Ана В. Човић[1]
Институт за упоредно право
Београд (Србија)

342.726:616-052
351.77:[616.98:578.834
Оригинални научни рад
Примљен 08/07/2020
Прихваћен 15/08/2020
doi: 10.5937/socpreg54-27284

ПРАВО НА ПРИВАТНОСТ И ЗАШТИТА ЛИЧНИХ ПОДАТАКА У ДОБА ПАНДЕМИЈЕ COVID-19

Сажетак: Током пандемије вируса COVID-19 појединци и друштво у целини примарно су се суочили са изазовима у области очувања здравља, физичког и менталног, али и са низом других проблема који су проузроковани вирусом и различитим мерама које су се, пре свега, односиле на ограничење слободе кретања и окупљања. Осим здравствених аспеката глобалне пандемије и њеног утицаја на светску привреду и економију, изузетно су значајни социолошки и правни аспекти, посебно у области поштовања и заштите зајемчених људских права као једног од основних постулата савременог демократског друштва. Када и у ком обиму је њихово ограничење оправдано и сврсисходно и где се налазе границе деловања државне власти и њених представника у ситуацијама када се пред њих ставља обавеза заштите опште безбедности и јавног здравља становништва, питања су која су одувек изазивала бројне полемике и опречна мишљења. Данас појединци, различите невладине, регионалне и светске организације покушавају да одговоре на питање да ли је током периода за нама човек као централни субјект правне заштите био виђен очима поштовања, саосећања и љубави оних којима је поверио да у његово име доносе одлуке или је људско достојанство слободног човека жртвовано зарад политичких и финансијских интереса појединаца и одређених интересних група. Живот у дигиталној ери и убрзани развој дигиталних технологија актуелизовали су питање заштите приватности и личних података, нарочито у периоду последње глобалне пандемије и појаве мобилних апликација за праћење контаката оболелих. Ово је поставило питање усаглашености њихове употребе са правном регулативом на међународном и националном плану у области заштите људских права.

Кључне речи: COVID-19, људска права, право на приватност, заштита личних података, пандемија, ванредно стање

[1] tankosicana@yahoo.com

Увод

Глобална пандемија вируса COVID-19 јединствена је у досадашњој историји, у погледу обима, односно броја држава које су њом биле погођене у истом временском периоду, као и у погледу њеног утицаја на различите сегменте и области друштвеног живота од којих су неке: утицај на породично окружење и односе међу члановима заједничког домаћинства; промене у пословању привредних субјеката и запослених у њима; увођење образовања деце путем интернет и телевизијских платформи; утицај на креирање медијске политике уз предлагање цензурисања одређених интернет садржаја; ограничење и забрана друштвених контаката увођењем изолације и самоизолације због чега је порастао број људи са симптомима депресије, изазване осећајем беспомоћности, посебно међу старијом популацијом; изазови у фукционисању здравственог и фармацеутског сектора.

Вишевековне борбе, револуције, ратови и животи појединаца посвећених идејама о човеку који својим рођењем заслужује да се развија и живи као слободан грађанин и слободно духовно биће, претходили су извојеваним победама на пољу признања и заштите људских права од стране држава и међународних организација. Људска права представљају неизоставан елемент савремених устава и бројних закона, као и предмет великог броја ратификованих међународних конвенција. Њиховом судском заштитом пред националним судовима не исцрпљују се средства утврђивања евентуалне повреде, јер након реализације свих правних лекова у унутрашњем праву постоји могућност обраћања Европском суду за људска права у Стразбуру. Број представки упућен Европском суду потврђује, с једне стране, препознавање значаја заштите заједмчених права од стране подносиоца представки и њихову свест о постојању и садржини права која им припадају, а с друге стране указује на бројне пропусте у унутрашњим правним системима држава потписница Европске конвенције о људским правима. Овај други показатељ представља разлог за забринутост, јер потврђује да се заједмчене права и слободе често не поштују, као и да судови нису увек дорасли улози која им према слову устава и закона припада. Тако се дешава да закони остају тек празна реч на папиру – правни основ за вишегодишње тражење правде и скупе поступке којима се излажу они најупорнији који ипак одлуче да личну сатисфакцију у виду пресуде и накнаде прузроковане штете пронађу пред судском инстанцом ван граница своје земље. У државама које немају потпуно поверење грађана, јер нису ефикасне и успешне у обезбеђивању и заштити људских права у мирнодопским условима и онда када не постоји општа опасност или ситуација која захтева процену потребе и обима њиховог ограничења, за време ванредних догађаја и околности неповерење људи значајно расте. Тада се дешава да одлуке државних органа, и онда када су потпуно оправдане и сразмерне, често наилазе на осуду, процењивање, преиспитивање, а отвара се и широк простор за изношење различитих теорија завере које људима, услед сумње у искреност и намере доносиоца одлука, почињу да делују реално и могуће. Тако је у приватним разговорима, али и у медијима, граница између оправданих мера, које се предузимају из најдубље бриге према човеку као појединцу и друштву у целини, и социјалног експеримента у коме смо узели учешће мимо своје воље, постала врло танка, скоро па неприметна, као да зрно сумње никог не заобилази.

Не треба заборавити да се, иако људска права произилазе из природног права, обим њихове заштите мењао током историје. Стога, ниво зајемчених људских права и слобода није нешто непроменљиво и та промена у пракси може да се одвија у два правца – у правцу њиховог унапређења, али и у правцу укидања или смањивања одређеног достигнутог нивоа права, упркос недвосмисленој законској забрани да се то чини. Право на приватност и заштиту личних података последњих година је препознато као право које захтева унапређење механизама заштите услед убрзаног развоја дигиталних технологија, што се огледа у усвајању бројних правних докумената у овој области, на међународном и националном нивоу држава. Важно је уочити који су били изазови у области заштите ових права током пандемије и указати на њих због неких будућих, сличних или сложенијих ситуација, које се тренутно не могу предвидети.

Европски правни оквир за заштиту личних података и права на приватност

У члану 5. Европске конвенције о људским правима јемчи се право на слободу и сигурност. У ставу 1 се наводи да свако има право на слободу и сигурност личности, те да нико не може бити лишен слободе осим у случајевима предвиђеним Конвенцијом и у складу са законом одређеним поступком. Законито лишење слободе ради спречавања ширења заразних болести један је од случајева у којима Конвенција предвиђа одступање од права из члана 5.[2]

Члан 8. прописује право сваког на поштовање свог приватног и породичног живота, свог дома и преписке, као и обавезу јавних власти да се не мешају у остваривање овог права, осим ако је то у складу са законом и неопходно у демократском друштву у интересу националне сигурности, јавне сигурности или економске добробити земље, ради спречавања нереда или криминала, заштите здравља или морала, права и слобода других.

У члану 15. се прецизира да у време рата или друге ванредне ситуације која прети животу нације, свака висока уговорна страна може предузети мере одступања од својих обавеза из ове Конвенције у мери коју строго захтевају потребе ситуације, под условом да такве мере нису у супротности са њеним другим обавезама по међународном праву. Није дозвољено одступање од члана 2. (право на живот), осим у случају смрти која је последица законитих ратних дела или члана 3. (забрана мучења), члана 4. став 1. (забрана ропства и принудног рада) и члана 7. (кажњавање само на основу закона). Свака висока уговорна страна која се користи овим правом изузећа обавештава генералног секретара Савета Европе у потпуности о свим мерама које је предузела и разлозима за то, а такође је у обавези да обавести генералног секретара Савета Европе када такве мере престану да делују и одредбе Конвенције почну поново да се спроводе у потпуности. Члан 15. је сличан члану 4. Међународног пакта о грађанским и политичким правима и члану 27. Америчке конвенције о људским правима. Многи устави такође садрже сличне одредбе за проглашавање ванредне ситуације. Члан 15. тако омогућава државама да предузимају мере које не би биле дозвољене у складу са уобичајеним

[2] Закон о ратификацији Европске конвенције за заштиту људских права и основних слобода, *Službeni list Srbije i Crne Gore – međunarodni ugovori*, br. 9/2003, 5/2005 i 7/2005 – kor. i *Službeni glasnik RS – Međunarodni ugovori*, br. 12/2010 i 10/2015.

критеријумима Конвенције и у том погледу су опасности које ванредна стања представљају за људска права очигледне. Због тога се чланом 17. прописује забрана злоупотребе права, те се наводи да се ништа у Конвенцији не може тумачити тако да подразумева право било које државе, групе или особе да се бави било којом активношћу или врши било које дело које има за циљ поништење неког од наведених права и слобода или њихово ограничење у већој мери од онога што је предвиђено Конвенцијом. У члану 18. се наводи да се ограничења наведених права и слобода, дозвољена Конвенцијом, не примењују у друге сврхе осим оних за које су прописана.

