5. PRIVATNOST I ZAŠTITA OSOBNIH PODATAKA U DIGITALNOM OKRUŽENJU

Suvremeni koncept ljudskih prava ima duboke religijske, filozofske i političke korijene koji sežu daleko u prošlost. Iako mu začetke nalazimo već prije 2000 godina u kršćanstvu, a zatim i u drugim religijama, te u djelima filozofa drevne Grčke, kada se po prvi put upućuje na jednakost ljudi, pojedina su ljudska prava kroz povijest priznavana u drugo vrijeme i drugačijem opsegu u različitim zemljama diljem svijeta.

Političke korijene ljudskih prava nalazimo već u Velikoj povelji (*Magna Charta Libertatum*), koju je 1215. bio prisiljen potpisati engleski kralj, priznajući građanima određena prava i na taj način ograničavajući svoju vlast. Kasnije u 17. i 18. stoljeću taj se koncept nadopunjuje idejom o prirodnom pravu, pravu koje pripada svakom čovjeku po samoj prirodi i zbog toga što je ljudsko biće. Filozofi tog doba, poput Locke-a, Paine-a, Mill-a, Thoreau-a i dr. formulirali su, uobličili i proširili taj koncept, što je omogućilo da se nakon borbe za američku nezavisnost i Francuske revolucije neka od tih prava priznaju u američkoj *Deklaraciji o nezavisnosti* 1776. i francuskoj *Deklaraciji o pravima čovjeka i građanina* iz 1789. godine. Kasnije u 19. i početkom 20.-tog stoljeća uslijedilo je priznavanje tih prava u zakonodavstvima brojnih zemalja. Sam opseg zaštite ovisio je uvelike o povijesnom, kulturnom i političkom okruženju i prilikama unutar tih zemalja. Istovremeno, takva je zaštita bila ograničenog dometa i donekle protivna samoj prirodi ovih prava. Naime, univerzalnost ljudskih prava zahtijevala je isto takav opći, sveobuhvatan i ujednačen pristup njihovom priznanju i zaštiti na međunarodnom planu.

Nakon drugog svjetskog rata, vođeni spoznajama o neljudskostima za njegova trajanja kao i eventualnim posljedicama nekog budućeg rata, svijest o potrebi zaštite ljudskih prava i temeljnih sloboda na međunarodnom planu sve više jača. Kao rezultat toga uslijedilo je njihovo priznanje *Općom deklaracijom o ljudskim pravima* Ujedinjenih naroda iz 1948., te *Konvencijom za zaštitu ljudskih prava i temeljnih sloboda* Vijeća Europe iz 1950.. Njima je priznato i potvrđeno neotuđivo pravo svakog pojedinca na određene osobne, političke, socijalne, kulturne i gospodarske slobode i prava, te uspostavljen međunarodni sustav zaštite. Tako je jedan apstraktni pojam dobio svoje ozbiljenje u nacionalnim pravnim porecima i obvezujućim međunarodnim ugovorima. Te zajedničke vrijednosti priznate su i u *Povelji o temeljnim pravima Europske unije*[1] u kojoj se već u preambuli naglašava da se Unija temelji temelji na nedjeljivim, univerzalnim vrijednostima ljudskog dostojanstva, slobode, jednakosti i solidarnosti. te na načelima demokracije i vladavine prava.

No, ljudska prava nisu nepromjenjiva kategorija, već su podložna stalnom preispitivanju, širenju i prilagođavanju pod utjecajem neprekidnih promjena u odnosima komuniciranja i raznovrsnim oblicima gospodarskog, političkog, socijalnog i duhovnog života i interakcije. Permanentne promjene u tehnologiji, gospodarstvu i društvu nužno vode odgovarajućim dopunama, izmjenama i promjenama pravne regulative, pa se i pravni sustavi moraju podjednako brzo mijenjati i prepletati s drugim mjerama i instrumentima društvenog reguliranja i zaštite društva od eventualnih neželjenih djelovanja i mogućih posljedica. To se posebno odnosi na područje ljudskih prava i temeljnih sloboda.

[1] Povelja o temeljnim pravima Europske unije pravno je obvezujuća od 1. prosinca 2009.

5.1. Pravo na privatnost i zaštitu osobnih podataka

5.1.1. O pojmu i nastanku prava na privatnost

Privatnost ima korijene daleko u prošlosti, te se u većoj ili manjoj mjeri spominje već od davnina u različitim zemljama i kulturama. Tako npr. Biblija ima brojna upućivanja na privatnost, a zaštita privatnosti u različitim aspektima postojala je i u hebrejskoj kulturi, staroj Grčkoj i drevnoj Kini.[2] U početku se najčešće radilo o pravu pojedinca na nepovredivost doma. Tako se već oko 200. godine u Zborniku židovskih zakona – Mishni – štiti osoba od tuđeg zavirivanja u svoju kuću.[3] Kroz povijest, privatnost se vrlo često povezivala s pravom vlasništva i odnosima koji iz toga proizlaze za pojedinca, što je poznato još od vremena starih atenjana.[4] No, unatoč tome što je riječ o temeljnom ljudskom pravu, poznatom i priznatom diljem svijeta do danas nema općeprihvaćene definicije privatnosti. kao ni suglasnosti u pogledu sadržaja toga prava. Postojeće definicije uvelike ovise o vremenu, sredini, okruženju i kontekstu u kojem se taj pojam koristi.

Tako je za Westina to "želja ljudi da slobodno biraju pod kojim uvjetima i u kojoj mjeri će izložiti sebe, svoje stavove i svoje ponašanje drugima",[5] dok je za Michaela to "pravo pojedinca da bude zaštićen od nedopuštenog zadiranja u njegov osobni život ili posao, ili njegove obitelji, neposrednim fizičkim mjerama ili objavljivanjem informacija".[6] Definicija *privatnosti* u Black`s Law Dictionary po kojoj je to "pravo biti ostavljen na miru; pravo pojedinca da bude pošteđen od neopravdanog publiciteta; i pravo na život bez neovlaštenog miješanja javnosti u stvari koje se javnost nužno ne tiču.",[7] ukazuje na složenost tog pojma kao i na različite aspekte tog prava.

Razlog je to zbog čega se često pravi razlika između informacijske, tjelesne, komunikacijske i prostorne privatnosti. U takvoj podjeli *informacijska* privatnost uključuje uspostavu pravila upravljanja, prikupljanja i korištenja osobnih podataka kao što su kreditne informacije ili zdravstveni podaci; *tjelesna* se odnosi na fizičku zaštitu pojedinca od različitih postupaka kao što su testiranje na drogu ili pretraživanje¸ *komunikacijska* se odnosi na sigurnost i privatnost pošte, telefona, elektroničke pošte i drugih oblika komunikacije; dok se *prostorna* odnosi na određivanje granica nedopuštenog miješanja u obiteljsko i drugo okruženje (npr. radno mjesto ili javni prostor).[8] Roger Clarke tome dodaje i *medijsku* privatnost, koja obuhvaća različite aspekte ljudskog ponašanja, a posebno one najosjetljivije poput seksualnih sklonosti i navika, političkih aktivnosti i vjerskih običaja, i to kako u privatnom tako i javnom životu čovjeka.[9] Različiti aspekti privatnosti govore o tome koliko je privatnost složena kategorija koja se kroz povijest mijenjala u zavisnosti o stupnju društvenog razvoja i demokratskim procesima unutar različitih zemalja. Štoviše, u novije se vrijeme pojedini aspekti prava na privatnost, poput

---

[2] Moore, B. Jr., *Privacy. Studies in Social and Cultural History,* Armonk, New York 1984., str. 82.
[3] Brezak, M. *Pravo na osobnost*, Nakladni zavod Matice Hrvatske, Zagreb 1998., str.17.
[4] Moore, *op.cit*. (bilj. 110), str. 82. i 108.
[5] Westin, A. F., *Privacy and Freedom*, Atheneum, New York 1967., str. 7.
[6] Michael, J., *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*,. UNESCO, Darmouth 1994., str. 1..
[7] *Black`s Law Dictionary,* 1991., West Publishing co., St. Paul, Minn.
[8] Privacy International, *Privacy & Human Rights 1999 – Executive Summary,* http://privacyinternational.org/survey/summary.html, str. 4. (04.12.2000.).
[9] Clarke, R., *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, 1999., http://www.rogerclarke.com/DV/Intro.html, str. 2. (01.07.2015.).

zaštite osobnih podataka, posebno izdvajaju i zasebno navode. Razlog tome je sve veća složenost njihove zaštite i njihova izloženost opasnostima i sve brojnijim zloporabama.

Međunarodno priznanje prava na privatnost uslijedilo je u okviru Ujedinjenih naroda izglasavanjem *Opće deklaracije o ljudskim pravima* 1948. godine. Ona propisuje da nitko ne smije biti izvrgnut samovoljnom miješanju u njegov privatni život, obitelj, dom ili prepisku, niti napadima na njegovu čast i ugled, te da svatko ima pravo na zaštitu zakona protiv ovakvog miješanja ili napada (čl. 12.). U čl. 8. *Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda* svakome se jamči pravo na poštivanje privatnog i obiteljskog života, doma i dopisivanja. Ustavom Republike Hrvatske jamči se pravo privatnosti svakom njenom građaninu u svakim njenim aspektima.[10] Tako Ustav jamči pravo na *prostornu* (čl. 34.), *informacijsku* (čl. 37), i *komunikacijsku* (čl. 36.) privatnost, a prihvatimo li koncept privatnosti u širem kontekstu, tada i *tjelesnu* (čl. 23.) privatnost.

Kako u pogledu definicije, tako se i u pogledu opsega i sadržaja ovog prava mišljenja se razlikuju. Prilično široko tumačenje nalazimo u *Deklaraciji o sredstvima javnog priopćivanja i ljudskim pravima* iz 1970. po kojoj se pravo na privatnost sastoji "prvenstveno u mogućnosti da se živi prema vlastitom nahođenju uz minimalna uplitanja. Odnosi se na privatni, obiteljski i kućni život, fizički i moralni integritet, čast i ugled, ne predstavljanje u krivom svjetlu, neobjavljivanje nepotrebnih i neugodnih podataka, neovlašteno objavljivanje privatnih fotografija, na zaštitu od špijunaže i neopravdanih ili neprihvatljivih indiskrecija, na zaštitu od zlonamjernog korištenja privatnih razgovora, na zaštitu od širenja informacija priopćenih ili primljenih od pojedinaca u povjerenju".[11] Stoga ne iznenađuje da niti razgraničenje od drugih osobnih prava nije jasno određeno, pa tako ima i onih koji smatraju kako su u određenom smislu, sva ljudska prava samo aspekti prava na privatnost.[12] Nasuprot tome, postoje mišljenja da su neka od navedenih osobnih prava, poput prava na čast i ugled, sadržajno različita i priznata u drugo vrijeme, pa ih zato treba razgraničiti i pojmovno razlikovati.[13] Spomenute teškoće definiranja, sadržajnog određivanja i razgraničenja u odnosu na druga prava proizlaze iz raznovrsnosti i bogatstva čovjekova intelektualnog i emocionalnog, osobnog i obiteljskog, te privatnog i javnog života, kao i složenosti, raznovrsnosti i brojnosti odnosa u koje on stupa s drugim ljudima i javnim institucijama.

