and safety on the internet%28lsero%29.pdf (last visited 11 February 2019).

Livingstone, Carr, and Byrne, 'One in Three: Internet Governance and Children's Rights', *Global Commission on Internet Governance Paper Series No. 22* (2015).

Lupton and Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for Their

Rights', 19 *New Media and Society* (2017) , available at http://journals.sagepub.com/doi/full/10.1177/1461444816686328.

Lyon, 'Editorial. Surveillance Studies: Understanding Visibility, Mobility and the Phenetic Fix', *Surveillance & Society* (2002).

Macenaite and Kosta, 'Consent for Processing Children's Personal Data in the EU: Following in US Footsteps?', 26 *Information & Communications Technology Law* (2017).

Martin, , del Alamo, 'Forget About Being Forgotten From the Right to Oblivion to the Right of Reply', in S. Gutwirth, R. Leenes and P. De Hert (eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (2016).

Marx, 'What's New About the "New Surveillance"? Classifying for Change and Continuity', *Surveillance & Society* (2002).

Marx G.T., *Windows into the Soul: Surveillance and Society in an Age of High Technology* (2016).

Mascheroni G. and Ólafsson K., *Net Children Go Mobile: Risks and Opportunities* (2014), 2nd Ed. Educatt.

Maslow, 'A Theory of Human Motivation', *Psychological Review* (1943).

Mayer-Schönberger, 'Generational Development of Data Protection in Europe', in P. E. Agre and M. Rotenberg (eds.), *Technology and Privacy* (1997).

McKinley, 'Cleaning Up After Cookies', *Technical Report, ISEC PARTNERS* (2008) , available at https://www.nccgroup.trust/us/our-research/cleaning-up-after-cookies/.

McNealy, 'The Emerging Conflict between Newsworthiness and the Right to Be Forgotten', 39 *Northern Kentucky Law Review* (2012).

Mendonca-Richards A., *The Right to Be Forgotten, Rehabilitated, and to Know: Two Important Cases against Google*, 2018, available at https://www.farrer.co.uk/news-and-insights/the-right-to-be-forgotten-rehabilitated-and-to-know-two-important-cases-against-google/ (last visited 25 September 2019].

Merchant and Allenbey, 'Soft Law: New Tools for Governing Emerging Technologies', *Bulletin of the Atomic Scientists* (2017].

Metz C., *The Week in Tech: YouTube Fined $170 Million Over Child Privacy Violations*, 2019, The New York Times, available at https://www.nytimes.com/2019/09/06/technology/youtube-fine-child-privacy.html (last visited 26 November 2019).

Metz R., *Beyond San Francisco, More Cities Are Saying No to Facial Recognition*, 2019, CNN Business, available at https://edition.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html (last visited 10 December 2019].

Micheti, Burkell, and Steeves, 'Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand', *Bulletin of Science, Technology & Society* (2010].

Mitrou et al., 'Social Media Profiling: A Panopticon or Omniopticon Tool?', (2014].

Montgomery, 'Youth and Surveillance in the Facebook Era: Policy Interventions and Social Implications', 39 *Telecommunications Policy* (2015] , available at http://dx.doi.org/10.1016/j.telpol.2014.12.006.

Montgomery and Chester, 'Data Protection for Youth in the Digital Age: Developing a Rights-Based Global Framework', 1 *European Data Protection Law Review* (2015] , available at https://edpl.lexxion.eu/article/EDPL/2015/4/6.

Mordini, 'Policy Brief on: Whole Body – Imaging at Airport Checkpoints: The Ethical and Policy Context', in R. von Schomberg (ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields* (2011).

Mozur P., *In Hong Kong Protests, Faces Become Weapons*, 2019, New York Times, available at https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html (last visited 10 December 2019).

Nys, 'The Scope of Exemptions for Medical Research', in D. Beyleveld et al. (eds.), *The Data Protection Directive and Medical Research Across Europe* (2004).

Olivier D. and Chiffelle J., *Identity Revolution: Multi-Disciplinary Perspectives* (2009).

Olsen N., *Biometrics Laws and Privacy Policies*, 2019, PrivacyPolicies.Com, available at https://www.privacypolicies.com/blog/privacy-policy-biometrics-laws/ (last visited 7 July 2019].

Ortiz-Ospina E., *The Rise of Social Media*, 2019, available at https://ourworldindata.org/rise-of-social-media (last visited 1 December 2019).

Pasztor A. and Wall R., *Drone Regulators Struggle to Keep Up With the Rapidly Growing Technology*, 2016, Wall Street Journal, available at https://www.wsj.com/articles/drone-regulators-struggle-to-keep-up-with-the-rapidly-growing-technology-1468202371 (last visited 5 November 2019].

Peacock M.C., Miller S.E. and Pérez D.R., *A Proposed Framework for Evidence-Based Regulation* (2018].