Члан 17. Међународног пакта о грађанским и политичким правима, који произилази из члана 12. Универзалне декларације о људским правима, успоставља заштиту од „произвољног или незаконитог уплитања" у „приватност, породицу, дом или преписку појединца."

У овој области је значајна и Конвенција о заштити лица у односу на аутоматску обраду личних података[3], која у члану 6. утврђује да се лични подаци у вези са расним пореклом, политичким опредељењем, верским убеђењем или неком другом врстом убеђења, као и лични подаци у вези са здравственим стањем или сексуалним животом могу аутоматски обрађивати само у случају да домаће законодавство предвиђа одговарајуће гаранције за то. Исто важи и за личне податке из казнене евиденције. Свих 47 земаља Савета Европе су стране у овој Конвенцији (Конвенција 108), која је отворена и за државе које нису чланице Савета Европе. Она је ажурирана 2018. године (данас је позната као 108+) и њу су потписале све државе Савета Европе. Наша држава је 26. маја 2020. године ратификовала Протокол Савета Европе од 18. маја 2018. године, којим се предметна Конвенција унапређује у погледу начела пропорционалности, законитости и транспарентности (Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.223).

Европска унија је ажурирала законодавство о заштити података 2016. године доношењем Опште уредбе о заштити података о личности (Уредба (ЕУ) 2016/679 ГДПР) и Директиве о заштити физичких лица у вези са обрадом података о личности, која су повезана са кривичним делима или извршењем кривичних санкција (ЕУ) 2016/680.[4] Уредба (ЕУ) 2016/679 у члану 9. прописује да подаци о здравственом стању представљају посебну категорију података о личности, чија обрада није допуштена, осим у тачно одређеним случајевима међу којима је и јавни интерес у области јавног здравља, као што је заштита од озбиљних прекограничних претњи за здравље или обезбеђивање високих стандарда квалитета и безбедности здравствене заштите, лекова и медицинских средстава.[5] Поштујући принцип законитости, обрада личних података мора

[3] *Službeni glasnik RS – Međunarodni ugovori*, br. 1/92, *Službeni list SCG – Međunarodni ugovori*, br. 11/2005 – dr. zakon и *Službeni glasnik RS – Međunarodni ugovori*, br. 98/2008 – dr. zakon i 12/2010).

[4] Directive EU 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[5] 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.

да се заснива на сагласности субјекта података или на другим законским основама које су утврђене у Уредби (члан 6.), што у време пандемије и креирања апликација за праћење контаката заснованих на близини доводи до питања да ли се такве апликације и њихово коришћење могу ослањати на пристанак. Бивша радна група изнела је став да „ако се сагласност састави као део одредаба и услова који се не преговарају, претпоставља се да нису слободно дати" (Члан 29, Смернице за сагласност, 2018), што значи да се добровољно учешће у апликацијама за тражење контаката не мора нужно ослањати на пристанак као правни основ за обраду података (Guild, Mendos Kuskonmaz, 2020). Општа уредба о заштити података о личности (ЕУ) 2016/679 нема механизме за ефикасну заштиту од коришћења анонимних података за предиктивно алгоритамско одлучивање, оцењивање ризика и класификацију засновану на понашању, које се могу користити за неједнако третирање појединаца или група (Mühlhoff, 2020).

Европски одбор за заштиту података издао је Упутство о обради података о личности у контексту вируса COVID-19 (Statement on the processing of personal data in the context of the COVID-19 outbreak)[6], у коме се јасно указује на значај заштите података о личности и током ванредног стања.

Национални правни оквир за заштиту личних података и права на приватност

Наша приватност обухвата податке који се односе на наше брачно стање, верска и политичка убеђења, новчане трансакције, етничко порекло, здравствено стање, криминални досије, генетски материјал. Данас када живимо у добу убрзаног напретка и развоја дигиталних технологија које прожимају сваки аспект нашег породичног, пословног и друштвеног живота, заштита приватних података од јавности и контролисање њихових токова добијају једну нову димензију. То значи да је неопходно да знамо не само са ким ми делимо наше податке, него и ко је овлашћен да их прикупља и у које сврхе. Законодавац је препознао ову област као једну од суштинског значаја у последњој деценији, што је за последицу имало усвајање посебних закона којима се регулише заштита и остваривање овог права. Бројне друштвене мреже, финансијске трансакције и плаћања путем интернета, и друге активности којима приступамо у виртуелном свету, учинили су да појединац и његова приватност у сајбер простору лако могу бити угрожени на различите начине – од прислушкивања, ширења вируса, изложености вербалном насиљу, до крађе идентитета.

Све одредбе о људским и мањинским правима тумаче се у корист унапређења вредности демократског друштва и у складу са важећим међународним стандардима и праксом међународних институција у овој области. Члан 18. Устава Републике Србије („Сл. гласник РС", бр. 98/2006) прописује да се људска и мањинска права зајемчена Уставом примењују непосредно, док се законом може прописати само начин њиховог остварења када је то Уставом изричито предвиђено или када је неопходно због природе појединог права, када се ни у ком случају не сме

[6] Statement on the processing of personal data in the context of the COVID-19 outbreak https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en, 29.05.2020.

утицати на његову садржину. Ограничења ових права су допуштена законом, у случајевима и у обиму који то Устав предвиђа, без задирања у њихову суштину, а достигнути ниво људских и мањинских права се не може смањивати (чл. 20. Устава РС). У истом члану се наводи да су сви државни органи, а посебно судови, дужни да у овим ситуацијама воде рачуна да ли постоји сразмера између ограничења права и сврхе, односно да ли се сврха могла остварити и мањим ограничењем. Право је сваког грађанина да захтева судску заштиту и уклањање последица које су том приликом настале, уколико сматра да му је повређено или ускраћено право зајемчено Уставом, а на располагању му стоји и могућност обраћања међународним институцијама.

Неповредивост тајне писама и других средстава комуницарања је неповредива и заштићена чланом 41, а заштита података о личности се јемчи чланом 42. Прописује се да је забрањена и кажњива употреба података о личности изван сврхе за коју су прикупљени, у складу са законом, осим за потребе вођења кривичног поступка или заштите безбедности државе, на начин предвиђен законом. Такође, утврђује се право сваке особе да буде обавештена о прикупљеним подацима о својој личности, као и право на судску заштиту у случају њихове злоупотребе.

Одступања од зајемчених права су дозвољена за време ванредног стања или ратног стања у обиму у којем је то неопходно, а престају престанком ванредног или ратног стања (члан 202. Устава РС). Члан 200. Устава прописује услове и поступак за проглашење и престанак ванредног стања.[7] Дана 15. марта 2020. године на територији Републике Србије председник Републике, председник Народне скупштине и председник Владе донели су Одлуку о проглашењу ванредног стања,[8] које је на снази било до 6. маја 2020. године када је Одлуком Народне скупштине укинуто.[9] Члан 53. Закона о заштити становништва од заразних болести („Сл. гласник 15/2016. и 68/2020), предвиђа да министар здравља може, на предлог Комисије и института, наложити забрану или ограничење кретања становништва на подручју које је зах-

[7] Ванредно стање проглашава Народна скупштина у ситуацији када јавна опасност угрожава опстанак државе или грађана, а одлука о његовом увођењу важи најдуже 90 дана, након чега се може продужити за још 90 дана одлуком већине од укупног броја посланика. Том приликом Народна скупштина може прописати мере којима се одступа од Уставом зајемчених људских и мањинских права. Ако Народна скупштина није у могућности да се састане, одлуку о проглашењу ванредног стања доносе заједно председник Републике, председник Народне скупштине и председник Владе, под истим условима, а мере којима се одступа од људских и мањинских права може прописати Влада, уредбом, уз супотпис председника Републике. У том случају, одлуку о ванредном стању треба да потврди Народна скупштина у року од 48 сати од њеног доношења, односно чим буде у могућности да се састане. Ако Народна скупштина не потврди одлуку, она престаје да важи завршетком прве седнице Народне скупштине одржане по проглашењу ванредног стања. Исто важи и за уредбу Владе о мерама одступања од људских и мањинских права. Влада је дужна да је поднесе на потврду Народној скупштини у року од 48 сати од доношења, односно чим Народна скупштина буде у могућности да се састане, а у супротном, мере одступања престају да важе 24 сата од почетка прве седнице Народне скупштине одржане након проглашења ванредног стања.

[8] *Službeni glasnik RS*, br. 29/2020.

[9] *Službeni glasnik RS*, br 65/2020.