Unatoč različitim stavovima glede nastanka, pojma i sadržaja ovog prava, jedinstveno je mišljenje da privatnost zaslužuje opće priznanje i zaštitu jer je riječ o neotuđivom pravu čovjeka, čije je ostvarenje preduvjet slobode i jednakosti građana. Takva zaštita je nužna, kako iz općih, tako i iz osobnih razloga. Ona je pokazatelj demokratičnosti nekog društva, slobode i jednakosti građana i preduvjet ostvarenja vladavine prava. Neke od važnijih *osobnih* razloga njenom priznanju možemo naći u radu Lynn Gillam *Ethics, Privacy and Confidentiality.* Po njoj je privatnost: *prvo*, vid *autonomije* jer čovjeku daje kontrolu nad njegovim životom, a dio te kontrole odnosi se na to da zna što o njemu znaju drugi, što mu omogućava da djeluje u različitim društvenim okruženjima i s različitim stupnjem intimnosti u odnosu na druge ljude; *drugo*, važna je za osobni *identitet*, jer je nužna pri njegovu kreiranju, razlikovanju od drugih ljudi, te otkrivanju i kreiranju nas samih; i *treće*, važna je za *društvene odnose* u koje stupamo, jer različite međuljudske odnose karakterizira različiti stupanj intimnosti. Štoviše,

[10] *Ustav Republike Hrvatske*, 56/1990, 135/1997, 113/2000, 28/2001, 76/2010, 5/2014.
[11] U Republici Hrvatskoj ova Deklaracija prihvaćena je *Zaključcima o prihvaćanju akata Savjeta Europe o slobodi izražavanja i informiranja*, NN 7/91.
[12] Fernando, V., *Legal personality, privacy and the family*, u Henkin (ur.), *The Internetional Bill of Rights,* Columbia University Press, New York, 1981., navod iz: Privacy International, *Privacy and Human Rights 2000 Overview*, na Internet adresi: <www.privacyinternational.org/survey/phr2000/overview.html> (04.12.2000.)
[13] Gavella, N., *Osobna prava*, str. 212-213.

uspostavljanjem odnosa ili čineći ih bliskijima i intimnijima otkrivamo o sebi stvari koje bi inače smatrali privatnim.[14]

Osim tih "osobnih", opći razlozi u prilog cjelovite i sveobuhvatne zaštite privatnosti proizlaze iz zajedničkih interesa građana, odnosno interesa nacionalnih ili regionalnih zajednica. Neki od njih su: 1) ispravljanje nepravdi radi kršenja ljudskih prava u prošlosti, zbog čega su mnoge zemlje u Južnoj Americi, Južnoj Africi i Centralnoj Europi donijele novo zakonodavstvo kako do toga više ne bi došlo; 2) promicanje elektroničkog poslovanja, odnosno zaštite korisnika od zloporaba njihovih osobnih podataka; i 3) nužnost usklađivanja zakonodavstava s pravnim sustavom Europske unije, bilo zbog želje za što skorijim priključenjem Europskoj uniji ili zbog usklađivanja sa strogim zahtjevima EU u pogledu protoka podataka van njenih granica a radi osiguranja daljnjeg nesmetanog poslovanja.[15] U prilog općoj i cjelovitoj zaštiti privatnosti ide i niz drugih razloga osobne, političke, etičke i pravne prirode.

5.1.2. Ograničenja osobnih prava

Iako iznimno važni za svakog čovjeka, pravo na privatnost i pravo na zaštitu osobnih podataka, kao i ostala osobna prava, nisu apsolutna već se iznimno i u točno propisanim okolnostima mogu ograničiti i to tuđim pravima i slobodama te zakonskim ograničenjima.[16] Takva ograničenja nalazimo već u Ustavu koji predviđa se se slobode i prava mogu ograničiti samo zakonom da bi se zaštitila sloboda i prava drugih ljudi te pravni poredak, javni moral i zdravlje (čl. 16.) ili pak u doba ratnog stanja ili neposredne ugroženosti neovisnosti i jedinstvenosti države, te velikih prirodnih nepogoda kada je to moguće učiniti dvotrećinskom odlukom Hrvatskog sabora (čl. 17.). No, i u tim slučajevima svako ograničenje slobode ili prava mora biti *razmjerno* naravi potrebe za ograničenjem u svakom pojedinom slučaju.

U praksi je česta kolizija prava na privatnost i prava na slobodu izražavanja. Ustav jamči pravo na slobodu mišljenja i izražavanja misli, što osobito obuhvaća slobodu tiska i drugih sredstava priopćavanja, slobodu govora i javnog nastupa, slobodno osnivanje svih ustanova javnog priopćavanja i pravo na pristup informacijama koje posjeduju tijela javne vlasti, dok istovremeno zabranjuje cenzuru (čl. 38). koje također podliježe ustavnim i zakonskim ograničenjima. Tako sloboda izražavanja ne smije biti zlorabljena radi pozivanja ili poticanja na bilo koji oblik nesnošljivosti jer je Ustavom zabranjeno i kažnjivo svako pozivanje ili poticanje na rat ili uporabu nasilja, na nacionalnu, rasnu ili vjersku mržnju ili bilo koji oblik nesnošljivosti. (čl. 39.). Ovakvo ustavnopravno određenje i jamstvo prava na slobodu izražavanja u skladu je s navedenim međunarodnim ugovorima.

Unatoč jasnom određenju da slobode i prava ne smiju ići na štetu sloboda i prava drugih ljudi, sloboda izražavanja često za posljedicu ima zadiranje u čast, ugled i privatnost pojedinaca. Takvo je izražavanje posebno opasno kada se vrši putem sredstava javnog priopćavanja, posredstvom kojih se informacije prenose velikom broju ljudi. Napokon, i sam koncept privatnosti i njegovo pravno određenje u neposrednoj su vezi sa slobodom izražavanja i sredstvima javnog priopćavanja. Naime, Brandeis i Warren u radu *The Right to Privacy,* objavljenom u "Harvard Law Review" 1890. godine, po nekima "najutjecajnijem pravnom članku ikada objavljenom", ukazujući na potrebu pravne zaštite od sve brojnijih slučajeva

---

[14] Gillam, L., *Ethics, Privacy and Cinfidentiality*, 2000, www-nursing-unimelb.edu.au/gdcmpub/gdcmcrse/cim/CIM_Week_8.pdf (10.02.2001.), str. 11.

[15] Privacy International, *Privacy and Human Rights 2000 Overview*, www.privacyinternational.org/survey/phr2000/overview.html (04.12.2000.).

[16] Sokol, S., Smerdel, B., *Ustavno pravo,* Informator, Zagreb 1998., str. 74.

ugrožavanja i zadiranja "žutog" tisaka u intimni život ljudi, postavili su pravne temelje prava na privatnost, utvrdili razlike u odnosu na druga prava i prvi odredili njena ograničenja. Upozoravajući kako su u to vrijeme nedavna otkrića i poslovne metode dovele do zahtjeva za promjenama i potrebe za prilagođavanjem pravne regulative, ukazali su na nužnost zaštite osobnosti i osiguranja pojedincima onog što je sudac Cooley nazvao pravom "biti ostavljen na miru".[17] Već tada su uočene opasnosti od informacijskih tehnologija i potreba za uspostavljanjem ravnoteže između različitih osobnih prava poput prava na slobodu izražavanja i prava na privatnost ili prava na zaštitu osobnih podataka i prava na pristup informacijama, posebno kada je riječ o javnom priopćavanju (informiranju) putem tiska, radija i televizije.

Posebno pitanje u tom kontekstu predstavlja pravo na privatnost javnih osoba. U spomenutoj Deklaraciji se u pogledu toga navodi da "poštovanje privatnosti osobe koja sudjeluje u javnom životu predstavlja posebni problem. Formula prema kojoj ´privatni život prestaje tamo gdje počinje javni` nedovoljna je za rješenje ovog problema. Osobe koje igraju neku ulogu u javnom životu imaju pravo na zaštitu privatnog života *osim u slučajevima kada se ovaj posljednji odražava na javni život.* Time što pojedinac ima neku javnu *funkciju ne uskraćuje mu se pravo na privatnost."* U praksi Europskog suda za ljudska prava sud je zauzeo stav da je odlučujući čimbenik pri utvrđivanju ravnoteže između zaštite privatnog života i slobode izražavanja doprinos koji objavljene fotografije ili članci imaju u raspravi koja je od općeg interesa.[18]

Budući da je riječ o suprotstavljenim interesima, s jedne strane prava pojedinca da sačuva svoju osobnost te, s druge, prava javnosti da bude informirana, odgovornost za takve informacije u svakom konkretnom slučaju ovisiti će o istinitosti samih informacija, načinu na koji su prikupljene, mediju putem kojeg su priopćene, te osobi koja ih je priopćila (njenoj namjeri i djelatnosti koju obavlja) kao i osobnom pravu koje je time povrijeđeno.[19] Obzirom na složenost tog odnosa, zakonsku nedosljednost[20] i potrebu da se istovremeno osigura privatnost i informiranost građana, ova su prava često suprotstavljena ali istovremeno i nerazdvojiva. Naime, pravo pojedinca na slobodu izražavanja podrazumijeva također i njegovo pravo da osim slobodnog širenja ideja i informacija također i prima takve informacije i ideje iz okoline, u čemu je djelatnost javnog priopćavanja i uloga javnih glasila od neprocjenjive važnosti. Informiranost građana, posebno kada je riječ o pitanjima od javnog interesa, preduvjet je njihove slobode i jednakosti i mjerilo demokratičnosti svake društvene zajednice. O dostupnosti informacija neposredno ovisi aktivno učešće građana u političkom, socijalnom, kulturnom i svakom drugom životu. Istovremeno, pravo na privatnost, između ostalog, podrazumijeva da pojedinac može sam odlučivati o tome "koliko će s drugima dijeliti – svoje misli, svoje osjećaje i podatke o svom osobnom življenju",[21] odnosno "da slobodno bira pod kojim uvjetima i u kojoj mjeri će izložiti sebe, svoje stavove i svoje ponašanje drugima".[22] Na taj način ova se prava međusobno ne isključuju, već su naprotiv, komplementarna.

Pravo na slobodu izražavanja nije ograničeno na izgovorenu ili napisanu riječ, objavljenu fotografiju ili karikaturu, već se odnosi na najrazličitije oblike izražavanja što u praksi može dovesti do uklanjanja ili ograničavanja različitih zabrana. Primjer toga predstavlja zabrana izvoza kriptografskog softvera koji je jedno od najefikasnijih sredstava zaštite informacijske i

---

[17] Warren, S., Brandeis, L.D., *The right to privacy,* Harvard Law Review Vol. 4, No. 5, 1890.
[18] *Hannover v. Germany*, (Application no. 59320/00), Strasbourg, 24. lipnja 2004.
[19] Gavella, N., *Osobna prava,* str. 193. i dalje.
[20] Alaburić, V., *Mediji vs. privatnost – kritička analiza hrvatskog civilnog i kaznenog zakonodavstva*, Hrvatska pravna revija, br. 3/2002., str. 13. i dalje.
[21] Simons, G.L., prema S. Lilić, *Data protection and new Technologies in Public Administration*, Zbornik Pravnog fakulteta u Zagrebu, br. 6/1988., str. 797.
[22] Westin, A. F., *Privacy and Freedom*, Atheneum, New York 1967., str. 7.

komunikacijske privatnosti građana. Tako je u SAD-u, gdje takva zabrana postoji, sud u Kaliforniji u slučaju *Bernstein v. United States Department of Justice* proglasio zabranu izvoza kriptografskog softvera neustavnom jer se njome ograničava ustavno pravo na slobodu govora. Naime, Daniel Bernstein, profesor na Sveučilištu Illinois, razvio je enkripcijsku metodu poznatu pod nazivom "Snuffle", napisao je program koji omogućava njeno korištenje i namjeravao objaviti izvorni kod na Internetu. Tome se suprotstavilo niz državnih agencija i ministarstava tvrdeći da to predstavlja povredu Zakona o kontroli izvoza naoružanja (Arms Export Control Act - AECA) u kojem je jaki enkripcijski softver na istoj listi sa nuklearnim oružjem, te je predviđena novčana kazna od milijun dolara i kazna zatvora do 10 godina za njegov izvoz u druge zemlje. Nakon što je Bernstein tužio nadležno ministarstvo, okružni sud a zatim i žalbeni sud donijeli su presude u njegovu korist. Na taj je način po prvi put programski jezik izjednačen s prirodnim čovjekovim jezikom, pa je i zabrana objavljivanja izvornog koda postala protivna pravu na slobodu izražavanja.