Picker, 'Competition and Privacy in Web 2.0 and the Cloud', *John M. Olin Law & Economics Working Paper No. 414* (2008].

Porter D., *Data Ownership in the Cloud – How Does It Affect You?*, 2016, available at https://www.getfilecloud.com/blog/2016/11/data-ownership-in-the-cloud-how-does-it-affect-you/#.Xek8eZNKjIU (last visited 5 December 2019).

Poster M., *The Mode of Information: Poststructuralism and Social Context* (1st ed., 1990).

Poullet, 'About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation?', in S. Gutwirth, Y. Poullet and P. De Hert (eds.), *Data Protection in a Profiled World* (2010).

Rheingold, 'The Virtual Community: Homesteading on the Electronic Frontier', (2000).

Rodota, 'Data Protection as a Fundamental Right', in S. Gutwirth et al. (eds.), *Reinventing Data Protection?* (2009).

Roosendaal, 'Facebook Tracks and Traces Everyone: Like This!', *Tilburg Law School Legal Studies Research Paper Series No. 03/2011* (2010) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1717563.

Roosendaal, 'We Are All Connected to Facebook...by Facebook!', in S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?* (2012).

Rundle, 'International Personal Data Protection and Digital Identity Management Tools', *Berkman Center Research Publication No. 2006-06* (2006) , available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=911607.

Schünemann W.J. and Baumann M.-O., *Privacy, Data Protection and Cybersecurity in Europe* (2017).

Sharma N., *India's among the World's Top Three Surveillance States*, 2019, Quartz India, available at https://qz.com/india/1728927/indias-among-the-worlds-top-three-surveillance-states/ (last visited 7 December 2019].

Shave, 'Privacy and Security in Our Complex Digital World (Online)', *IQ: The RIM Quarterly* (2016] , available at https://search.informit.com.au/documentSummary;dn=049096323490954;res=IELAPA.

van der Sloot, 'Privacy as Human Flourishing: Could a Shift towards Virtue Ethics Strengthen Privacy Protection in the Age of Big Data?', 5 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* (2014] , available at https://www.jipitec.eu/issues/jipitec-5-3-2014/4097/sloot.pdf.

Sluijs, Larouche, and Sauter, 'Cloud Computing in the EU Policy Sphere Interoperability, Vertical Integration and the Internal Market', *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2012].

Solove, 'Conceptualizing Privacy', 90 *California Law Review* (2002] , available at http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2.

Solove D.J., *The Digital Person: Technology and Privacy in the Information Age* (2004], New York University Press.

Standage T., *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers* (2 (revised, 2014].

Steeves, 'Young Canadians in a Wired World, Phase III: Life Online', *MediaSmarts* (2014].

Stefanick L., *Controling Knowledge: Freedom of Information and Privacy Protection in a Networked World* (2011].

Stern G., *Can Regulators Keep Up with Fintech?*, 2017, available at https://insights.som.yale.edu/insights/can-regulators-keep-up-with-fintech (last visited 7 September 2019).

Strahilevitz, 'A Social Networks Theory of Privacy', *The University of Chicago Law Review* (2005).

Svantesson D.J., *Extraterritoriality in Data Privacy Law* (2013).

Tamò and George, 'Oblivion, Erasure and Forgetting in the Digital Age', 5 *Journal of Intellectual Property, Information Technology and E-Commerce Law* (2014) , available at http://www.jipitec.eu/issues/jipitec-5-2-2014/3997.

Taylor, 'No Privacy without Transparency', in R. Leenes et al. (eds.), *Data Protection and Privacy: The Age of Intelligent Machines* (2017).

de Terwangne, 'The Right to Be Forgotten and Informational Autonomy in the Digital Environment', in A. Ghezzi, Â. Guimarães Pereira and L. Vesnić-Alujević (eds.), *The Ethics of Memory in a Digital Age: Interrogating the Right to Be Forgotten* (2014).

Tsai P., *Data Snapshot: Biometrics in the Workplace Commonplace, but Are They Secure?*, 2018, Spiceworks, available at https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure (last visited 9 September 2019].

Tufekci, 'Big Questions for Social Media Big Data: Representativeness, Validity and Other Methodological Pitfalls', *Proceedings of the Eighth International AAAI Conference on Weblogs and Social Media* (2014] , available at https://www.aaai.org/ocs/index.php/ICWSM/ICWSM14/paper/view/8062/8151.

Tufekci, 'Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites', *Bulletin of Science, Technology & Society* (2008].

UK Information Commissioner's Office (UK ICO), *Consultation GDPR Consent Guidance*, 2017, available at https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf (last visited 23 November 2019).