ваћено одређеном заразном болешћу. На основу тога је 10. марта 2020. године Влада РС донела одлуку којом је COVID-19 проглашен заразном болешћу.[10]

У Закону о заштити података о личности („Службени гласник РС", бр. 87/2018), подаци о здравственом стању се дефинишу као посебни подаци о личности и њихова обрада је регулисана чланом 17. у коме се таксативно наводе ситуације у којима је обрада ових података допуштена. Тако се у ставу 1. наводи да је неопходан изричит пристанак лица на које се подаци односе, осим ако је законом прописано да се обрада не врши на основу пристанка, а у ставу 9. се утврђује допуштеност обраде када је неопходна у циљу остваривања јавног интереса у области јавног здравља, као што је заштита од озбиљних прекограничних претњи здрављу становништва или обезбеђивање високих стандарда квалитета и сигурности здравствене заштите, лекова или медицинских средстава. Члан 18. прецизира да је обрада коју врше надлежни органи у посебне сврхе, којом се открива расно или етничко порекло, политичко мишљење, верско или филозофско уверење или чланство у синдикату, као и обрада генетских података, биометријских података у циљу јединствене идентификације физичког лица, података о здравственом стању или података о сексуалном животу или сексуалној оријентацији физичког лица, допуштена само ако је то неопходно, уз примену одговарајућих мера заштите права лица на које се подаци односе.

Додатне смернице за поступање у доба пандемије COVID-19 налазе се и у заједничком саопштењу председавајуће Комитета Конвенције 108 и Комесара за заштиту података Савета Европе од 30. марта 2020. године, у коме се истиче да државе током пандемије треба да обрате пажњу да ли и у ком обиму предузете мере утичу на демократију, владавину права и поштовање људска права, укључујући и права на приватност и заштиту података о личности.[11] Наглашава се да је, у новонасталим околностима, потребно посебно обратити пажњу на обраду података у вези са здрављем становништва и да Препорука CM/Rec(2019)2 о здравственим подацима (Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data) садржи смернице о остваривању права на приватност и заштиту података о личности, између самих здравствених радника, али и између здравственог и других сектора. С тим у вези, не треба објављивати осетљиве податаке о личности (нпр. здравствене податаке), а радње које се тичу обраде треба вршити само ако су обезбеђене посебне, додатне техничке и организационе мере

[10] Уредбом о мерама у ванредном стању (*Službeni glasnik RS*, br. 31/2020-3 од 16. марта 2020) ограничено је и спречено кретање људи са овим вирусом, као и особа за које постоји сумња да су заражене; забрањено је одржавање скупова на отвореном и ограничено је у затвореном простору; Министарству унутрашњих послова омогућено је да изврши наредбу за затварање свих прилаза одређеном објекту или простору и онемогућавање напуштања истих. Наредбом о ограничењу и забрани кретања лица на територији Републике Србије (*Službeni glansik RS*, br. 34/2020, 39/2020, 40/2020, 46/2020 и 50/2020) уведена је забрана кретања у периоду дужем од 24 сата за сва лица на територији државе, што је поставило питање оправданости мере која није представљала ограничење права кретања, већ његово потпуно укидање.

[11] Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, Strasbourg, 30 March 2020, https://rm.coe.int/covid19-joint-statement/16809e09f4

заштите. Као најважнији изазов у масовној обради података о личности, ради спречавања ширења пандемије, препознају се следећи ризици:

– могућност поновне идентификације лица на основу претходно анонимних података;
– могућност обраде података од стране послодаваца током трајања пандемије, због чега послодавци треба да обрађују само оне податке о личности који су неопходни за идентификацију потенцијално оболелих, уз пуно поштовање принципа нужности, пропорционалности и одговорности. Државним органима би могли да открију неке податке о здравственом стању запослених, само уколико за то постоји одговарајући правни основ;
– телекомуникационе компаније, интернет платформе и интернет провајдери постају укључени у борбу против ширења COVID-19, што за последицу има да се од њих све чешће тражи достављање података својих корисника, како би се утврдила њихова геолокација. Закључује се да обрада ових података за већи број лица може да се врши само ако би, на основу валидних доказа, могла да допринесе престанку ширења пандемије, уз спречавање и минимизирање ризика остваривања права на приватност, односно вршењем оне радње из домена обраде која је најмање агресивна по остваривање права на приватност;
– приликом обраде података у образовним системима неопходно је да постоји одговарајући правни основ и сагласност родитеља или законског старатеља малолетних лица, као и могућност да родитељи имају увид у обраду података своје деце.

Јавно објављивање личних података о здравственом стању, без пристанка особа чији су подаци, представља кривично дело, будући да Закон о правима пацијената[12], Закон о здравственој заштити[13] и Закон о здравственој документацији и евиденцијама у области здравства[14] изричито забрањују такву обраду личних података, осим уз сагласност особе о којој је реч. Поред те сагласности, други ваљани основ могла би бити судска одлука, а све друго може представљати и кривично дело.

Уочени изазови током пандемије COVID-19 : мобилне апликације за праћење заражених

Може се рећи да је пандемија изазвана вирусом COVID-19 била изненадан, ненајављен и сложен тест провере знања и способности представника државних власти, а у исто време и тест поверења које (не) уживају међу својим грађанима. У борби против пандемије на велика врата се уводе мобилне апликације чија је делотворност под знаком питања, а које могу довести до кршења људских права ако немају ефикасне заштитне мере за заштиту приватности. Мобилне апликације чија би сврха била обавештавање корисника о њиховим контактима са појединцима позитивним на COVID-19 (и у ситуацији када особе нису знале да су потенцијално заражене) већ су имплементиране у неким азијским земљама (Сингапур, Кина, Тајван и

[12] *Službeni glasnik RS*, br. 45/2013, 25/2019.

[13] *Službeni glasnik RS*, br. 25/2019.

[14] *Službeni glasnik RS*, br. 123/2014, 106/2015, 105/2017, 25/2019.

Јужна Кореја), а око 14 држава чланица ЕУ иницирало је или разматра њихов развој (Lazarević, Bajić, 2020). Треба имати у виду да око 60% популације треба да инсталира апликацију како би она имала жељене резултате, као и да је социјално (не)поверење у државне институције у директној вези са исходом, односно успехом оваквих мобилних апликација (Lazarević, Bajić, 2020). BBC је 2017. године покренуо апликацију под називом 'BBC Pandemic' у оквиру националног експеримента у Великој Британији који је прикупљао податке добровољаца који су апликацију користили за процену како ће се заразна болест попут грипа проширити и утицати на људе у Великој Британији. На основу прикупљених података изграђен је математички модел који се односи на питања као што је стопа смртности, а документарни филм о експерименту је емитован 2018. године. Овај експеримент и сличне најаве великог вируса у непосредној прошлости, повећавају број различитих теорија завере и број њихових присталица.

Европски парламент је 17. априла усвојио резолуцију, захтевајући потпуну транспарентност како би људи могли проверити основни протокол за сигурност и приватност ових апликација (European Parliament resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)).

Када се говори о увођењу хитних мера, као што су мере надзора које су уведене у циљу сузбијања тероризма, сведоци смо да „оне често иду предалеко, не постижу жељени ефекат и када буду одобрене, често надмашују своје оправдање", закључују у организација Хјуман рајтс воч (Human Rights Watch, 2020). Циљ употребе ових мобилних апликација је праћење кретања заражених особа, идентификација особа са којима су ступали у контакт у периоду у којем су заражени, праћење поштовања мера карантина и социјалног дистанцирања, а захваљујући збирним подацима о локацији утврђују се актуелна жаришта вируса. На тај начин се може предвидети његово даље ширење и утврдити какав је резултат дотадашњих предузетих мера здравствене заштите. GPS мобилног телефона му омогућава да прати своју локацију на удаљености од метар и по до три метра, а многе апликације за паметне телефоне бележе податке о локацији које затим могу да добију владе и посредници података. С друге стране, блутут се користи за директно повезивање уређаја у непосредној близини ради преноса података (на удаљености до око десет метара), па се сматра бољим решењем, јер уместо локације прати директне интеракције са високим процентом тачности. Такође, подаци могу да се чувају локално на уређају, а не на централизованој бази података, што представља бољу опцију са аспекта заштите права на приватност.

У периоду од неколико месеци, организације за заштиту људских права у више држава су забележиле случајеве кршења права на приватност и заштиту личних података, у вези са употребом мобилних телефона и мобилних апликација.[15] Изра-

[15] У Израелу је уредба о ванредним ситуацијама, коју је влада одобрила 17. марта, овластила Shin Bet, израелску службу за унутрашњу безбедност, да без пристанка корисника прима, прикупља и обрађује „технолошке податке", укључујући податке о локацији, од компаније Telcos, како би се проценило који су грађани били изложени вирусу. Министарство здравља шаље упозорења на телефоне људи и наређује им да се ставе у карантин. Влада је заобишла парламент у одобравању уредбе о ванредним ситуацијама. Врховни суд Израела је касније пресудио да влада треба да донесе закон којим се ауторизује да „испуњава принципе заштите приватности".

жава се забринутост да програми за праћење мобилних телефона омогућавају владама да, услед недостатка транспарентности, прикупљају, користе и чувају податке изван онога што је неопходно за законите и циљане мере надзора болести, што је посебно забрињавајуће у земљама које имају евиденцију о свеобухватном надзору, попут Кине, Етиопије и Русије (у којој постоји комбинација података о мобилној локацији са другим врстама података, као што је препознавање лица) (Human Rights Watch, 2020).