5.1.3. Informacijske tehnologije i privatnost

Utjecaj informacijskih tehnologija na privatnost od otkrića Guttenbergova tiskarskog stroja u petnaestom stoljeću do danas, bila je dvojaka. Na jednoj strani, ona je imala odlučujući ulogu u širenju informacija i znanja, promicanju ljudskih prava i razvoju svjesti o potrebi njihova priznanja i zaštite; a na drugoj, dovodeći u pitanje ispravnost i opravdanost prava i postupaka pojedinaca i vladajućih struktura sve je više poticala i razvijala svijest o potrebi priznanja i zaštite ljudskih prava i temeljnih sloboda.

Druga informacijska revolucija na prijelazu iz 19. u 20. stoljeće, omogućila je da se pitanju ljudskih prava pristupi zajednički i prilično ujednačeno. Vrlo često upravo radiju i televiziji možemo zahvaliti što se informacije o ugrožavanju ljudskih prava i sloboda brzo šire. Iako je to još uvijek bilo ograničenog opsega, zbog prostornog ograničenja i dometa tadašnjih informacijskih tehnologija, ono je ipak odigralo značajnu ulogu u priznavanju tih prava unutar različitih pravnih poredaka. Tek od devedesetih, razvojem, slanjem i komercijalnim korištenjem komunikacijskih satelita za potrebe medija, stvorene su pretpostavke za dostupnost tih tehnologija na širim prostorima, što je poznatije kao "CNN efekt". Iako CNN-ovim televizijskim prijenosom nasilja i masakra studenata s trga Tiananmen nije ugrožena kineska vlast i suverenost, može se sa sigurnošću kazati da su urodili takvim stupnjem reakcije svijeta do koje ne bi došlo da nije bilo takvog javnog priopćavanja. Dostupnost i brzina širenja takvih informacija omogućava brzu reakciju svijeta na suzbijanje i sprječavanje takvih pojava. Danas se taj pojam koristi kao sinonim za utjecaj medija na formuliranje vanjske politike u prvom redu vodećih zemalja i međunarodnih organizacija kada u nekim regijama i zemljama dođe do humanitarne ili ratne krize (npr. Afganistan, Irak, Sirija itd.)

Međutim, odlučujući utjecaj donijela je *informatička revolucija*. Razvoj računala, računalnih mreža, elektroničkog poslovanja i elektroničkog izdavaštva ostavilo je dubokog traga na ljudska prava. Tome je posebno pridonio razvoj i širenje Interneta. Za razliku od drugih informacijskih tehnologija, Internet je već odavno nadišao nacionalne granice, koristeći već postojeću informatičku tehnologiju i komunikacijsku infrastrukturu, te omogućavajući tako najširem krugu ljudi diljem svijeta da globalno komuniciraju. Njemu vrlo često možemo zahvaliti što se svijest o ugrožavanju ljudskih prava i sloboda sve više širi i van granica nacionalnih država. Naime, potencijal Interneta da postane temeljna infrastruktura i medij globalnog informacijskog društva upravo počiva na činjenici da on nadilazi nacionalne granice suverenih država, te kontrole i dominantnog utjecaja njihovih vlasti. Njegove karakteristike - globalnost, otvorenost, dostupnost, decentraliziranost i neovisnost od posebne infrastrukture -

čine ovaj medij jedinstvenim i bitno drugačijim od drugih. Budući da je Internet istovremeno sredstvo masovnog interaktivnog komuniciranja i sredstvo javnog priopćavanja, ovaj je medij nezamjenjiv u promicanju i ostvarivanju slobode izražavanja i informiranja te zaštite privatnosti. Anonimnost koju on pruža od presudnog je značaja jer omogućava ljudima da izraze svoja politička, vjerska i druga uvjerenja bez bojazni za svoj tjelesni i duhovni integritet. Zato i ne iznenađuje mišljenje mnogih da je riječ o najdemokratskijem mediju od svih informacijskih tehnologija do danas.

No, istovremeno treba priznati kako su upravo informacijske tehnologije, i prije pojave računala i Interneta, ponekad omogućavale da se ljudskih prava ugroze na način kakav prije nije bio moguć. Tisak, radio i televizija često su kroz povijest bile izvorom raznih neistinitih informacija i manipulacija, te sredstvo za ostvarenje različitih nemoralnih i nezakonitih ciljeva, najčešće od strane vladajućih struktura. Čak i onda kada to nije bio slučaj, informacijske su tehnologije koristile vlastima u totalitarnim režimima kako bi učvrstili svoju moć i ostvarili svoje ciljeve. Pokazuje to nacistička propaganda putem javnih glasila prije i za vrijeme II svjetskog rata, te korištenje IBM-ovih strojeva za pronalaženje, popis i sistematizaciju Židova, Roma i ostalih koji su prošli strahote u nacističkim koncentracionim logorima.[23] Čak i jednostavne informacijske tehnologije ponekad su poslužile vlastima da se obračunaju s neistomišljenicima. Tako je već spomenuti slučaj masakra studenata na trgu Tiananmen 1989. poslužio kineskoj vladi za identifikaciju demonstranata, korištenjem snimki iz kamera postavljenih za kontrolu prometa.[24] Sveprisutni video nadzor kako na radnim mjestima, javnim površinama i zgradama, tako i drugdje, koristi se za nadzor sve većeg broja ljudi. Događaji od 11. rujna 2001. godine u New Yorku, kao i opasnosti od informacijskog ili kibernetičkog terorizma, tome su još više pridonijeli. Širom svijeta počeli su se donositi novi zakoni kojima državna sigurnost jača na račun osobnih prava i sloboda građana.

Razvoj informatičke i komunikacijske tehnologije donio je nove opasnosti za građane, njihova prava i slobode, omogućavajući organizacijama, pojedincima i grupama da zloporabe tu infrastrukturu provodeći informacijski i komunikacijski nadzor nad ljudima i suparnicima, političkim neistomišljenicima, sindikalnim čelnicima, novinarima, kupcima, zaposlenicima i drugim osobama. Istovremeno, već spomenuta anonimnost, omogućila je velikom broju ljudi da Internet koriste za prezentaciju i distribuciju različitih nemoralni i nezakonitih sadržaja kojima se zadire u dostojanstvo, ugled ili čast građana, pri čemu su nerijetko žrtve maloljetnici i djeca. Sve su brojniji sadržaji koji pozivaju ili potiču na rat ili uporabu nasilja, na nacionalnu, rasnu ili vjersku mržnju ili druge oblike nesnošljivosti, čak i na ubojstva i samoubojstva. Kao posljedica toga u velikom broju zemalja sve je više onih koji smatraju da treba ograničiti pristup Internetu, njegovim servisima i sadržajima. Iako se ta ograničenja pravdaju potrebama nacionalne sigurnosti i sprječavanja prezentacije i distribucije nemoralnih i nezakonitih sadržaja, nerijetko ona idu na štetu slobode izražavanja i informiranja, a mogu poslužiti i za suzbijanje aktivnosti političkih neistomišljenika.[25] Od takvih ograničenja nisu se suzdržale niti najrazvijenije zemlje poput SAD-a, Njemačke, Francuske i Novog Zelanda, a i tamo gdje ih još nema postoje inicijative da se uvede cenzura na Internetu, odnosno da se ograniči sloboda izražavanja.

---

[23] V. više u Black, E., *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation*, Three Rivers Press, 2002.

[24] Denning, D. E., *Information Warfare and Security*, Addison Wesley Longman, Inc., Reading, Massachusetts, 1999., str. 193.

[25] *Silencing The Net: Threat to Freedom of Expression On-line,* Humans Rights Watch, http://www.oneworld.org/news/partner_news/index.htm/ (21.11.2002.)

Osim navedenog, kršenju privatnosti pridonose i brojni drugi trendovi, kao što su:

1. *globalizacija* – koja uklanja zemljopisna ograničenja protoku podataka;

2. *konvergencija* - koja vodi ukidanju tehnoloških barijera između sustava, posebno informacijskih sustava koji na taj način međusobno komuniciraju, izmjenjuju i obrađuju različite oblike podataka;

3. *multimedija* – koja spaja različite oblike prijenosa i izražavanja podataka i slika tako da se informacije prikupljene u određenom obliku mogu lakše prevesti u neki drugi oblik.[26]

4. *antiterorizam* – koji posebno nakon 11. rujna 2001. za posljedicu ima donošenje novih ili izmjene postojećih zakona kojima se daju sve veće ovlasti redarstvenim vlastima, provođenje masovnog nadzora i zadržavanje lokacijskih i prometnih podataka u elektroničkim komunikacijama, kao i druge mjere kojima se ograničava privatnost građana.

Tome svakako treba dodati različite pojavne oblike kiberkriminala i kiberterorizma kojima se mogu ugroziti i temeljna ljudska prava, kao što je pravo na život kao i sve veću "glad" za podacima kako u javnom, tako i privatnom sektoru, te nisku informatičku obrazovanost najvećeg broja korisnika. Istovremeno, to je popraćeno brojnim novim tehnologijama koje omogućavaju da se ograniči sloboda izražavanja i informiranja, te da se privatnost građana ugrozi na način kakav prije nije bio moguć.

Poznato je da najveća opasnost privatnosti prijeti od javnog sektora, odnosno vlasti koje ih, zahvaljujući svojem položaju i ulozi u društvu, mogu zakonski ograničiti ili zloporabom tehnologija ugroziti. Castells takve tehnologije naziva *tehnologijama kontrole* jer je „*kontrola informacija srž državne moći tijekom cijele povijesti*."[27]

5.1.4. Tehnologije kontrole

Tehnologije kontrole obuhvaćaju: tehnologije identifikacije, nadzora i istrage. *Tehnologije identifikacije* uključuju korištenje lozinki, cookie datoteka i procedura za provjeru autentičnosti. *Tehnologije nadzora* često se oslanjaju na tehnologije identifikacije i omogućuju lociranje korisnika, presretanje poruka, praćenje komunikacijskih tokova, te nadzor aktivnosti udaljenih računala. *Tehnologije istrage* vezane su uz izgradnju baza podataka prikupljenih kroz obradu rezultata nadzora i pohranjivanja informacija radi njihove daljnje obrade i uparivanja. Budući da se iste tehnologije mogu koristiti za različite svrhe (identifikaciju, nadzor ili istragu) gotovo je nemoguće napraviti jasno razgraničenje između njih.

a) Tehnologije identifikacije

U praksi brojnih zemalja sve se češće koriste različiti identifikacijski sustavi koji omogućavaju fizički ili daljinski pristup nekom računalnom sustavu, njegovim resursima i internetskim servisima. Trend rasta broja takvih sustava u neposrednoj je vezi s korištenjem visokih tehnologija ali i sa sve većom ponudom digitalnih usluga i sadržaja od strane javnog i privatnog sektora.

---

[26] Privacy International, *Privacy & Human Rights 1999*, http://www.privacyinternational.org/survey/summary.html (04.12.2000.)

[27] Castells, M., *Internet galaksija*, Naklada Jesenski i Turk, Zagreb, 2003., str. 188.

U virtualnom svijetu čovjek ostavlja elektronički trag o svom prisustvu, svojim navikama i interesima bilo na tuđim ili vlastitim računalnim sustavima. Takav je npr. slučaj s "kolačićima" (engl. Cookies) – tekstualnim informacijama pohranjenim u formi datoteka na disku našeg kompjutora kada posjetimo neku Internet stranicu. Takve informacije između ostalog omogućavaju: automatsko spajanje na web poslužitelj, izbor onoga što želimo vidjeti na web stranicama, prikazivanje željenih informacija bez dodatnog traženja, te prikazivanje oglasa i drugih sadržaja koji nas zanimaju. No, istovremeno oni sadrže podatke o našim navikama, sklonostima, interesima te se kao takvi mogu zlorabiti od strane onih kojima su te informacije dostupne.