Ustaran, 'The Scope of Application of EU Data Protection Law and Its Extraterritorial Reach', in *Beyond Data Protection:Strategic Case Studies and Practical Guidance* (2013).

Vaidhyanathan S., *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (2018).

Vandekerckhove B., *Protecting Data Flow in Shifting Privacy Regulations*, 2019, Security Boulevard, available at https://securityboulevard.com/2019/06/protecting-data-flow-in-shifting-privacy-regulations/ (last visited 14 December 2019].

Venier S. and Mordini E., Competitiveness and Innovation Framework Programme: ICT Policy Support Programme (ICT PSP), 2011.

Vervaele, 'Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?', in S. Gutwirth, R. Leenes and P. De Hert (eds.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges* (2014).

Wallace P., *The Psychology of the Internet* (1999].

Warren, , Brandeis, 'The Right to Privacy', in F. D. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology* (1984).

Warren and Brandeis, 'The Right to Privacy', 4 *Harvard Law Review* (1890] , available at http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C%0D.

Weber, 'The Right to Be Forgotten: More than a Pandora's Box?', 2 *JIPITEC* (2011].

Weiser, 'The Functions of Internet Use and Their Social and Psychological Consequences', *CyberPsychology & Behavior* (2001].

Wessler N.F., *A Federal Court Sounds the Alarm on the Privacy Harms of Face Recognition Technology*, 2019, ACLU, available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/federal-court-sounds-alarm-privacy-harms-face/ (last visited 5 September 2019).

Whitney L., *Apple to Refund at Least $32.5M for Kids' in-App Purchases*, 2014, available at https://www.cnet.com/news/apple-to-refund-at-least-32-5m-for-kids-in-app-purchases/ (last visited 25 November 2019].

Williams A., *Here I Am Taking My Own Picture*, 2006, New York Times, available at https://www.nytimes.com/2006/02/19/fashion/sundaystyles/here-i-am-taking-my-own-picture.html (last visited 6 December 2019).

Yamanouchi K., *Fingerprints, Facial Scans Becoming More Commonplace at Airports*, available at https://www.thestar.com.my/tech/tech-news/2018/04/12/fingerprints-facial-scans-becoming-more-commonplace-at-airports (last visited 9 November 2019].

Zanfir, 'The Right to Data Portability in the Context of the EU Data Protection Reform', *International Data Privacy Law* (2012].

Zarsky, 'Responding to the Inevitable Outcomes of Profiling: Recent Lessons from Consumer Financial Markets, and Beyond', in S. Gutwirth, Y. Poullet and P. De Hert (eds.), *Data Protection in a Profiled World* (2010).

Zeng, 'Research on Privacy Protection in Big Data Environment', *Journal of Engineering Research and Applications* (2015].

Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization', *Journal of Information Technology* (2015] , available at http://dx.doi.org/10.1057/jit.2015.5.

Арсовска Б., *Кина Воведува Застражувачки Надзор На Луѓето, Животот Ќе Зависи Од Поени*, 2018, available at https://www.fakulteti.mk/news/21092018/kina-voveduva-zastrashuvachki-nadzor-na-lugjeto-zhivotot-kje-zavisi-od-poeni (last visited 8 November 2019).

Гроздановски Т., *Како Ќе Функционира Оценувањето На Жителите Во Кина?*, 2017, available at https://www.fakulteti.mk/news/17-12-04/kako_kje_funkcionira_ocenuvanjeto_na_zhitelite_vo_kina (last visited 8 November 2019].

Ѓуркова, 'Правото На Приватен Живот и Правото На Заштита На Лични Податоци Во Европското Законодавство Во Судир Со Националната Безбедност', *Правник Бр.239* (2012].

Доревски Ѓ., 'Пресметување Во Облак и Миграција На Апликации - Анализа и Споредба' (2017] ( Универзитет „Св. Климент Охридски" - Битола/available at http://www.fikt.uklo.edu.mk/assets/uploads/2017/11/Dorevski-Gjoko-17-09-magisterski-trud.pdf].

Macmanus R., *A Guide to Recommender Systems*, 2009, available at https://readwrite.com/2009/01/26/recommender_systems/ (last visited 20 March 2019).

Мидрак Р., *Што е Препознавање На Лицето?*, 2019, EYewated, available at https://mk.eyewated.com/што-е-препознавање-на-лицето/ (last visited 15 December 2019].

Мидрак Р.Л., *Што е Data Mining?*, EYewated, available at https://mk.eyewated.com/што-е-data-mining/ (last visited 15 December 2019).

Митевска М., *Видео Надзор Само За Безбедност, Во Спротивно Нема Приватност*, 2019, Радио Слободна Европа, available at https://www.slobodnaevropa.mk/a/30297066.html (last visited 5 December 2019].

Наумовски Г. et al., *Право На Инфоратичка Технологија* (2013].