Употреба мобилних апликација за праћење у условима пандемије, осим права на приватност и заштиту личних података, у директној је вези и са правом на слободу и безбедност. Члан 5. Европске конвенције о људским правима штити право на слободу и безбедност особе, али се дозвољава законито затварање особа ради спречавања ширења заразних болести. *Coronavirus Act 2020* у Великој Британији омогућио је полицајцима и имиграционим службеницима да притворе особу у ограниченом периоду уколико је заражена или да је одведу на одговарајуће место за скрининг и и процену. Велика Британија је увела мере затварања углавном кроз Одељак 45P Закона о јавном здравству (контрола болести) из 1984. године, а прописи предвиђају кривично дело за напуштање својих домова „без оправданог разлога" (Greene, 2020).[16]

У Кини је уведен нови систем под називом „Здравствени код" (Health Code) који користи велики број мобилних података и тачака геолокације, које прикупљају кинеске технолошке компаније како би се одредила жаришта. Апликација сваком од својих око 700 милиона корисника додељује једну од три боје: зелена омогућава неограничено кретање, жутој је потребно 7 дана карантина, а црвеној 14 дана карантина. Да би ушли у зграде, отишли до супермаркета, користили јавни превоз и кретали се по свом кварту, људи морају скенирати QR код на контролном

Парламент у Јерменији је 31. марта усвојио амандмане којима се властима дају широка овлашћења за надзор, које захтевају од компаније Telcos да преда телефонске записе свим својим купцима, укључујући телефонске бројеве и локацију, време и датум њихових позива и СМС порука. Власти могу да користе те податке за идентификовање појединаца који су заражени и треба да буду изоловани или који би требало да буду у карантину, или за надгледање појединаца у изолацији или карантину.

У Русији је премијер 20. марта наложио министарству комуникација да дизајнира национални систем за праћење људи који су били у контакту са пацијентима позитивним на коронавирус, користећи податке о локацији које пружају мобилни телефони. Министарство комуникација је 1. априла потврдило да је дизајнирало систем, а од регионалних власти се захтевало да доставе спискове бројева мобилних телефона особа заражених коронавирусом, као и телефонске бројеве грађана који су у карантину код куће зато што су путовали у иностранство или су имали контакт са зараженим људима.

У Еквадору је 16. марта председник издао уредбу којом је овластио владу да користи податке са сателитских и мобилних телефонских платформи за праћење људи који су тестирани позитивно на вирус, оних који су били у блиском контакту са неким ко је био позитиван, као и оних који имају симптоме и оних који су подвргнути обавезној изолацији због уласка у земљу из иностранства (Human Rights Watch, 2020).

[16] Европски суд за људска права је закључио да члан 5. само штити слободу у класичном смислу физичке слободе, али не даје право особи да ради оно што жели или иде тамо где жели *(P v Cheshire West & Chester Council*; *P & Q v Surrey County Council* [2014] UKSC19).

пункту (Human Rights Watch, 2020). Систем омогућава корисницима да пријаве незаконите или неовлашћене активности, као што су велика јавна окупљања. Ова апликација не служи само да би се имао увид у здравствено стање корисника, на основу чега се процењује да ли се они могу слободно кретати или не, већ је њена улога и у размени информација с полицијом, чиме се „поставља образац за нове облике аутоматизованих социјалних контрола које би могле да трају дуго након што епидемија нестане" (Sander, 2020, str. 2). У исто време, отвара се простор за дискриминацију одређених група, као на пример старијих грађана који нису вични руковању паметним телефонима и немају неопходна знања, те због непоседовања QR кода могу бити ускраћени за приступ јавном превозу, продавницама, здравственим установама.

У Јужној Кореји представници власти чине доступним јавности „текстове за безбедносне смернице" у којима се описују кретања људи којима је недавно дијагностикован вирус, без навођења њиховог имена, али уз личне податке као што су пол и старост, који са подацима о локацији могу учинити доступним неке детаље који се тичу њиховог приватног и породичног живота, што чини оправданим одређене бојазни о прелазу са биометријског надзора „преко коже" на надзор „испод коже" (Sander, 2020). Тако је могуће замислити да нека будућа пандемија буде оправдање за надгледање температуре и крвног притиска. Национална комисија за људска права Јужне Кореје критиковала је власти због пружања више информација него што је неопходно за заустављање ширења болести, што је довело до кршења приватности и људских права заражене особе, укључујући „секундарну штету, јер пацијенти постају мета критике, ругања и мржње на мрежи", те је уместо пружања историје путовања сваког појединца препоручено само дељење локације и времена када су заражени људи посећивали места (Human Rights Watch, 2020).

У Норвешкој је Национални институт за јавно здравље 16. априла покренуо добровољну апликацију за самоизвештавање у циљу надгледања кретања корисника и њиховог упућивања у карантин уколико су били изложени некоме ко је позитивно тестиран на коронавирус. Када се потврди да корисник има коронавирус, апликација преузима податке о својој локацији, шаље текстуалну поруку сваком другом кориснику који се налази више од 15 минута од те особе и упућује их да пређу у карантин (Human Rights Watch, 2020). Јавним здравственим агенцијама је од краја маја доступна заједничка Apple – Google технологија за праћење контаката, коју је прво имплементирала Швајцарска (апликација SwissCovid).

Док сведочимо убрзаном увођењу појачаног дигиталног надзора и сужавању простора права и слобода за које смо веровали да нам рођењем припадају, поставља се и питање научних доказа о ефикасности података до којих се долази путем мобилних апликација које се инсталирају, или ће се инсталирати, у циљу контроле вируса. Употреба таквих података може бити „несразмерна инвазија на право на информационо самоодређење" (Mühlhoff, 2020). Такође, ако се процес брзих иновација и измене законодавства у том правцу наставе тренутним темпом, резултат би могао имати дугорочне последице, због ширења алгоритмичких поступака за управљање популацијом. То би могло довести до употребе тих података приликом одлучивања ко ће имати приступ медицинским услугама, пословима, образовању, али и

до предвиђања нечијег лошег здравља – физичког и менталног, или потенцијалне претње по безбедност, чиме би се друштво поделило на невидљиве друштвене класе које би се другачије третирале у погледу приступа могућностима, ресурсима и информацијама (Mühlhoff, 2020).

Закључак

Владе не смеју да се мешају у право на приватност, уколико не могу да докажу да је мешање предвиђено законом, предузето ради легитимног циља (на пример, заштите јавног здравља) и да је неопходно и сразмерно постизању тог циља. Изузетно, строжа ограничења права могу се извршити дерогацијама (члан 4. Међународног пакта о грађанским и политичким правима и члан 15. Европске конвенције о људским правима), а државе могу одступити од права на приватност и слободу изражавања у време ванредне ситуације која угрожава живот нације. Међутим, одступања су дозвољена само у мери у којој су ове мере неопходне, уколико нису у супротности са другим обавезама међународног права и не укључују дискриминацију.

Не могу се прихватити аргументи да је садашњи режим правне заштите података неадекватан за тренутне изазове, нити се сме допустити да последица пандемије буде прихватање нижих стандарда заштите података и мање приватности (Guild, Mendos Kuskonmaz, 2020). Ово посебно ако имамо у виду да се велики број података налази у рукама влада од којих многе имају историју репресије и дискриминације према већ маргинализованим заједницама, укључујући верске заједнице и политичке дисиденте (Human Rights Watch, 2020). Осим ових, постоје и друга питања која захтевају одговоре у што краћем року, пре неке будуће пандемије или неког новог „таласа" који се већ најављује:

- пошто се тачност информација добијених путем блутут повезивања може смањити у присуству других уређаја за пренос сигнала, као и у зградама велике густине насељености или у парковима, питање је колико су такви подаци поуздани, нарочито у борби против вируса, ако се не може са сигурношћу знати да ли су људи били у затвореном простору или на отвореном, јесу ли носили маске или не, итд;
- према подацима организације Хјуман рајтс воч, жене имају око 31% мању могућност приступа интернету од мушкараца у неким земљама, а широм света око 327 милиона мање жена од мушкараца има паметни телефон, услед ниже писмености (од око 781 милиона људи старијих од 15 година који су неписмени, готово две трећине су жене и девојке). Уколико апликације за праћење постану услов за улазак у јавне или приватне просторе, маргинализована популација која је мање способна да преузме те апликације суочиће се са дискриминацијом, а међу њима и старија популација;
- разлике у употреби мобилних телефона, дигиталној писмености и технолошком прихвату могу такође искључити рањиву или маргинализовану популацију из јавних здравствених одговора који се неоправдано ослањају на праћење локације за мобилне уређаје, будући да се процењује чак две

милијарде корисника мобилних телефона поседује уређаје који нису конфигурисани за подршку овој технологији, што је око четвртина свих мобилних телефона који се данас користе (Human Rights Watch, 2020).