Također, prividna nevidljivost i udaljenost na Internetu stvara kod korisnika osjećaj anonimnosti i sigurnosti, pa često i sami daju osobne podatke ili poduzimaju one radnje koje u fizičkom svijetu nikada ne bi. Tome posebno pridonose tzv. web registracijski formulari koji se ispunjavaju kako bi se moglo pristupiti nekim Internet stranicama, odnosno sadržajima koji se na njima nude. Prikupljanje, povezivanje i analiziranje takvih podataka uz pomoć informatičke tehnologije, te njihovo kombiniranje s već postojećim podacima omogućavaju stvaranje *profila* velikog broja ljudi. Zato ne iznenađuje da je sve veći broj tvrtki i pojedinaca, tzv. informacijskih brokera, koji prodajom osobnih podataka do kojih su došli najčešće nesmotrenošću korisnika njihovih usluga ili kupaca, ostvaruju značajan profit. Od takvih aktivnosti nisu izuzeti ni maloljetnici i djeca od kojih se, zbog njihove lakovjernosti, lako dobivaju podaci o obiteljskim prilikama. Tržište osobnih informacija, skriveno od pogleda javnosti, već je 1999. po nekim procjenama premašilo vrijednost od 1,5 milijardi dolara.[28] Danas, kada se ti podaci pribavljaju na zakonit ili nezakonit način, putem socijalnih mreža i drugih internetskih servisa, nemoguće je utvrditi njegovu vrijednost. Osim za marketinške potrebe, ovakvi podaci mogu dovesti i do tzv. "krađe identiteta" i lažnog predstavljanja, pri čemu se oni najčešće zlorabe za vršenje raznih kaznenih djela poput kompjutorske prijevare. Istovremeno, sve je veća količina osobnih podataka koji se o korisnicima Interneta prikupljaju na brojnim web stranicama, što nije popraćeno adekvatnim mjerama zaštite. Opasnost je da te podatke koriste i potencijalni poslodavci odlučujući o nečijem zaposlenju ili pak kriminalci radi iznude. Otvaraju se tako i mogućnosti stvaranja tzv. "podatkovnih utočišta" (*data haven*) ili "kriminalnih podatkovnih utočišta" (*criminal data haven*), u manje razvijenim zemljama s nepostojećom ili nedostatnom zakonskom regulativnom. Ovakve "rajeve podataka", s golemim bankama podataka koje sadrže i najosjetljivije osobne informacije s najrazličitijih područja ljudske djelatnosti, poput financija, zdravstva, trgovine, saobraćaja, kulture i pravosuđa, moguće je iskoristiti bilo kada i u bilo koju svrhu od strane pojedinaca, grupa ili javne vlasti.

Profiliranje u najširem smislu tog pojma uključuje rudarenje (engl. *data mining*) velike količine podataka koji se prikupljaju u postupku skladištenja podataka (engl. *data warehousing*) da bi se potom donijeli zaključci o poveznicama između određenih sadržaja koji se odnose na konkretne osobe kako bi se postigao određeni cilj (npr. da se osoba ponaša na određeni željeni način).[29] Pritom se koriste različite moderne tehnologije kao što su nadzor i praćenje putem GPS tehnologija i dubinsko pregledavanje sadržaja paketa prometa koji se prenose mrežom (engl. *Deep Packet Inspection,* skraćeno: DPI), videonadzor i dr. Osim u komercijalne svrhe, profiliranje se koristi u svrhu borbe protiv teških kaznenih djela poput terorizma (npr. u kontekstu predviđanja terorističkih prijetnji i napada) ili pak nadzor korištenja i nezakonite distribucije autorskih djela, poput softvera, muzike i filmova. Postupci profiliranja

[28] Reidenberg, J.R., *Restoring Americans Privacy in Electronic Commerce*, 14 Berkeley Tech. L.J. 771 (1999).
[29] Dinant, J-M. *et al, Application of Convention 108 to the profiling mechanism: Some ideas for the future work of the consultative committee (T-PD)*,
http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/CRID_Profiling_2008_en.pdf, str. 3-4.

sve su popularniji i zato što ne podrazumijevaju pretjerano visoke troškove za postizanje željenih rezultata. Oni mogu uključivati i praćenje ponašanja pojedinaca tijekom njihova korištenja elektroničkih komunikacijskih usluga i usluga informacijskog društva kako bi se u odnosu na njih poduzimale ciljane radnje poput ponude personaliziranih oglasa (*online ciljano ili bihevioralno oglašavanje*). To je čest slučaj kod pružanja internetskih usluga koje su za korisnike besplatne i koje se u većoj ili manjoj mjeri financiraju na temelju suradnje davatelja navedenih usluga s oglašivačima. Takvo oglašavanje traži što veću predvidljivost mogućeg ponašanja pa prema tome i sve detaljnije podatke o ponašanju korisnika radi izrade što točnijeg profila. U razmatranju takvog oglašavanja posebna se pozornost, među ostalim, upućuje pitanju razmjene informacija o *online* ponašanju pojedinca unutar mreže većeg broja oglašivača.[30]

Posljednjih godina razmatraju se i pitanja u vezi s primjenom tehnologije *identifikacije putem radiofrekvencije* (dalje: RFID), posebice RFID uređaja i aplikacija za obradu osobnih podataka i povezivanje na komunikacijske mreže. Naime, ugradnjom RFID etikete svakoj se stvari dodjeljuje jedinstveni identitet. Riječ je o elektroničkom čipu s pohranjenim informacijama koji ima mogućnost komunikacije radiosignalima (radiovalovima) s RFID čitačem. Tako RFID čitač koji komunicira s etiketom može učitati, na primjer, svojstva stvari u kojoj je etiketa ugrađena. U RFID etiketi se također mogu pohranjivati osobni podaci koje RFID uređaji/aplikacije mogu čitati, odnosno obrađivati, a uz povezivanje na komunikacijsku mrežu ti se podaci mogu i dalje prenositi i obrađivati također i u, primjerice, javnoj elektroničkoj komunikacijskoj mreži. RFID tehnologija nije novost, no uslijed sve intenzivnije primjene RFID sustava i njihovu mogućnosti daljnjeg povezivanja na komunikacijske mreže i zatim obrade prenesenih podataka, posljednjih su godina na razini EU-a posebno aktualna nastojanja da se utvrde postupci ranog prepoznavanja i minimalizacije rizika koje njezina uporaba može imati na privatnost pojedinaca.[31]

b) Tehnologije nadzora

Razvoj visokih tehnologija dovelo je i do stvaranja takvih sustava koji omogućavaju masovno praćenje, nadzor i presretanje komunikacija, njihovu trajnu pohranu na digitalnim medijima i povezivanje s drugim podacima o nekoj osobi. Sustav nadzora elektroničke pošte pod nazivom *Carnivore* razvijen je za potrebe FBI-a u SAD. Iako se tvrdi da će se koristiti isključivo za istražne radnje, mogućnosti zloporabe izazvale su veliku bojazan i kritike američke javnosti. Ovim se sustavom automatski pregledavaju i pohranjuju sve elektroničke poruke koje sadrže neku od prethodno određenih ključnih riječi kao i podaci o njihovim pošiljaocima. Istovremeno, policije brojnih zemalja pokazale su velik interes za uvođenjem i korištenjem takvog ili sličnog sustava i na svojem teritoriju.

Sličan sustav naziva *Echelon*, nastao je sporazumom Velike Britanije, SAD-a, Kanade, Australije i Novog Zelanda za vrijeme hladnog rata, s ciljem prikupljanja i razmjene obavještajnih podataka. Njegovim usavršavanjem stvoren je sustav za masovni nadzor komunikacija diljem svijeta bez obzira je li riječ o elektroničkoj pošti, fiksnoj ili mobilnoj telefoniji ili fax porukama ili različitim internet servisima. Ako poruke koje se na taj način prenose sadrže neku od ključnih riječi, komunikacija se automatski presreće a poruke se pohranjuju radi daljnje analize. Dovelo je to već devedesetih do reakcije Europske unije kako

---

[30] Art. 29 WP, *Opinion 2/2010 on online behavioural advertising*, 00909/10/EN, WP 171, 22.6.2010.

[31] *Commission Recommendation of 12.5.2009 on implementation of privacy and data protection principles in applications supported by RFID*, SL L 122, 16.5.2009., str. 47-51.; *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 12.1.2011, http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf (01.07.2015.).

bi se utvrdilo koristi li se isti i za elektroničku špijunažu građana zemalja članica, dok se u Francuskoj istražuje njegovo korištenje za potrebe gospodarske špijunaže. Dok Europski parlament istražuje Echelon, francuski list "Nouvel Observateur" objavio je da Francuska već deset godina špijunira satelitske komunikacije u potrazi za političko-diplomatskim, vojnim i industrijskim informacijama pomoću svoje špijunske satelitske mreže. I druge zemlje razvijaju ili već koriste slične sustave, a i tamo gdje ih još nema postoji interes vlasti za njih. Tako je u SAD-u za potrebe FBI-a razvijen sustav nadzor elektroničke pošte naziva *Carnivore*. Iako se tvrdi da će se koristiti isključivo za istražne radnje, mogućnosti zloporabe izazvale su veliku bojazan i kritike američke javnosti i udruga za zaštitu ljudskih prava. Ovim se sustavom automatski pregledavaju i pohranjuju sve elektroničke poruke koje sadrže neku od prethodno određenih ključnih riječi kao i podaci o njihovim pošiljaocima. Istovremeno, policije brojnih zemalja pokazale su velik interes za uvođenjem i korištenjem takvog ili sličnog sustava i na svojem teritoriju. Bojazan od ovakvih tehnologija i mogućnosti njihovih zloporaba navodi se i u izvještaju Europskog parlamenta pod nazivom *An Appraisal of the Technologies of Political Control* kao i izvještaju Komisije za ljudske slobode Europskog Parlamenta *Assessing the Technologies of Political Control*, iz 1997. godine, u kojima se izražava zabrinutost da se mnoge od ovih tehnologija koriste također i za praćenje aktivnosti disidenata, aktivista za ljudska prava, novinara, studentskih vođa, manjina, sindikalnih vođa i političkih oponenata.

Pravdajući to potrebama nacionalne sigurnosti i borbe protiv terorizma SAD tvrde da se takvi sustavi isključivo koriste radi prevencije i sprječavanja takvih pojava, što su Julian Assange, glavni urednik i osnivač WikiLeaksa, i Edward Snowden, bivši zaposlenik CIA-e, u više navrata argumentirano opovrgli objavom tajnih dokumenata iz arhiva obavještajnih agencija. U medijima su se od 2013. pojavili brojni članci o prisluškivanju građana i političkih čelnika diljem Europske unije od strane američke Agencije za nacionalnu sigurnost (NSA) i srodne britanske obavještajne agencije GCHQ. S druge strane, 2015. objavljeno je da su „ukradeni" osobni podaci i identifikacijski brojevi svih službenika u SAD-u, što je dovelo do povlačenja brojnih službenika iz veleposlanstava i drugih predstavništva širom svijeta.

No, opasnost je još veća jer se, osim za prisluškivanje čelnika drugih zemalja i progon političkih neistomišljenika, ove tehnologije mogu iskoristiti i za stvaranje kompleksnih dosijea o najširem krugu građana. U prilog tome govori i istraga španjolskog državnog odvjetništva koje je 2013. pokrenulo predistražne radnji radi sumnje da američke obavještajne službe špijuniraju više od 60 milijuna španjolskih građana.[32] Burno je odjeknula i vijest britanskog lista Daily Mail koji je 2012. objavio da je dvoje britanskih državljana zabranjen ulazak u SAD nakon što su na Twitteru prije putovanja objavili šalu da "idu uništiti Ameriku" i "iskopati Marlyn Monroe", što na britanskom slengu znači zabavu. Označeni kao „potencijalna prijetnja" uhićeni su nakon slijetanja u Los Angelesu, privedeni, satima ispitivani da bi nakon noći provedene u odvojenim ćelijama bili odvezeni natrag u zračnu luku i vraćeni zarakoplovom za Pariz.[33] Masovni nadzor komunikacija ne provodi se samo na socijalnim mrežama već i svim drugim internetskim servisima.