Наумовски Г. and Рашковски Д., *Право и Информатичка Технологија* (2019].

Оргера С., *Што е Веб Прелистувач?*, EYewated, available at https://mk.eyewated.com/што-е-веб-прелистувач/ (last visited 15 December 2019).

Стојановска Е. and Ананиевска Ј., *Приватност,Информирање,и Јавниот Интерес: Правото На Приватност Наспроти Правото На Јавноста Да Знае*.

Тошкова Д., Водич За Заштита На Личните Податоци, 2018.

*Article 29 Data Protection Working Party Guidelines on the Right to Data Portability*, 2017, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

*Case C-131/12 Google Spain SL and Google Inc. v. Agencia Espanola de Protección de Datos (AEPD), Mario Costeja González*, 2014, available at http://curia.europa.eu/juris/liste.jsf?num=C-131/12.

*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, 1981, available at https://rm.coe.int/1680078b37.

*Directive 95/46/EC*, 1995, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046.

*Discussion Paper on Data Portability: Personal Data Protection Commission In Collaboration with Competition and Consumer Commission of Singapore*, 2019, available at https://www.cccs.gov.sg/resources/publications/occasional-research-papers/pdpc-cccs-data-portability (last visited 4 December 2019].

*Does Facebook Really Not Sell Your Data to Advertisers?*, 2018, Thejournal.Ie, available at https://www.thejournal.ie/mark-zuckerberg-facebook-sell-data-3957290-Apr2018/ (last visited 13 November 2019).

*European Commission Working Paper SEC(2012) 72 Final*, 2012, available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN (last visited 15 October 2019].

*European Convention on Human Rights*, 1950, available at https://www.echr.coe.int/Documents/Convention_ENG.pdf.

*Final Report of the Federal Trade Commission Advisory Committee on Online Access and Security*, 2000, available at https://govinfo.library.unt.edu/acoas/papers/finalreport.htm (last visited 28 November 2019).

*First Report on the Implementation of the Data Protection Directive (95/46/EC) COM(2003) 265 Final*

(2003), available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0265:FIN:EN:PDF.

*GDPR: Show Me the Data*, 2017, Pega, available at https://www.pega.com/gdpr-survey (last visited 7 December 2019].

*Handbook on European Data Protection Law* (2014], available at https://fra.europa.eu.

*NT 1 & NT 2 v Google LLC [2018] EWHC 799 (QB)*, 2018, available at http://www.bailii.org/ew/cases/EWHC/QB/2018/799.html.

*Patel v. Facebook, Inc., No. 18-15982 (9th Cir. 2019)-JD*, 2019, available at https://law.justia.com/cases/federal/appellate-courts/ca9/18-15982/18-15982-2019-08-08.html.

*Privacy Advocates Statement on NTIA Facial Recognition Process FINAL*, 2015, available at https://www.documentcloud.org/documents/2104377-privacy-advocates-statement-on-ntia-facial.html (last visited 7 July 2019).

'Problems with the EU's Proposed 'Right to Be Forgotten'', *Info Security* (2012) , available at https://www.infosecurity-magazine.com/news/problems-with-the-eus-proposed-right-to-be/.

*Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to Processing of Personal Data on the Free Movement on Such Data (General Data Protection Regulation) COM/2012/011 Final - 2012/0011 (COD)*, 2012, available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012PC0011 (last visited 10 January 2019].

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Da, OJ L 119, 2016.

*The Universal Declaration of Human Rights*, 1948, available at https://www.un.org/en/universal-declaration-human-rights/.

*United Kingdom ("UK") Information Commissioner's Office – Guide to General Data Protection Regulation (GDPR) /Individuals Rights / Right to Data Portability*, available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/ (last visited 4 December 2019).

*United Nations Conference on Trade and Development, "Data Protection Regulations and International Data Flows: Implications for Trade and Development"*, 2016, available at https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf (last visited 10 December 2019].

*United Nations Conference on Trade and Development 'Data Protection and Privacy Legislation Worldwide'*, available at https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (last visited 7 November 2019).

*VON HANNOVER v. GERMANY (Application No. 59320/00)*, 2004, available at https://hudoc.echr.coe.int/eng#%7B%22itemid%22:[%22001-61853%22]%7D.

*Кина Го Гради Најмоќниот Систем За Препознавање Лице Во Светот*, 2019, Studenti.Mk, available at https://studenti.mk/kina-go-gradi-najmokjniot-sistem-za-prepoznavanje-lice-vo-svetot/ (last

visited 5 November 2019].

*Прирачник За Европското Законодавство За Заштита На Податоците* (2016].

*Прирачник За Информатичка и Комуникациска Технологија*, available at http://aa.mk/WBStorage/Files/Priracnik IKT Mak.pdf (last visited 1 January 2019).