Полицијски час и ванредно стање се могу укинути, али не и последице које могу настати услед убрзаних и недовољно промишљених дигиталних новина. Због тога је овом проблему неопходно приступити уз предузимање неопходних мера заштите зајемчених људских права и укључивање свих релевантних субјеката, стручњака из области информационих технологија, али и правника, социолога и здравствених радника, како би се пронашао прихватљив модел у служби заштите јавног здравља и појединца, уз поштовање достигнутог нивоа људских права и слобода. У супротном, можда ризикујемо да у будућности постанемо друштво савршено здравих робова или робота, у коме питање замене QR кодова и различитих мобилних апликација масовним чиповањем постаје врло реална могућност.

Ana V. Čović[1]
Institute of Comparative Law
Belgrade (Serbia)

RIGHT TO PRIVACY AND PROTECTION OF PERSONAL DATA IN THE AGE OF THE COVID-19 PANDEMIC

(Translation In Extenso)

Abstract: During the COVID-19 virus pandemic, individuals and society as a whole faced primarily challenges in the field of health, physical and mental, but also a number of other problems caused by the virus and various measures mainly related to restriction of freedom of movement and freedom of assembly. Apart from the health aspects of the global pandemic and its impact on the world economy, the sociological and legal aspects are extremely important, especially in the field of respect and protection of guaranteed human rights as one of the basic postulates of modern democratic society. When and to what extent their restriction is justified and expedient, as well as the exact limits of action of the state government and its representatives in situations when they are obliged to protect the general safety and public health of the population, are issues that have always caused numerous controversies and conflicting opinions. Today, individuals, various non-governmental, regional and world organisations, are trying to answer the question whether during the past period man as a central subject of legal protection was seen through the eyes of respect, compassion and love of those whom he entrusted to make decisions on his behalf or whether the human dignity or a free man was sacrificed for the sake of political and financial interests of individuals and certain interest groups. Life in the digital era and the accelerated development of digital technologies have made the issue of privacy and personal data protection topical, especially in the period of the last global pandemic and the appearance of mobile applications for monitoring the contacts of patients. This raised the question of compliance of their use with legal regulations at the international and national level in the field of human rights protection.

Keywords: COVID-19, human rights, right to privacy, personal data protection, pandemic, state of emergency.

Introduction

The global COVID-19 pandemic is historically unprecedented in terms of scope and the number of countries simultaneously affected by it, as well as in terms of its impact on various segments and areas of social life, some of which are: impact on family environment

[1] tankosicana@yahoo.com

and interpersonal relations between members of the same households; changes in the operation of businesses and their employees; introduction of education via the internet and TV platforms; impact on shaping media policies with proposed censorship of certain internet content; restricted and prohibited social contacts by way of introducing isolation and self-isolation, as a result of which there has been an increase in the number of persons showing the symptoms of depression, caused by the feeling of helplessness, especially among the elderly population; challenges in terms of proper functioning of healthcare and pharmaceutical sectors.

Many centuries of struggle, revolutions, wars and the lives of individuals dedicated to ideas about man, who by being born into this world deserves to grow up and live as a free citizen and free spiritual being, preceded the accomplishment of victories in the area of recognising and protecting human rights by states and international organisations. Human rights represent an indispensable element of modern constitutions and numerous laws and are also the subject of a large number of ratified international conventions. The fact that human rights are protected before national courts does not exhaust the means for identifying possible breaches of such rights. Once all legal remedies have been exhausted locally, there is the possibility to refer particular cases to the European Court of Human Rights in Strasbourg. On the one hand, the number of applications submitted to the European Court confirms that the importance of protecting guaranteed human rights is recognised by submitting parties and also their awareness of the existence and content of the rights which belong to them. On the other hand, those applications indicate numerous lapses in national legal systems of the signatory states of the European Convention on Human Rights. The latter indicator is a cause for concern because it confirms that guaranteed rights and freedoms are often not upheld and also that courts are often no match for the role bestowed upon them according to the letter of law and constitution. Thus, it happens that the laws remain merely a dead letter – legal grounds for many years of seeking justice and expensive proceedings faced by the most persistent ones who nevertheless decide to seek personal satisfaction in the form of judgement and indemnification for incurred damage before the court outside their country. People's distrust grows substantially in countries which do not enjoy their citizens' trust, due to such countries being inefficient and unsuccessful in ensuring the protection of human rights in peacetime conditions and in situations when there is no general danger or situations which require assessment of the need for utilisation and scope of restrictions, when extraordinary events and circumstances occur. Then decisions taken by state authorities, even when they are fully justified and proportionate, are often subject to disapproval, assessment and questioning giving rise to a broad expanse for presenting various conspiracy theories, which people eventually find to be realistic and possible as a result of doubt in genuineness and intentions of decision-makers. Accordingly, in private conversations, but in the media as well, the line between justifiable measures taken as a consequence of the deepest concern for man as an individual and society as a whole and the social experiment in which we involuntarily participate, has become very thin, almost imperceptible, as if this shred of doubt has not left any of us unscathed.

We should not forget that although human rights derive from natural rights, the scope of the former has changed throughout history. Therefore, the level of guaranteed human rights and freedoms is subject to change and this change may in practice take place in two

different directions – the direction of human right enhancements but also in the direction of abolishing and diminishing certain achieved levels of rights, despite this unequivocally being prohibited by the law. In recent years the right to privacy and personal data protection has been recognised as the right entailing the improvement of protection mechanisms as a consequence of intensive development of digital technologies, which is reflected in the adoption of a large number of international and country-level legal documents which govern this area. It is important to note the challenges of personal data protection during the pandemic and point them out for some future similar or even more complex situations which at this point cannot be foreseen.

European legal framework for personal data protection and the right to privacy

Article 5 of the European Convention on Human Rights guarantees the right to liberty and security. Paragraph 1 thereof stipulates that everyone has the right to liberty and security of person and that no one can be deprived of their liberty save in the cases envisaged per the Convention and in accordance with a procedure prescribed by law. The lawful detention of persons for the prevention of the spreading of infectious diseases is one of situations in which the Convention envisages derogation from the rights set forth in Article 5.[2]

Article 8 stipulates that everyone has the right to respect for his private and family life, his home and his correspondence, along with the obligation of a public authority not to interfere with the exercise of this right except if such is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of other.

Article 15 specifies that in time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law. It is not allowed to derogate from Article 2 (Right to life), except in the event of demise which is a consequence of lawful wartime activities or Article 3 (Prohibition of torture), Article 4, Paragraph 1 (Prohibition of slavery and forced labour) and Article 7 (No punishment without law). Any High Contracting Party availing itself of this right of derogation will keep the Secretary General of the Council of Europe fully informed of the measures which it has taken and the reasons therefor and it shall also to inform the Secretary General of the Council of Europe when such measures have ceased to operate and the provisions of the Convention are again being fully executed. Article 15 is similar to Article 4 of the International Covenant on Civil and Political Rights and Article 27 of the American Convention on Human Rights. Also, many constitutions contain similar

[2] Law on Ratification of the European Convention on the Protection of Human Rights and Fundamental Freedoms, *Službeni list Srbije i Crne Gore – međunarodni ugovori*, no. 9/2003, 5/2005 and 7/2005 – corr., and *Službeni glasnik RS – Međunarodni ugovori*, no. 12/20102 and 10/2015.

provisions regarding the declaration of the state of emergency. Article 15 thus allows states to take measures which would otherwise not be permitted as per standard criteria of the Convention, and in this respect, dangers posed by the states of emergency, in terms of human rights, are apparent. Prohibition of abuse of rights is therefore prescribed in Article 17, which stipulates that nothing in the Convention may be interpreted as implying for any state, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth or at their limitation to a greater extent than is provided for in the Convention. Article 18 sets forth that the restrictions of the said rights and freedoms permitted under the Convention are not to be applied for any purpose other than those for which they have been prescribed.

Article 17 of the International Covenant on Civil and Political Rights, deriving from Article 12 of the Universal Declaration of Human Rights, stipulates the protection against 'arbitrary or unlawful interference' with 'his or her privacy, family, home or correspondence'.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is significant in this area[3]. Article 6 of this Convention stipulates that personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same applies to personal data relating to criminal convictions. All 47 Council of Europe member states are parties to this Convention (Convention 108), which also welcomes Council of Europe non-member states. The Convention was updated in 2018 (it is known as Convention 108+) and signed by all Council of Europe member states. On 26th May 2020, our country ratified the Council of Europe Protocol dated 18th May 2020, per which the said Convention was improved in terms of proportionality, lawfulness and transparency (Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.223).