Istovremeno razvijeni su brojni jednostavniji i jeftiniji sustavi audio, audiovizualnog i komunikacijskog nadzora, namijenjeni prisluškivanju i praćenju zaposlenika i drugih osoba, te presretanju njihove elektroničke komunikacije, sve se više koriste na radnim i javnim mjestima, a moguće ih je povoljno nabaviti i putem Interneta. S obzirom na trend minijaturizacije i pad cijena takve opreme ona postaje dostupna velikom broju fizičkih i pravnih osoba. Zato ne

---

[32] HINA, 29.10.2013.

[33] http://www.dailymail.co.uk/news/article-2093796/Emily-Bunting-Leigh-Van-Bryan-UK-tourists-arrested-destroy-America-Twitter-jokes.html (10.02.2012).

iznenađuje činjenica da su nadzor i prisluškivanje zaposlenika od strane poslodavaca poprimili u razvijenim zemljama masovne razmjere. Osim prisluškivanja telefonskih razgovora i pregledavanja elektroničke pošte, nadziru se i navike zaposlenika na Internetu. Pravdajući to razlozima sigurnosti i tajnosti poslovanja, te sprječavanjem tzv. "krađe vremena", tj. korištenja informacijske tehnologije od strane ovlaštenih korisnika ali za vlastite potrebe, sve češće dolazi do otpuštanja radnika na temelju tako prikupljenih informacija.

Uz sve dobre strane, nesagledive su posljedice koje Internet stvari *(Internet of Things*) može imati na privatnost. Pametne kuće, pametni televizori, ugrađene web kamere, sustavi kućnog audiovizualnog nadzora i njihova sve veća povezanost putem interneta omogućava nam da daljinski upravljamo njima putem pametnih telefonima ili računala. Realna opasnost prijeti od toga da se takva komunikacije presretne ili da se preuzme nadzor nad tim uređajima. Na taj način u pitanje dolazi i naša prostorna privatnost.

c) Tehnologije istrage

Tehnologije istrage uključuju stvaranje golemih baza podataka sa osobnim podacima građana. Prvenstveno se odnose na takve baze u javnom sektoru, ali i na sve veći broj baza koje stvaraju hakeri, informacijski brokeri i kriminalci za svoje potrebe.

Nove tehnologije i digitalne usluge, ma koliko korisne bile, stvaraju nove mogućnosti zloporaba i otvaranju nova pitanja na koja pravna regulativa treba dati odgovor. Takav je slučaj sa *uslugom računarstva u oblaku* (engl. *cloud computing*) koja ovisno o pojedinom modelu podrazumijeva i pohranu osobnih podataka na poslužiteljima koji se nalaze pod kontrolom trećih strana (to jest davatelja tih usluga) i kojima korisnik koji je ugovorio korištenje te usluge pristupa daljinski najčešće ne znajući za lokaciju gdje su njegovi podaci pohranjeni. Štoviše, moguće je da se podaci prenose i na poslužitelje u trećim zemljama koje nemaju osiguranu odgovarajuću razinu zaštite osobnih podataka. Otvara to niz pitanja, kao što su: pitanja odgovornosti za provedbu zaštite u multinacionalnom okruženju, tko i u kojim uvjetima može pristupati navedenim podacima (uključujući redarstvene i sudske vlasti), vlasništva nad podacima pa sve do načina na koji se osigurava njihova zaštita od gubitka ili uništenja, odnosno bilo kojeg oblika zlouporabe, mjerodavnog prava i načina rješavanja sporova u multinacionalnom okruženju. Ta se pitanja intenzivno razmatraju na razini EU-a osobito u kontekstu jedinstvene europske strategije za razvoj računalstva u oblaku koja je donesena 2012. g.[34]

Posebno su opasne moguće zloporabe tzv. *biometrije* kao postupka "prikupljanja, obrađivanja i pohranjivanja podataka o čovjekovim fizičkim karakteristikama za potrebe identifikacije i autorizacije"[35]. Ove se metode temelje na fizičkim ili karakternim osobinama neke osobe, a najčešće se koriste za identifikaciju korisnika pri pristupu objektima, prostorijama, računalnim sustavima ili pojedinim informacijskim resursima i servisima, kao i kod eventualnog utvrđivanja njihovih prava (ovlaštenja) nakon takvog pristupa. Takva su npr. razna tehnička i programska rješenja kojima se vrši identifikacija osoba putem otiska prstiju, otiska dlana, potpisa ili načina pisanja, glasa, snimanjem zjenice oka ili načina i jačine pritiska na tipkovnicu. Pored dobrih strana, jer takva rješenja predstavljaju vrlo pouzdanu metodu provjere identiteta pristupnika, stvaranje baza podataka sa fizičkim osobinama ljudi može se zlorabiti kako bi se povezali najrazličitiji podaci o pojedincu pohranjeni u različitim informacijskim i

---

[34] *Unleashing the Potential of Cloud Computing in Europe*, COM/2012/0529 final, 27.9.2012.

[35] Privacy International, *Privacy & Human Rights 1999*, http://www.privacyinternational.org/survey/summary.html (04.12.2000.), str. 1.

kompjutorskim sustavima diljem svijeta. Primjer toga su biometrijske putovnice i baze podataka u kojima su pohranjeni podaci o tome.

Zasigurno najopasniji oblik biometrije predstavlja tzv. DNA identifikacija usporedbom temeljnog genetskog materijala s onim koji je o građanima prethodno prikupljen i pohranjen u tzv. *genetičkim bazama podataka*. Budući da se u nekim zemljama već kreiraju takve baze podataka (npr. SAD, Njemačka, Kanada, Velika Britanija),[36] tome treba pristupiti iznimno oprezno jer se njihovom analizom može utvrditi ne samo sadašnje ili prošlo stanje, već i sklonosti neke osobe ka obolijevanju kao i njeno eventualno buduće zdravstveno stanje. Budući da su informacije roba kojom se sve više trguje, za očekivati je da će se i takvi podaci naći na tržištu. Na taj način može se dovesti velik broj ljudi u diskriminirajući odnos spram drugih, posebno kada je riječ o poslovima koje oni mogu obavljati.

Velika su očekivanja od tehnologije *trodimenzionalnog ispisa*. Kao što su Web 2.0 tehnologije omogućile da korisnici postanu aktivni kreatori sadržaja na Internetu, 3D pisači i trodimenzionalni ispis omogućavaju im da postanu kreatori tjelesnih stvari. Mogućnosti njihove primjene su brojne pa se tako od početnog stvaranja prototipova različitih proizvoda u industriji oni danas sve više koriste i u medicini, stomatologiji, arhitekturi, dizajnu, modi, gradnji te na brojnim drugim područjima. Iako se razvijaju već od osamdesetih godina, tek od nedavno su dostupni širem krugu građana. Istovremeno, sve su veće nedoumice i bojazan da bi njihov razvoj i korištenje mogao imati nesagledive posljedice za pojedince i društvo. Počev od gubitka radnih mjesta u proizvodnji, preko ugrožavanja prava intelektualnog vlasništva do još većih zloporaba. Tako je pomoću njih moguće izraditi oružje (prvi funkcionalni pištolj napravljen je uz pomoć 3D pisača 2013.), a radi se i na stvaranju ljudskih organa slažući ljudske stanice sloj po sloj. Otvara to mnoga moralna, pravna i etička pitanja na koje će trebati pravovremeno dati odgovor.

5.1.5. Aktivnosti na pravnoj zaštiti komunikacijske i informacijske privatnosti

Istovremeno s aktivnošću međunarodnih i regionalnih organizacija na pravnoj zaštiti osobnih podataka odvijala se i aktivnost brojnih zemalja na donošenju novih zakona. Treba naglasiti da izvještaji i studije nekih nacionalnih komisija nisu bile samo osnova za donošenje zakona o zaštiti podataka u pojedinim zemljama, nego su također doprinijeli pojašnjenju samog koncepta "privatnosti" i razvoju prava zaštite podataka.[37]

Prvi takav zakon donesen je u njemačkoj pokrajini Hessen 1970., a zatim 1973. u Švedskoj, 1974. u Sjedinjenim američkim državama, 1977. u Saveznoj republici Njemačkoj, 1978. u Austriji, Danskoj, Francuskoj i Norveškoj 1979. i 1982. u Luxemburgu, 1981. u Irskoj i Izraelu, 1982. u Australiji i Kanadi, 1984. u Velikoj Britaniji, 1987. u Finskoj, 1988. u Irskoj, Japanu i Nizozemskoj, 1991. u Portugalu, 1992. u Belgiji i Švicarskoj, 1992. i 1995. u Španjolskoj i 1997. u Italiji i Grčkoj. Dodatni zakoni o zaštiti podataka mogu se naći u mnogim zakonodavstvima (npr. Kanada, Savezna Republika Njemačka, Švicarska ili Sjedinjene Američke Države) kao i u mnogim posebnim zakonima koji reguliraju zaštitu privatnosti u

[36] *Ibid*., str. 2.
[37] *Databanks in a Free Society / Computers, Record keeping and Privacy /; Report of the Project on Computer Databanks of the Computer Science and Engineering Board*, Nacional Academy of Sciences. Quadrangle Books, 1972.

područjima od posebnog interesa (npr. u području telekomunikacija, policijskih podataka ili online usluga). U nekim je zemljama radi zaštite privatnosti došlo i do ustavnih promjena, kao npr. Brazilu (čl. 5 (0) X), Nizozemskoj (čl. 10), Portugalu (čl. 25) i Španjolskoj (čl. 18.4).

Od sedamdesetih godina, kada su počele zakonodavne reforme na području informacijske privatnosti, moguće je razlikovati dva različita pristupa zaštiti: opći ili cjeloviti i područni pristup.

Opći pristup - podrazumijeva donošenje sveobuhvatnog zakona o zaštiti osobnih podataka koji se temelje na osnovnim načelima utvrđenim u već spomenutim Smjernicama OECD-a iz 1980. i Europskoj konvenciji Vijeća Europe iz 1981. Karakterističan je za zemlje Europe. Primjenjuje se također i u Australiji, Novom Zelandu, Hong Kongu i Kanadi.Takvim zakonima određuju se stroga pravila u pogledu prikupljanja, obrade i prijenosa podataka, kako u javnom tako i u privatnom sektoru. O provođenju zakona brine se posebni javni službenik - povjerenik, ili ombudsman. Nadalje, ovim se zakonima "uređuje zaštita pojedinaca, a neki kao subjekt zaštite određuju i pravne osobe, kao što su sindikati i tvrtke...; svi daju pravo pristupa subjektu podataka, ali postoje razlike u postupcima ispravljanja netočnih podataka, kao i u stupnju angažiranja državnog autoriteta za zaštitu osobnih podataka."[38] Donošenje ovakvog, sveobuhvatnog zakona ne isključuje donošenje posebnih zakona ili propisa kojima se zaštita pruža na određenim, specifičnim područjima. Napokon, kao što smo već naveli, i samo Vijeće Europe donijelo je niz preporuka kojima se posebna zaštita pruža osobnim podacima u onim djelatnostima koje su od posebnog interesa, odnosno gdje se takvi podaci mogu zloporabiti u većoj mjeri.

Područni pristup - podrazumijeva donošenje posebnih zakona kojima se uređuju pojedini aspekti privatnosti, odnosno ona područja ili djelatnosti u kojima se pokaže veća potreba i interes za njenom zaštitom. Karakterističan je za SAD. Ne postoji jedan opći zakon već se prema potrebi, najčešće kada se već uoče moguće zloporabe, donosi poseban zakon ili nadopunjava neki postojeći kojim se regulira to područje. Tako su npr. u SAD doneseni The Federal Wiretap Statute, Electronic Communications Privacy Act, Privacy Protection Act,[39] kao i neki drugi zakoni. Problem s ovim pristupom je da zaštita najčešće kasni, kao što je to slučaj sa zdravstvenim i genetičkim podacima u SAD, jer ovaj pristup zahtijeva da se novo zakonodavstvo donese sa svakom novom tehnološkom inovacijom.[40] Najčešće ne postoji niti poseban službenik ili ured koji nadgleda provođenje zakona i zaštitu privatnosti već je to prepušteno građanima i njihovim udrugama ili samim pravnim osobama.