The European Union updated its data protection regulations in 2016 by passing the General Data Protection Regulation (Regulation (EU) 2016/67 GDPR) and Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (EU) 2016/680.[4] Article 9 of the Regulation (EU) 2016/67 stipulates that data regarding health constitute a special category of personal data, the processing of which is not permitted, with the exception of specifically defined cases which are in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of

[3] *Službeni list Savezne Republike Jugoslavije – međunarodni ugovori*, no. 1/92, *Službeni list SCG – Međunarodni ugovori*, no. 11/2005 – dr. zakon i *Službeni glasnik RS – Međunarodni ugovori*, no. 98/2008 – dr. zakon i 12/2010).

[4] Directive EU 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

healthcare and of medicinal products or medical devices.[5] While observing the principle of lawfulness, personal data processing must be based on the data subject's consent to the processing of his or her personal data based on other legal grounds, as duly stipulated per the Regulation (Article 6), which in the time of pandemic when proximity applications for tracking contacts are being created, raises the issue of whether such applications and their utilisation may rely on consent. Former Data Protection Working Party expressed their position that 'if consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given' (Article 29, Guidelines on Consent, 2018), which means that voluntary partaking in contact tracing applications does not necessarily have to rely on consent as lawful grounds for processing (Guild, Mendos Kuskonmaz, 2020). The General Data Protection Regulation (EU) 2016/679 does not contain mechanisms for efficient safeguards against the use of anonymous data for the purpose of predictive algorithmic decision-making, risk assessment and behaviour-based classification, which may be used for undue discriminatory treatment or individuals or groups of individuals (Mühlhoff, 2020).

The European Data Protection Board adopted a formal Statement on the processing of personal data in the context of the COVID-19 outbreak[6], which clearly emphasises the significance of personal data protection during the state of emergency.

National legal framework for personal data protection and the right to privacy

Our privacy includes data which refer to marital status, religious beliefs and political opinions, financial transactions, ethnic origin, health, criminal offence data, and genetic material. In today's world of intensive advancement and development of digital technologies, which underlie every aspect of our family, professional and social lives, personal data protection against the public and controls of personal data flows take on an entirely new dimension. This means that it is necessary to know not only who our personal data are shared with but also who is authorised to collect them and for what purpose. The legislator has recognised this field as an area of crucial importance in the last decade, which resulted in the adoption of specific laws which govern the right to personal data protection and the exercise of this right. Many social networks, financial transactions and online payments and other activities which we access in a virtual environment have made natural persons and their privacy in cyberspace vulnerable in many ways – surveillance, virus spreading, exposure to verbal violence and ultimately identity theft.

All provisions with regard to human and national minority rights are construed in favour of improving the values of democratic society and in line with prevailing international standards and practices of relative institutions which deal with this matter.

[5] 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.

[6] Statement on the processing of personal data in the context of the COVID-19 outbreak https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en, 29/05/2020

Article 18 of the Constitution of the Republic of Serbia (*Službeni glasnik RS*, no. 98/2006) prescribes that guaranteed human and minority rights are implemented directly, whereas the law may prescribe manner of exercising these rights only if explicitly stipulated in the Constitution or necessary to exercise a specific right owing to its nature, whereby the law may not under any circumstances influence the substance of the relevant guaranteed right. Restrictions of these rights are lawfully permissible in cases and to the extent envisaged by the Constitution, however without encroaching upon the substance of the relevant guaranteed right (Article 20 of the Constitution of the Republic of Serbia). The same Article notes that state bodies, particularly the courts, are in such situations obliged to consider whether there is a proportion between restriction and purpose and possibility to achieve the purpose of the restriction with less restrictive means. Everyone has the right to judicial protection and they also have the right to elimination of consequences arising from the violation if they believe that any of their human or minority rights guaranteed by the Constitution have been violated or denied; they have the right to address international institutions.

Confidentiality of letters and other means of communication is inviolable and guaranteed as per Article 41, whereas protection of personal data is guaranteed pursuant to Article 42. Use of personal data for any purpose other than the one they were collected for is prohibited and punishable in accordance with the law, unless this is necessary to conduct criminal proceedings or protect safety of the country, in a manner stipulated by the law. In addition, it is stipulated that everyone has the right to be informed about personal data collected about them and right to judicial protection in case of the abuse of such data.

Upon declaration of the state of emergency or war, derogations from guaranteed human and minority rights are permitted only to the extent deemed necessary and cease to be effective upon ending of the state of emergency or war (Article 202 of the Constitution of the Republic of Serbia). Article 200 of the Constitution sets forth conditions for declaring and ending the state of emergency.[7] On 15th March 2020, the President of

[7] The state of emergency is declared by the National Assembly when the survival of the state or its citizens is threatened by a public danger, whereby the decision on the state of emergency is effective 90 days at the most, following which the National Assembly may extend the state of emergency for additional 90 days, by the majority vote of the total number of deputies. The National Assembly may then prescribe measures which derogate from human and minority rights guaranteed by the Constitution. If the National Assembly is not in a position to convene, the decision declaring the state of emergency is adopted by the President of the Republic together with the Speaker of the National Assembly and the Prime Minister, under the same terms, and measures which provide for derogation from human and minority rights may be prescribed by the Government, in a decree, with the President of the Republic as a cosignatory. In such situations, the National Assembly verifies decision on the state of emergency within 48 hours from its passing, that is, as soon as it is in a position to convene. If the National Assembly fails to verify this decision, it ceases to be effective upon the end of the first session of the National Assembly held after the declaration of the state of emergency. The same applies to Government decree on measures providing for derogation from human and minority rights. The Government is obliged to submit the decree within 48 hours from its passing, that is, as soon as the National Assembly is in a position to convene. In other respects, the measures providing for derogation cease to be effective 24 hours prior to the beginning of the first session of the National Assembly held after the declaration of the state of emergency.

the Republic of Serbia, Speaker of the National Assembly and Prime Minister rendered Decision on Declaring the State of Emergency[8], which was in effect until 6th May 2020, when the state of emergency ended according to the Decision of the National Assembly.[9] Article 53 of the Law on Protection of Population against Infectious Diseases (*Službeni glasnik RS*, no. 15/2016 and 68/2020) stipulates that the Minister of Health may, upon suggestion of the Committee and Institute, instruct movement prohibition or restrictions for population within an area affected by particular infectious disease. Based on this, the Government of the Republic of Serbia rendered Decision per which COVID-19 was declared an infectious disease.[10]

The Law on Personal Data Protection (*Službeni glansik RS*, no. 87/2018), health--related data are defined as special personal data and the processing thereof is set forth in Article 17, which specifically lists situations in which the processing of such data is permitted. Accordingly, paragraph 1 indicates that explicit consent of the data subject is required, unless the law stipulates that relative processing is not to be conducted based on consent, while paragraph 9 defines when data processing is permitted for the purpose of achieving public interests in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices. Article 18 stipulates that data processing conducted by competent authorities for specific purposes, such data disclosing racial or ethnic origin, political opinions, religious or philosophical beliefs or membership in trade unions, as well as the processing of genetic data, biometric data for the purpose of unique identification of a natural person, data regarding health or sex life or sex orientation of a natural person, is permitted only if such processing is necessary, whereby appropriate protection of rights of the data subject must be ensured.

Additional guidelines for the manner in which to act during the COVID-19 pandemic are contained in the Joint Statement issued by the Committee of Convention 108 and the Council of Europe Data Protection Commissioner, dated 30th March, which emphasises that during the pandemic, countries should take note of whether and to what extent undertaken measures affect democracy, rule of law and exercise of human rights, including the right to privacy and personal data protection.[11] It especially emphasises that under the new

---

8 *Službeni glansik RS*, no. 29/2020.

9 *Službeni glansik RS*, no. 65/2020.

10 Per Decree on Measures during the State of Emergency (*Službeni glansik RS*, no. 31/2020-3 dated 16th March 2020) restrictions were imposed in terms of the movement of persons infected with the virus, as well as persons suspected to be infected; a ban on any outdoor events was introduced as well as restrictions regarding indoor events; the Ministry of Interior was allowed to block any access to particular facilities or premises and to prevent that such premises are exited. The Order on the Restrictions and Prohibition of Movement for Persons in the Territory of the Republic of Serbia (*Službeni glansik RS*, no. 34/2020, 39/2020, 40/2020, 46/2020 and 50/2020) introduced the prohibition of movement during periods exceeding 24 hours for all persons in the territory of the country, which raised the issue of whether this measure is justified, it being not only a restriction of movement but its full cancellation.

11 Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data

circumstances it is of utmost importance to take note of data processing, such data referring to health of the population and that Recommendation CM/Rec(2019)2, which deals with health-related data (Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data). It contains guidelines on how to exercise the right to privacy and personal data protection rights, among healthcare professionals themselves, but also between the health sector and other sectors. In this regard, sensitive personal data are not to be disclosed (e.g. health-related data), and data processing activities should be carried out only provided that special, additional technical and organisational protection measures are in place. The following have been identified as the most challenging issues in large-scale personal data processing, for pandemic-prevention purposes:

- possible re-identification of persons based on previously anonymised data;
- possible data processing by employers during the pandemic, because of which employers should process only such personal data which are necessary for the purpose of identification of potentially exposed employees, with full respect of the principle of necessity, proportionality and accountability. Health-related data about employees may be disclosed to state authorities only in strict compliance with the underlying legal basis;
- Telecommunications companies, online platforms and internet service providers are also actively involved in the fight against the spread of COVID-19 and are increasingly required to share subscriber data, in order to determine subscribers' geolocation. It can therefore be concluded that the large-scale processing of such data may be conducted only if based on valid proof that this could contribute to ending pandemic spread, along with preventing and minimising the risks of failure to exercise the right to privacy, i.e. by conducting such data processing activity which is the least invasive in terms of exercising the right to privacy;
- When processing data in educational systems, it is of primary importance that a proper legal basis is chosen and the approval by parents or legal guardian for minors obtained. Also, parents must be allowed to gain insight into the processing of their children's data.

Public disclosure of health-related personal data, without the consent of data subjects, constitutes criminal offence, given the fact that the Law on Patients' Rights[12], the Law on Healthcare[13] and the Law on Health-Related Documentation and Records[14] explicitly prohibit such processing of personal data, unless explicit consent of the data subject has been obtained. In addition to this consent, other valid basis could be a court decision, whereas everything else may constitute criminal offense.

Protection Commissioner of the Council of Europe, Strasbourg, 30th March 2020, https://rm.coe.int/covid19-joint-statement/16809e09f4

[12] *Službeni glansik RS*, no. 45/2013, 25/2019.

[13] *Službeni glansik RS*, no. 25/2019.

[14] *Službeni glansik RS*, no. 123/2014, 106/2015, 105/2017, 25/2019.

Challenges identified during the COVID-19 pandemic: mobile tracking applications for the monitoring of infected persons

We can safely say that the pandemic caused by the COVID-19 outbreak was a sudden, unexpected and complex test of knowhow and ability of state authorities' representatives and at the same time also a test of trust they (do not) enjoy among the citizens. Mobile tracking applications have had a high-profile introduction as a means for combating the pandemic. The effectiveness of these applications is questionable, and if they do not contain embedded and efficient privacy protection measures, they may lead to various violations of human rights. Mobile applications whose purpose would be to alert users of their contacts with COVID-19 positive persons (even in situations when those persons were unaware of their potential infection), have already been implemented in certain Asian countries (Singapore, China, Taiwan and South Korea), while approximately 14 EU member states have launched them or are considering their development (Lazarević, Bajić, 2020). We should keep in mind that approximately 60% of population need to install the application in order for it to achieve desired results, and also that social (dis)trust in state institutions is directly connected with the outcome, i.e. failure of such mobile applications to succeed (Lazarević, Bajić, 2020). In 2017, BBC launched the *BBC Pandemic* application, as part of a nation-wide experiment conducted in Great Britain. The aim of the experiment was to collect data from volunteers who utilised the application for the purpose of assessing how an infectious disease, such as flu, may spread and affect the people of Great Britain. Based on collected data, a mathematical model was built, this model dealing with issues such as mortality rates. A documentary filmed based on this experiment was broadcast in 2018. This experiment and similar hints of a major outbreak in recent past resulted in higher numbers of various conspiracy theories and their advocates.

On 17th April, the European Parliament adopted a resolution thereby demanding full transparency so as for natural persons to be able to check the basic safety and privacy protocols of these applications (European Parliament Resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)).

When discussing the introduction of emergency measures, such as surveillance measures originally introduced for terrorism-combating purposes, we have witnessed that they 'often go too far, fail to have their desired effect, and, once approved, often outlast their justification', concludes the Human Rights Watch organisation (Human Rights Watch, 2020). The aim of the use of these mobile applications is to track infected persons' movements, identify persons with whom they were in contact during the period of their infection, monitor compliance with quarantine measures and social distancing measures, and thanks to cumulative data on location, currently active virus hotspots are determined. Future spread of the virus may be foreseen, and the results of healthcare measures undertaken until any particular date can be established in this manner. Mobile phones' GPS allows the tracking of location within the perimeter of 1.5 to 3 metres while many smartphone applications keep record of location data, which then can be obtained by governments and data agents. On the other hand, Bluetooth is used to directly connect with devices in immediate vicinity, for data transfer purposes (within the distance of approx. 10 metres), so it is considered a better solution because rather than tracking locations, it

tracks direct interaction with a high percentage of accuracy. Furthermore, data may be stored locally on the device itself instead of a centralised data base, which is a better option in terms of protection of the right to privacy.

Over the period of several months, human rights protection organisations in a number of states have identified cases of the violation of the right to privacy and personal data protection, all this with regard to the use of mobile phones and mobile phone applications.[15] Concerns are being voiced whether mobile phone tracking software will allow governments, as a result of the lack of transparency, to aggregate, utilise and store data which are beyond the scope necessary for lawful and targeted disease monitoring purposes, which is particularly worrying in countries which maintain records of extensive tracking, such as China, Ethiopia and Russia (in which there is a combination of data about the location with other types of data, such as facial recognition) (Human Rights Watch, 2020).

The use of mobile tracking applications in the circumstances of the pandemic, in addition to the right to privacy and personal data protection, is directly associated with the right to liberty and security. Article 5 of the European Convention on Human Rights protects the right to liberty and security of person, but it allows for the lawful detention of persons for the prevention of the spreading of infectious diseases. The British *Coronavirus Act 2020* allowed police officers and immigration officers to detain a person over a limited period of time if such a person is infected, and duly take the person to appropriate screening and evaluation facility. Great Britain introduced the lockdown measures primarily based on

[15] The decree declaring the situation of emergency was approved by the Government of Israel on 17th March. Per the Decree, *Shin Bet*, the Israel Security Agency, was permitted to receive, collect and process 'technological data' without users' consent. This included data about the location obtained from the Telcos Company, so as to assess whether citizens were exposed to the virus. The Ministry of Health sends to people alerts via the mobile phone and orders them to remain quarantined. The Government sidestepped the Parliament when the decree on extraordinary situations was adopted. The Supreme Court of Israel later ruled that the Government should pass a law per which they are authorised to 'respect the principles of privacy protection'.
On 31st March, the Armenian Parliament adopted amendments per which authorities were given a broad scope of authorisations, requiring the Telcos telecommunications company to present phone records to all its users, including telephone numbers and location, time and date of phone calls and text messages. Authorities may use these data for the purpose of identifying natural persons who are infected and who should be isolated or quarantined, or for the monitoring of isolated or quarantined natural persons.
On 20th March, the Prime Minister of Russia ordered the Ministry of Communications to design a national system for tracking people who have had contact with corona positive patients, based on the use of location data available from mobile phones. On 1st April, the Ministry of Communications confirmed that it had designed the system, while local authorities were required to deliver the lists of mobile phone numbers for persons infected with the coronavirus, as well as mobile phone numbers of persons quarantined in their homes because they had travelled abroad or had had contact with infected persons.
On 16th March, the President of Ecuador issued a decree per which he authorised the Government to utilise data generated from satellite and mobile phone platforms in order to track people who tested positive for the virus, persons who were in direct contact with a person who tested positive, persons who show symptoms as well as persons who had to undergo mandatory isolation due to entering Ecuador from a foreign country. (Human Rights Watch, 2020).

Section 45P of the Public Health Act (Control of Disease) of 1984, with relative regulation envisaging criminal offence charges in the event of leaving his/her residence 'without justifiable reason' (Greene, 2020).[16]

A new system called the Health Code has been introduced in China. The system uses a large quantity of mobile data and geolocations, which are collected by Chinese technology companies for the purpose of pinpointing infection hotspots. The application offers one of three colour codes to each of its 700 million users: green – which allows unrestricted movement, yellow – which requires a seven-day quarantine, and red – which requires a fourteen-day quarantine. Application users must scan QR codes at checkpoints if they want to enter buildings, go to the supermarket, use public transportation or move around their neighbourhoods (Human Rights Watch, 2020). The system allows users to report illegal or unauthorised activity, such as large public gatherings. This application is used not only to gain insight into the health of its users, on which basis assessments are made as to whether they may or may not move freely, but its role is also to exchange information with the police, 'setting a template for new forms of automated social control that could persist long after the epidemic subsides' (Sander, 2020, p. 2). At the same time, room is being made for the discrimination of certain groups, such as senior citizens who are not 'tech-savvy' and do not have the necessary skills to be able to use smartphones. Consequently, they will not have QR codes and thus may be denied access to public transportation, stores and healthcare institutions.