Ova dva pristupa moguće je kombinirati s različitim oblicima ***samoregulacije***. Samoregulacija podrazumijeva uspostavljanje pravila ponašanja i standarda od strane tvrtki i raznih udruženja proizvođača, davatelja usluga (korisnika podataka), te udruga kupaca i drugih korisnika usluga čiji se podaci prikupljaju. Polazi se od pretpostavke kako upravo ti subjekti imaju najveću korist od toga da se ojača povjerenje u Internet i elektroničko poslovanje, pa je očigledan njihov interes da se pruži zaštita potencijalnim kupcima, odnosno korisnicima njihovih usluga. Unatoč naporima brojnih organizacija i nevladinih udruga, prema nekim podacima ovakav oblik regulacije na Internetu nije polučio ozbiljnije rezultate jer nedostaju efikasni mehanizmi za sankcioniranje onih koji to zloporabe.[41]

[38] Brezak, M., *op.cit*. (bilj. 111), str. 87.

[39] O tim zakonima vidi više Street, F.L., *Law of the Internet,* Lexisx Law Publishing, Charlotesville, Virginia 1998., str. 98. i dalje.

[40] Privacy International, *Privacy & Human Rights 2000*, http://www.privacyinternational.org/survey/phr2000/overview.html (01.02.2002), str. 3.

[41] *Ibid.*

No u kombinaciji s opisanim pristupima samoregulaciju ne treba zapostaviti, jer je već i sam zahtjev da se na svim Internet stranicama, gdje se prikupljaju osobni podaci građana obavezno mora navesti uvjete i načine korištenja istih (politika privatnosti), obveza za onog koji takve podatke prikuplja te značajan doprinos jačanju svijesti o opasnostima koje prijete pojedincima kada daju svoje podatke drugima.

Ovome treba dodati i nastojanja industrije da razvije takve tehnologije koje će jamčiti sigurnost korisnicima i tako "zaštitu privatnosti staviti u njihove ruke".[42] Tehnička samopomoć je zasigurno jedna od bitnih komponenti zaštite privatnosti i sigurnosti komuniciranja na Internetu To se u prvom redu odnosi na korištenje raznih kriptografskih proizvoda, zatim usluga koje korisnicima omogućavaju anonimnost, kao i niza besplatnih programa kojima se u većoj ili manjoj mjeri štiti privatnost pri komuniciranju ili drugom korištenju informatičke tehnologije. Iako se primjenom takvih tehnologija ne može u cjelosti jamčiti privatnost podataka, mrežnog rada i komuniciranja, može se u kombinaciji sa cjelovitom pravnom zaštitom i samoregulacijom ipak postići zadovoljavajući stupanj sigurnosti i privatnosti korisnika.

Iz prethodnog možemo zaključiti da se pitanjima zaštite privatnosti pristupilo uglavnom jedinstveno, regulirajući ih pravno na jedan od dva opisana načina, bilo donošenjem jednog općeg zakona ili posebnih zakona i propisa na pojedinim područjima. Razlike, međutim, postoje na području kaznenopravne zaštite. Naime, dok su zemlje običajnog prava rijetko pribjegavale kaznenim sankcijama, zemlje kontinentalnog prava činile su to češće. Budući da je to protivno samoj *ultima-ratio* funkciji kaznenog prava, neki smatraju kako je u tom pogledu potrebno provesti dekriminalizaciju,[43] dok su drugi mišljenja kako je to, obzirom na sve veće informacijske potrebe javnog i privatnog sektora, te povećane tehničke mogućnosti zadiranja u privatnost građana, neopravdano.

Zaštita osobnih podataka područje je prava na čiji je razvoj u Republici Hrvatskoj osobito snažno utjecala relevantna prava stečevina EU-a. Posljednjih je godina upravo na razini prava EU-a prepoznata nužnost osiguravanja novog pravnog okvira, nužno podržanog tehnološkim rješenjima, koji će se učinkovito uhvatiti u koštac s brojnim novijim izazovima i rizicima globaliziranog digitalnog okruženja i brzog tehnološkog razvoja, a koji, među ostalim, omogućuju sve različitije, intenzivnije i rasprostranjenije aktivnosti obrade osobnih podataka. U navedenim je uvjetima, naime, nužno osigurati mehanizme smislene i doista učinkovite zaštite prava pojedinaca u vezi s obradom njihovih osobnih podataka. Neodvojivo od toga je i osiguravanje provedbe potrebnih sigurnosnih mjera radi zaštite podataka, mreža i informacijskih sustava, kao i primjerenog sustava sankcioniranja svih oblika zlouporaba.

5.2. Opći okvir zaštite osobnih podataka – uvodne napomene

U pravu Republike Hrvatske zaštita osobnih podataka uživa status temeljnog ljudskog prava od donošenja Ustava iz 1990. godine. Članak 37. Ustava propisuje sljedeće:

Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom.

---

[42] *Ibid.*

[43] Više u Sieber, U., *Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society*, Computer und Recht, 1995., str. 100.; Alaburić, V., *Mediji vs. privatnost – kritička analiza hrvatskog civilnog i kaznenog zakonodavstva*, Hrvatska pravna revija br. 3/2002, str. 16.

Zakonom se uređuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u državi.

Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovoga prikupljanja.

Međutim, na zakonskoj razini područje zaštite osobnih podataka nije bilo cjelovito uređeno sve do 2003. g. kada je donesen *Zakon o zaštiti osobnih podataka*[44], a kojime je između ostalog uspostavljeno domaće tijelo zaduženo za nadzor nad provedbom zaštite osobnih podataka u RH - *Agencija za zaštitu osobnih podataka* (dalje i kao: AZOP). Pretežit utjecaj na razvoj domaćeg zakonodavnog okvira zaštite osobnih podataka imao je prvi temeljni akt EU-a u području opće zaštite osobnih podataka - *Direktiva 95/46/EZ o zaštiti pojedinaca u pogledu obrade osobnih podataka i slobodnog kolanja takvih podataka* (Opća Direktiva o zaštiti osobnih podataka, dalje u tekstu: Direktiva ZOP).[45] Osim toga važno je istaknuti da je Republika Hrvatska 2003. g. potpisala *Europsku konvenciju o zaštiti pojedinaca u pogledu automatske obrade osobnih podataka* te istu ratificirala 2005. g., zajedno s *Dodatnim protokolom u vezi nadzornih tijela i međunarodne razmjene podatak*a.[46] Ta Konvencija sve do danas predstavlja jedini međunarodnopravno obvezujući instrument s objedinjenim temeljnim načelima zaštite osobnih podataka, a pristupaju joj i države koje nisu članice Vijeća Europe.

Posljednjih godina pravo na zaštitu osobnih podataka dobiva sve veću važnost osobito u pravnom sustavu EU-a. Naime, po stupanju na snagu Lisabonskog ugovora 2009. g. stvoreni su uvjeti za temeljite izmjene u dosadašnjem pristupu regulaciji zaštite osobnih podataka na razini prava Europske unije. Danas se tako Ugovorom o funkcioniranju EU-a (dalje: UFEU) svima jamči pravo na zaštitu osobnih podataka (čl. 16. st. 1), a riječ je i o samostalnom temeljnom pravu prema članku 8. Povelje o temeljnim pravima EU-a. U toj se odredbi utvrđuje i da se osobni podaci moraju obrađivati pošteno u za to utvrđene svrhe, na temelju pristanka osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi, utvrđenoj zakonom. Nadalje, svakome se jamči pristup prikupljenim podacima koji se na njega ili nju odnose, kao i pravo na njihov ispravak, te se utvrđuje da poštovanje navedenih pravila podliježe nadzoru neovisnog tijela. Posebno je važno istaknuti *novu pravnu osnovu za uređenje opće zaštite osobnih podataka* (čl. 16. st. 2. podstavak 1. UFEU-a) u skladu s kojom je Europska komisija početkom 2012. godine podnijela prijedlog Uredbe o općoj zaštiti osobnih podataka, koja bi zamijenila Direktivu ZOP. Poticaj za donošenje novog pravnog okvira osobito leži u činjenici da je važeći okvir zastario s obzirom na novije izazove koje za prava pojedinaca donosi nagli razvoj tehnologije te sve intenzivniji i kompleksniji uvjeti u kojima se obrađuju njihovi osobni podaci, pogotovo imajući u vidu obradu koja se odvija u digitalnom, globaliziranom okruženju.

Uredba 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka (Opća uredba o

[44] Narodne novine (NN) br. 103/03., 118/06., 41/08. i 130/11.; 106/12 – pročišćeni tekst.

[45] SL L 281/31, 23.11.1995. – izdanje na hrv .jeziku: 13/Sv. 007, str. 88-107., kako je izmijenjena Uredbom br. 1882/2003 od 29.9.2003. o prilagodbi odredbi u vezi s odborima koji pomažu Komisiji u obavljanju njezinih provedbenih ovlasti predviđenih aktima koji podliježu postupku iz članka 251. Ugovora o EZ-u, s Odlukom Vijeća 1999/468/EZ, SL L 284/1, 31.10.2003. – izdanje na hrvatskom jeziku: 01/Sv.16, str. 96-148.

[46] Zakon o potvrđivanju Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola, NN MU 4/05; vidi i NN MU 6/05 i 12/05.

zaštiti podataka, dalje u tekstu i kao: Opća uredba ili Uredba)[47] donesena je 2016. g., a počela se primjenjivati u svim državama članicama pa tako i Hrvatskoj 25.5.2018. g. Uredba je stavila van snage ranije važeću Direktivu ZOP. Za razliku od Direktive ZOP, Uredba se primjenjuje izravno u svim državama članicama EU-a i u cijelosti je obvezujuća.

U Republici Hrvatskoj je nastavno na donesenu Opću uredbu donesen *Zakon o provedbi opće Uredbe o zaštiti podataka* (NN br. 42/18), koji je stupio na snagu 25. svibnja 2018. godine. Navedenim je zakonom stavljen izvan snage Zakon o zaštiti osobnih podataka i relevantni podzakonski propisi.

Paralelno s nastojanjima da se utvrde odrednice modernijeg i općenitog snažnijeg općeg pravnog okvira zaštite osobnih podataka EU-a, višegodišnji su napori u istom smjeru ulagani i na međunarodnopravnoj razini. To je rezultiralo značajnim izmjenama Europske konvencije o zaštiti pojedinaca u pogledu automatske obrade osobnih podataka (Konvencije 108), koje je u svibnju 2018. godine usvojilo Vijeće Ministara Vijeća Europe. Navedeni Protokol za izmjenu Konvencije 108 otvoren je za potpisivanje.[48]

5.3. Opća uredba o zaštiti podataka

5.3.1. Uvod

Opća uredba o zaštiti podataka utvrđuje tehnološki neutralna pravila u pogledu obrade osobnih podataka pojedinca i njihova slobodna protoka. Novim pravilima nastoji se u što je većoj mjeri ujednačiti europski domaći okvir zaštite osobnih podataka i na taj način osigurati što višu razinu pravne sigurnosti u aktivnostima obrade osobnih podataka i što više ujednačenu te provedivu zaštitu prava potrošača u EU-u, čiji su osobni podaci predmet tih obrada. Potreba što učinkovitije prilagodbe europskog pravnog okvira zaštite osobnih podataka izazovima novijih tehnologija i uvjetima digitalne ekonomije koje obilježavaju sve opsežniji i kompleksniji postupci obrade podataka pojedinaca, pogotovo u umreženom globaliziranom okruženju, predstavlja bitan povod za donošenje Uredbe. Osobito u spomenutom globalnom okruženju neometani je međunarodni prijenos osobnih podataka preduvjet cilju daljnjeg jačanja međunarodne trgovine i suradnje a koji, pokazuje se, dugoročno nije održiv bez istovremenog jačanja povjerenja potrošača u EU-u, odnosno bez istovremenog osiguravanja primjerene i provedive zaštite njihovih prava (u skladu s novim pravilima). Ispunjenje navedenih ciljeva očituje se i kroz postroženu odgovornost onih koji obrađuju osobne podatke ispitanika u EU-u, osnažene ovlasti nadzornih tijela za zaštitu osobnih podataka te novouvedene postupke namijenjene jačanju njihove međusobne suradnje i osiguravanju dosljedne primjene Uredbe u EU-u. Svako nadzorno tijelo za zaštitu podataka tijela (u Hrvatskoj je to Agencija za zaštitu osobnih podataka – AZOP) dužno je doprinositi dosljednoj

[47] SL 119, 04.5.2016, str. 1–88.; Ispravak Uredbe, SL L 127, 23.5.2018, str. 2–13.
[48] 128th Session of the Committee of Ministers - Ad hoc Committee on Data Protection (CAHDATA) – Protocol amending the Convention for the Protection of Individuals, CM(2018)2-addfinal, 18.5.2018.

primjeni Uredbe u EU-u. U tu svrhu nadzorna tijela surađuju međusobno, kao i s Europskom komisijom, te u određenim slučajevima s *Europskim odborom za zaštitu podataka* (EOZP) kao neovisnim tijelom EU-a s pravnom osobnošću, koje osigurava dosljednu primjenu Uredbe i savjetuje Komisiju o svim pitanjima u pogledu zaštite osobnih podataka u EU-u.[49] Europski odbor za zaštitu podataka, koji je zamijenio dosadašnju Radnu skupinu članka 29. (RS29), objavljuje na svojim mrežnim stranicama tumačenja Uredbe (kao smjernice, preporuke, najbolju praksu) u svrhu njezine dosljedne primjene diljem EU-a.[50]

5.3.2. Osnovni pojmovi

a) Osobni podatak, obrada osobnog podatka

Pojam osobnog podatka se kao i pojam obrade osobnog podatka ne mijenja značajno u Uredbi gledano u odnosu na Direktivu ZOP pa se u tom kontekstu i dalje smatraju relevantnima ranija tumačenja tih pojmova od strane Suda EU-a.

Osobni podatak je *svaki podatak koji se odnosi na pojedinca (fizičku osobu) čiji je identitet utvrđen ili se može utvrditi („ispitanik")*; pojedinac čiji se identitet može utvrditi je *fizička osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca* (čl. 4. t. 1. Uredbe). Nešto bitnije izmjene u Uredbi u odnosu na Direktivu ZOP predstavljaju novouneseni primjeri identifikatora na temelju kojih je moguće identificirati pojedinca, poput podataka o lokaciji i mrežnih identifikatora. U definiciji osobnog podatka kao „svakog podatka koji se odnosi na pojedinca čiji je identitet utvrđen ili se može utvrditi", pojam „svakog podatka" tumači se na način da obuhvaća razne vrste podataka, kako objektivne tako i subjektivne u obliku mišljenja ili ocjena, pod uvjetom da se oni „odnose" na dotičnu osobu.[51]

Obradu osobnog podatka podrazumijeva svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili na skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje

[49] Detaljnije o navedenom vidi u poglavlju VII. Uredbe. Vidi i čl. 15. Zakona o provedbi Opće uredbe kada je riječ o suradnji AZOP-a s nadzornim tijelima drugih država.
[50] Odbor je potvrdio i ranije izdane smjernice Radne skupine čl. 29. (dalje: RS29) za tumačenje Uredbe. Sva tumačenja Uredbe dostupna su na: European Data Protection Board, GDPR: Guidelines, Recommendations, Best Practices, https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en (neki prijevodi na hrvatski jezik dostupni su na: http://azop.hr/info-servis/detaljnije/smjernice).
[51] C-434/16, Peter Nowak protiv Data Protection Commissioner, EU:C:2017:994.

prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje (čl. 4. t. 2. Uredbe).

Neki od primjera obrade osobnih podataka prema praksi Suda EU-a jesu: uzimanje otisaka prstiju te njihovo spremanje na medij za pohranu podataka[52] te radnje gdje se podaci o prihodima i imovini fizičkih osoba (koji se prikupljaju iz dokumenata u javnoj domeni koje drže porezna tijela i obrađuju za objavljivanje) prenose na CD-ROM-u te obrađuju za potrebe SMS usluga (putem koje korisnici usluge mobilne telefonije mogu dobiti informacije o prihodima i imovini pojedinca, slanjem poruke s podacima o njegovom imenu i općini prebivališta).[53] Obradu osobnih podataka predstavljaju i aktivnosti davatelja usluge internet pretraživanja u vezi s osobnim podacima: pretraživanje osobnih podataka objavljenih na internetu, njihovo indeksiranje, privremenu pohranu i prikaz, tj. činjenje tih podataka dostupnima trećima prema određenom redoslijedu na stranici s rezultatima pretraživanja.[54] Nadalje, podaci koji se generiraju korištenjem elektroničkim komunikacijskim uslugama mogu se odnositi na identificirane fizičke osobe ili fizičke osobe koje mogu biti identificirane. Sud EU-a tako je potvrdio da zadržavanje prometnih podataka i podataka o lokaciji koji se odnose na korisnike elektroničkih komunikacijskih usluga, zajedno s podacima potrebnim za njihovu identifikaciju, predstavlja obradu osobnih podataka.[55]

Sud EU-a u svojoj je dosadašnjoj praksi tumačio pojam osobnog podatka prema ranijoj Direktivi ZOP, kroz primjenu dodatnih pojašnjenja (u uvodnim izjavama) kada je riječ o mogućnostima *neizravne identifikacije pojedinca u mreži*.[56] Navedeno se smatra primjenjivim i u kontekstu Uredbe, budući da u istoj mjeri i na isti način kao i Direktiva ZOP Uredba utvrđuje da se kod ispitivanja toga može li se identitet pojedinca utvrditi *trebaju uzeti u obzir sva sredstva radi izravnog ili neizravnog utvrđivanja identiteta za koja je po svemu sudeći izgledno da ih voditelj obrade ili bilo koja druga osoba može upotrijebiti*. Kako bi se utvrdilo je li po svemu sudeći izgledno da se koriste sredstva za utvrđivanje identiteta pojedinca, trebalo bi uzeti u obzir sve objektivne čimbenike, kao što su *troškovi i vrijeme potrebno za utvrđivanje identiteta, uzimajući u obzir i dostupnu tehnologiju u vrijeme obrade i tehnološki razvoj*.

To se primjenjuje se i u digitalnom okruženju u kojem pojedinci mogu biti pridruženi mrežnim identifikatorima koje pružaju njihovi uređaji, aplikacije, alati i protokoli (npr. IP adrese, identifikatori kolačića, oznake za radiofrekvencijsku identifikaciju). Tako mogu ostati tragovi koji se, posebno u kombinaciji s jedinstvenim identifikatorima i drugim informacijama koje primaju poslužitelji, mogu upotrijebiti za izradu profila fizičkih osoba i njihovu identifikaciju (uvodne izjave br. 26. i 30. Uredbe).

Naime, u *online* okruženju postoje informacije koje se smatraju dijelom digitalnog identiteta umreženog pojedinca, te postoji mogućnost da one pod određenim uvjetima predstavljaju njihove osobne podatke. Primjer su takvih informacija IP adrese kao jedinstvene

[52] C-291/12, Michael Schwarz protiv Stadt Bochum, EU:C:2013:670.

[53] C-73/07, Tietosuojavaltuutettu protiv Satakunnan Markkinapörssi Oy i Satamedia Oy, EU:C:2008:727.

[54] C-131/12, Google Spain SL, Google Inc. protiv AEPD, Mario Costeja González, EU:C:2014:317.

[55] Digital Rights Ireland Ltd (C-293/12) protiv Minister for Communications, Marine i Natural Resources i dr. i Kärntner Landesregierung (C-594/12) i dr., EU:C:2014:238.

[56] Time se potvrđuju ranija tumačenja RS29.: Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data, 01248/07/EN, WP 136, 20.6.2007.

identifikacijske oznake računala i drugih uređaja spojenih na internetu kojima se koriste pojedinci. Davatelji usluga pristupa internetu dodjeljuju IP adrese korisnicima svojih usluga i o tome vode evidenciju. IP adresa može biti statička ili dinamička. Dinamička IP adresa je promjenjiva, odnosno ona se mijenja svaki puta kada se korisnik spoji na internet, a kada mu se dodjeljuje nova adresa. U online uvjetima pretežito se koriste dinamičke IP adrese, no to ne znači istovremeno da u pravnom smislu ne postoji mogućnost utvrđivanja identiteta pojedinca na temelju takve adrese.

Sud EU-a do danas je u dva predmeta dao pravno obvezujuća tumačenja pojma osobnog podatka u vezi s digitalnim identifikatorima, konkretno IP adresom, sukladno Direktivi ZOP a osobito dodatnim pojašnjenjima iz uvodnih izjava te Direktive (a koje se, kako je već pojašnjeno, smatraju aktualnima i u kontekstu nove Uredbe). Tako je u predmetu C-70/10 (*Scarlet Extended SA protiv SABAM*)[57] Sud utvrdio da se IP adrese korisnika usluge pristupa internetu trebaju smatrati osobnim podacima *u odnosu na davatelje usluge pristupa internetu*. To stoga što davatelji tih usluga izdaju IP adrese kod spajanja na internet te vode bazu podataka korisnika usluga s podacima o izdanim IP adresama, kao i s njihovim identifikacijskim podacima kao što su ime, prezime i adresa.

U kasnijem je predmetu *C-582/14 (Patrick Breyer protiv Savezne Republike Njemačke*)[58] Sud utvrđivao pojam osobnog podatka s obzirom na dinamičke IP adrese koje prikupljaju, odnosno pohranjuju davatelji drugih internetskih usluga. U konkretnom se predmetu radilo o davatelju usluge internetskih medija (sadržaja), koji sam ne raspolaže dodatnim informacijama na temelju kojih je moguće identificirati pojedinca. Sud je utvrdio da okolnost da sam davatelj usluge ne raspolaže dodatnim informacijama uz pomoć kojih je moguća identifikacija osobe ne isključuje *per se* mogućnost da se dinamička IP adresa o kojoj je riječ za tog davatelja usluga pravno ne smatra osobnim podatkom. Sud je koristio tumačenje *neizravne identifikacije* pojedinca, utvrdivši na prvome mjestu da korištenje pojma „neizravno" od strane zakonodavca EU-a ima za cilj istaknuti da za pravni tretman informacije kao osobnog podatka *nije potrebno da ta informacija sama po sebi omogućuje identifikaciju osobe o kojoj je riječ*. Potom je tumačio mogućnost neizravne identifikacije pojedinca (u skladu s uvodnom izjavom br. 26. Direktive ZOP), a prema kojem će se raditi o osobnom podatku ako je identifikacija moguća korištenjem bilo kojeg sredstva kojeg bi voditelj obrade ili neka druga osoba razumno, tj. opravdano mogla koristiti. Prema tome, nije potrebno da se sve informacije koje omogućuju identifikaciju osobe o kojoj je riječ nalaze u posjedu samo jedne osobe. Međutim, identifikacija neće biti moguća i stoga se neće raditi o osobnom podatku ako je identifikacija osobe o kojoj je riječ *zabranjena zakonom ili ako je ona neostvariva u praksi*, npr. ukoliko bi zahtijevala nerazmjerne napore u pogledu vremena, troškova i rada, tako da se rizik identifikacije u stvarnosti čini neznatnim. U konkretnom primjeru Sud je utvrdio, međutim, da postoje pravni putevi koji omogućuju davatelju usluge internetskih medija da se obrati, *osobito u slučaju kibernetskih napada*, nadležnom tijelu kako bi ono poduzelo korake za identifikaciju pojedinca, odnosno za dobivanje tih informacija od davatelja usluge pristupa internetu i za pokretanje kaznenog postupka. Sukladno tome utvrdio je kako davatelj usluga internetskih medija raspolaže sredstvima koja se mogu opravdano koristiti za identifikaciju pojedinca na temelju pohranjenih IP adresa uz pomoć drugih osoba, konkretno nadležnog tijela i davatelja usluge