Representatives of state authorities in South Korea are making available the so called 'texts for safety guidelines', which describe the movements of people with recently diagnosed virus infection, without stating their names, however with noting personal data such as gender and age, which along with data about location may make available some details in terms of their private and family lives, which makes certain concerns regarding a dramatic transition from biometric surveillance 'over the skin' to biometric surveillance 'under the skin' justifiable (Sander, 2020). Thus, it is possible to imagine that some future pandemic will be an excuse for monitoring body temperature and blood pressure. The National Human Rights Commission of Korea has criticised South Korean authorities for providing more information than is necessary to stop the spread of disease, leading to a violation of privacy and human rights of an infected person, including 'secondary damages as patients become the target of criticism, taunts and hatred online', so rather than providing the travel history of each individual, the Commission has recommended that only the time and names of locations visited by infected people should be published (Human Rights Watch, 2020).

On 16th April, the Norwegian Institute of Public Health launched a voluntary self-reporting tracking application for the purpose of monitoring movements of application users and them being instructed to quarantine, in the event that any of them were exposed to a person who tested positive for the coronavirus. Once it is confirmed that an application user is positive for virus, the application will collect data about the location and send a text

[16] The European Court of Human Rights has concluded that Article 5 protects solely liberty in its standard form of physical liberty, however without providing person the right to do what he/she wants or go where he/she wants *(P v Cheshire West & Chester Council*; *P & Q v Surrey County Council* [2014] UKSC19).

message to all other user who are located within maximum 15 minutes from the infected person and duly instructs them to quarantine (Human Rights Watch, 2020). Since the end of May, public health agencies have at their disposal a joint Apple-Google contact tracking technology, which was first implemented in Switzerland (the SwissCovid application).

And while we are witnessing intensive introduction of stronger digital surveillance and shrinking room for rights and freedoms, which we thought were inherent when we were born into this world, the question is now raised as to scientific evidence in terms of the efficiency of data obtained via already (or still to be) installed mobile applications, for virus containing purposes. The use of such data may be 'a disproportionate invasion of the right to informational self-determination' (Mühlhoff, 2020).Furthermore, if the process of intensive innovation and change of legislation in this segment continue at this pace, the result could have long-term consequences due to the proliferation of algorithmic procedures for population management. This could lead to the use of these data for the purpose of deciding who will have access to medical services, jobs and educational opportunities, but also make predictions about who is in poor health or mentally unstable, who poses a potential security threat, thus dividing society into invisible social classes, which would be treated differently in terms of access to opportunities, resources and information (Mühlhoff, 2020).

Conclusion

Governments must not interfere with the right to privacy unless they can prove that such lawful interference was conducted for the purpose of achieving a legitimate objective (e.g. protection of public health) and that this interference is necessary and proportionate with the achievement of relative objective. By way of exception, stricter restrictions may be executed via derogations (Article 4 of the International Covenant on Civil and Political Rights and Article 15 of the European Convention on Human Rights), while states may derogate from the right to privacy and freedom of expression at the times of an emergency situation which is threatening the life of the nation. Nevertheless, such derogations are permitted only to the extent required by exigencies, provided that such measures are not inconsistent with other obligations under international law and do not include discrimination.

We must not accept claims that the current data protection regime is inadequate for the current challenges nor must we allowed that the COVID-19 pandemic panic us into accepting lower data protection standards and less privacy (Guild, Mendos Kuskonmaz, 2020). This is particularly relevant if we bear in mind that extensive data are in the hands of governments of which many have the long history of repression and discrimination of already marginalised groups, including religious communities and political dissidents (Human Rights Watch, 2020). In addition to these, there are other issues calling for prompt answers, before any future pandemic or some other new 'wave' that is already being announced:

- Since the accuracy of information obtained via Bluetooth connection may diminish in the presence of other signal-transmitting devices, as well as in thickly populated apartment blocks or in parks, the real issue is how reliable such data are, especially

in terms of combating the virus, if we cannot be certain whether people were indoors or outdoors, whether they wore face masks or not, etc;

- According to the information provided by Human Rights Watch, women are in some countries 31% less likely to have access to the internet than men, whereas there are 327 million fewer women worldwide who own a smartphone, due to lower literacy levels (out of approximately 781 million illiterate 15+ year old persons, almost two thirds are women and girls). If tracking applications become a prerequisite for accessing public of private spaces, the marginalised population, who are less capable of downloading such applications, will be faced with discrimination. The elderly are among this population;
- Different mobile phone use habits, digital literacy and technology acceptance may also exclude vulnerable or marginalised populations from public healthcare responses, which unjustifiably rely on mobile phone location tracking, since it is estimated that as many as two billion mobile phone users own devices which are not configured to support this technology. This represents approximately one quarter of all mobile phones which are used today (Human Rights Watch, 2020).

Curfew and the state of emergency can be suspended, but not the consequences which could arise from intensive technological advancements which have not been thoroughly thought through. This is why the approach to dealing with this issue must involve appropriate measures, which are to ensure the protection of guaranteed human rights and inclusion of all relevant stakeholders, such as IT experts but also lawyers, sociologists and health professionals, so as to come up with an acceptable model which would serve the purpose of protecting public and individual health, and ensure that human rights and freedoms are upheld at the achieved level. If we fail to do so, in the future we may run the risk of becoming a society of perfectly healthy slaves or robots, in which the issue replacing QR codes and various mobile applications with large-scale microchipping becomes a highly likely possibility.

REFERENCES / ЛИТЕРАТУРА

Constitution of the Republic of Serbia (2006). *Službeni glasnik Republike Srbije* 98/2006 [In Serbian]

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016L0680&-from=EN

European Parliament Resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences (2020/2616(RSP)). (2020, 17 April). Brussels. Available at https://www.europarl.europa.eu/doceo/document/TA-9-2020-0054_EN.html

Greene, A. Derogating from the European Convention on Human Rights in Response to the Coronavirus Pandemic: If not Now, When? (2020, April 14). Forthcoming, *European Human Rights Law Review* 2020. Available at http://dx.doi.org/10.2139/ssrn.3593358

Guild, E., Mendos Kuskonmaz, E. (2020, 4 May). COVID-19: A New Struggle over Privacy, Data Protection and Human Rights? *European Law Blog – News and Comments on EU Law*. Available at https://europeanlawblog.eu/2020/05/04/covid-19-a-new-struggle-over-privacy-data-protection-and-human-rights/

Human Rights Watch, Mobile Location Data and COVID-19: Q&A. (2020, May 13). Available at https://www.hrw.org/news/2020/05/13/mobile-location-data-and-covid-19-qa

Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, (2020, 30 March). Strasbourg: Council of Europe. Available at https://rm.coe.int/covid19-joint-statement/16809e09f4

Law on Confirming the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Službeni list Savezne Republike Jugoslavije – međunarodni ugovori*, 1/92, *Službeni list Srbije i Crne Gore – međunarodni ugovori*, 11/2005 – other law and *Službeni glasnik Republike Srbije – međunarodni ugovori* , 98/2008 – other law, and 12/2010) [In Serbian]

Law on Healthcare, *Službeni glasnik Republike Srbije* 25/2019. [In Serbian]

Law on Health-Related Documentation and Records, *Službeni glasnik Republike Srbije,* 123/2014, 106/2015, 105/2017, 25/2019. [In Serbian]

Law on Patients' Rights, *Službeni glasnik Republike Srbije* 45/2013, 25/2019. [In Serbian]

Law on Personal Data Protection, *Službeni glasnik Republike Srbije,* 87/2018. [In Serbian]

Law on Ratification of the European Convention on the Protection of Human Rights and Fundamental Freedoms, *Službeni list Srbije i Crne Gore – međunarodni ugovori,* 9/2003, 5/2005 and 7/2005 – corr., and *Službeni glasnik Republike Srbije – međunarodni ugovori*, 12/2010 and 10/2015. [In Serbian]

Lazarević, M. Bajić, D. (2020, May 8). COVID-19 tracing app in Serbia – How to pave the road with trust, transparency and inclusion, *Policy Brief*, European Policy Centre. Available at https://cep.org.rs/en/publications/brief-covid-19-tracing-app-in-serbia/

Mühlhoff, R. We Need to Think Data Protection Beyond Privacy: Turbo-Digitalization after COVID-19 and the Biopolitical Shift of Digital Capitalism (2020, March 30). Medium 2020. Available at SSRN: https://ssrn.com/abstract=3596506 or http://dx.doi.org/10.2139/ssrn.3596506

Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 223. (2018, 10 April). Strasbourg: Council of Europe. Available at https://rm.coe.int/16808ac918

Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data. (2019, March 27). Available at https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168093b26e

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). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Sander, B. Belli, L. COVID-19 Symposium: COVID-19, Cyber Surveillance Normalisation and Human Rights Law. (2020). Available at http://opiniojuris.org/wp-content/uploads/B.-Sander-J.-Rudall-eds-COVID-19-and-International-Law-Opinio-Juris-Symposium-copy-1.pdf

Statement on the processing of personal data in the context of the COVID-19 outbreak. (2020, March 20). European Data Protection Board. Available at https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en