[57] C-70/10, Scarlet Extended SA protiv SABAM, EU:C:2011:771.
[58] C-582/14, Patrick Breyer protiv Savezne Republike Njemačke, EU:C:2016:779.

pristupa internetu. Prema tome, dinamička IP adresa koju pohranjuje davatelj usluga internetskih medija kod posjeta njegovim internetskim stranicama predstavlja u odnosu na tog davatelja usluge osobni podatak, ako isti raspolaže pravnim sredstvima koji mu omogućuju identifikaciju pojedinca uz pomoć dodatnih informacija, a kojima raspolaže davatelj usluge pristupa interneta tog pojedinca.

b) Voditelj obrade

Prvenstvena je uloga pojma voditelja obrade utvrđivanje toga tko će biti odgovoran za usklađenost postupanja s propisima o zaštiti osobnih podataka, kao i načina na koji ispitanici mogu ostvarivati svoja prava u praksi (raspodjela odgovornosti).[59] Radi se o fizičkim ili pravnim osobama, tijelima javne vlasti, agencijama ili drugim tijelima, koji sami ili zajedno s drugima određuju svrhe i sredstva obrade osobnih podataka (čl. 4. t. 7. Uredbe). U slučaju postojanja više voditelja obrade, dakle voditelja obrade koji zajedno s drugima određuju svrhe i sredstva obrade, oni se nazivaju *zajedničkim voditeljima obrade.*

U situacijama zajedničkih voditelja obrade se u praksi prema ranijem okviru javljao čitav niz otvorenih pitanja, poglavito oko obveza i odgovornosti svih osoba koje su na pojedine načine uključene u postupak obrade. Ranije neregulirana ta su se pitanja stoga morala izričito urediti Uredbom, koja u tom dijelu bitno nadograđuje Direktivu ZOP. Propisuje se tako da zajednički voditelji obrade *kroz međusoban dogovor* (osim ako su i u mjeri u kojoj su odgovornosti voditelja utvrđene pravom EU-a ili države članice) *transparentno* određuju svoje odgovornosti za poštovanje obveza iz Uredbe, posebno u odnosu na ostvarivanje prava ispitanika i pružanje informacija o obradi. U tom dogovoru moraju biti razvidne pojedinačne uloge i odnosi zajedničkih voditelja obrade u odnosu na ispitanike, a kojima mora biti dostupna i sama bit dogovora. Posebno je bitno istaknuti da ispitanik ima pravo ostvarivati svoja prava iz Uredbe u vezi sa svakim voditeljem obrade, kao i protiv svakog od njih, bez obzira na spomenuti dogovor (čl. 26. Uredbe).

c) Posebna kategorija osobnih podataka

Pojedini osobni podaci po svojoj su prirodi osjetljiviji (tzv. posebna kategorija osobnih podataka) i njihova obrada može dovesti do većih rizika za temeljna prava i slobode ispitanika. Gledano u odnosu na Direktivu ZOP (i raniji Zakon o zaštiti osobnih podataka) Uredba proširuje definiciju te kategorije osobnih podataka. Radi se, naime, o osobnim podacima koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja ili članstvo u sindikatu, o genetskim podacima, biometrijskim podacima koji se obrađuju u svrhu jedinstvene identifikacije pojedinca, podacima koji se odnose na zdravlje, te o podacima o spolnom životu ili seksualnoj orijentaciji pojedinca (čl. 9. st. 1.).

[59] Article 29 Data Protection Working Party (RS29), Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN, WP 169, 16.2.2010., str. 4.; uvodna izjava br. 79. Uredbe.

Osim toga, Uredba uvodi i posebne definicije biometrijskih podataka, genetskih podataka i podataka koji se odnose na zdravlje.

Biometrijski podaci su osobni podaci koji su dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci (čl. 4. t. 14.). Kada je riječ o fotografijama treba skrenuti pozornost na pojašnjenje prema kojem obradu fotografija „ne bi trebalo sustavno smatrati obradom posebnih kategorija osobnih podataka jer su one obuhvaćene definicijom biometrijskih podataka samo pri obradi posebnim tehničkim sredstvima kojima se omogućuje jedinstvena identifikacija ili autentifikacija pojedinca“ (uvodna izjava br. 51.).

Genetski podaci su osobni podaci koji se odnose na naslijeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca, i koji su dobiveni osobito analizom biološkog uzorka dotičnog pojedinca (čl. 4. t. 13.).

Kada je riječ o podacima o zdravlju (koji su za razliku od biometrijskih i genetskih podataka već bili uključeni u posebnu kategoriju osobnih podataka prema ranijem okviru), Uredba uvodi definiciju istih podataka kao *podataka koji se odnose na zdravlje*. To su svi osobni podaci povezani s fizičkim ili mentalnim zdravljem pojedinca, uključujući pružanje zdravstvenih usluga, kojima se daju informacije o njegovu zdravstvenom statusu (čl. 4. t. 15.).

d) Izvršitelji obrade

U pogledu same definicije *izvršitelja obrade* Uredba ne odstupa od ranijeg okvira; radi se ovdje o fizičkim ili pravnim osobama, tijelima javne vlasti, agencijama ili drugim tijelima koji obrađuju osobne podatke *u ime voditelja obrade* (čl. 4. t. 8. Uredbe). Međutim, značajne izmjene u odnosu na dosadašnji okvir tiče se njihova pravnog tretmana, budući da se Uredba osim na voditelje obrade u nizu odredbi izravno primjenjuje i na izvršitelje obrade. Obveze koje izravno zahvaćaju i izvršitelje obrade uključuju, među ostalim: provedbu odgovarajućih tehničkih i organizacijskih mjera kako bi se osigurala odgovarajuća razina sigurnosti s obzirom na rizike (čl. 32.), izvješćivanje voditelja obrade nakon što sazna za povredu osobnih podataka (čl. 33.), vođenje pisanih evidencija kategorija aktivnosti obrade koje obavljaju za voditelja obrade (čl. 30. st. 2. *et seq.*), suradnju s nadzornim tijelom (čl. 31.), obvezu imenovanja službenika za zaštitu osobnih podataka u određenim slučajevima (čl. 37.) i dr. Osim toga važno je istaknuti da svaka osoba koja je pretrpila materijalnu ili nematerijalnu štetu zbog kršenja Uredbe ima pravo izravno zatražiti naknadu pretrpljene štete od izvršitelja obrade (čl. 82.), što nije do sada bio slučaj prema Direktivi ZOP (niti prema Zakonu o zaštiti osobnih podataka). Od daljnjih novosti u uređenju odnosa voditelja i izvršitelja obrade prema Uredbi valja naglasiti nadogradnju postojećih odredbi Direktive ZOP kada je riječ o takvu povjeravanju poslova obrade osobnih podataka, kao i značajno postrožene uvjete i odgovornost u takvim slučajevima (čl. 28., uvodna izjava br. 81.).

Prva bitna izmjena u tom smislu tiče se odgovornosti voditelja obrade u odnosu na izbor izvršitelja obrade. Naime voditelji obrade prema Uredbi smiju angažirati samo izvršitelje obrade koji jamče (osobito u pogledu stručnog znanja, pouzdanosti i resursa, sukladno dodatnim pojašnjenjima) *provedbu odgovarajućih tehničkih i organizacijskih mjera na način da je obrada u skladu s Uredbom i da se njome osigurava zaštita prava ispitanika*.

Nadalje, gledano u odnosu na Direktivu ZOP značajno se proširuje opseg odredbi koje moraju biti dio ugovora na temelju kojeg se izvršitelj obrade obvezuje prema voditelju (odnosno drugog pravnog akta u skladu s pravom EU-a ili pravom države članice), a koji mora sadržavati *predmet i trajanje obrade, prirodu i svrhu obrade, vrstu osobnih podataka i kategoriju ispitanika te obveze i prava voditelja obrade*. Spomenutim ugovorom odnosno drugim pravnim aktom (koji kao i do sada mora biti u pisanom obliku, što uključuje i elektronski oblik), mora se utvrditi osobito da izvršitelj obrade:

(1) obrađuje osobne podatke samo prema zabilježenim uputama voditelja obrade, među ostalim s obzirom na prijenose osobnih podataka trećoj zemlji ili međunarodnoj organizaciji, osim ako to nalaže pravo EU-a ili pravo države članice kojem podliježe izvršitelj obrade (u tom slučaju izvršitelj obrade izvješćuje voditelja obrade o tom pravnom zahtjevu prije obrade, osim ako se tim pravom zabranjuje takvo izvješćivanje zbog važnih razloga od javnog interesa);

(2) osigurava da su se osobe ovlaštene za obradu osobnih podataka obvezale na poštovanje povjerljivosti ili da podliježu zakonskim obvezama o povjerljivosti;

(3) poduzima sve potrebne mjere u skladu s Uredbom o sigurnosti obrade (čl. 32.);

(4) poštuje propisane uvjete za angažiranje drugog izvršitelja obrade (čl. 28. st. 2. i 4.);

(5) uzimajući u obzir prirodu obrade, pomaže voditelju obrade putem odgovarajućih tehničkih i organizacijskih mjera, koliko je to moguće, da ispuni obvezu voditelja obrade u pogledu odgovaranja na zahtjeve za ostvarivanje prava ispitanika (informacije o obradi te pravo na pristup, ispravak, brisanje, ograničenje obrade, pravo na prenosivost osobnih podataka, pravo na prigovor i automatizirano pojedinačno donošenje odluka);

(6) pomaže voditelju obrade u osiguravanju usklađenosti s obvezama oko sigurnosti podataka, postupaka procjena učinaka na zaštitu podataka i prethodnih savjetovanja (čl. 32.-36.), uzimajući u obzir prirodu obrade i informacije dostupne izvršitelju obrade;

(7) po izboru voditelja, briše ili vraća voditelju obrade sve osobne podatke nakon dovršetka pružanja usluga vezanih za obradu te briše postojeće kopije osim ako je obveza njihove pohrane propisana pravom EU-a ili države članice;

(8) voditelju obrade stavlja na raspolaganje sve nužne informacije za dokazivanje poštovanja svojih obveza (čl. 28.) i koje omogućuju revizije, uključujući inspekcije, koje provodi voditelj obrade ili drugi revizor kojeg je ovlastio voditelj obrade, te im doprinose. S ovime je u vezi i novouvedena obveza izvršitelja obrade da odmah obavijesti voditelja obrade ako smatra da je koja njegova uputa protivna Uredbi ili drugim pravilima zaštite osobnih podataka EU-a, odnosno države članice.

Pitanje angažmana *podizvođača* kao drugog izvršitelja obrade, kojeg prvi izvršitelj želi angažirati za obavljanje pojedinih njemu povjerenih poslova obrade od strane voditelja, bitno je pitanje koje se vrlo često javlja u praksi, a koje nije bilo uređeno ranijim okvirom. Uredbom se taj propust ispravlja na način da se utvrđuje da će taj angažman biti dopušten samo ako ga

je *prethodno pisano odobrio voditelj obrade*. Nadalje, taj drugi izvršitelj (podizvođač) mora biti podvrgnut *istim obvezama* kao i (prvi) izvršitelj obrade prema ranije spomenutom ugovoru, odnosno drugom pravnom aktu između voditelja i izvršitelja obrade. To se poglavito odnosi na obvezu davanja jamstava za provedbu odgovarajućih tehničkih i organizacijskih mjera kako bi obrada bila usklađena s Uredbom. Ne ispunjava li drugi izvršitelj obrade (podizvođač) svoje obveze zaštite podataka, prvi izvršitelj obrade ostaje *u cijelosti odgovoran* voditelju obrade što se tiče (ne)izvršavanja obveza drugog izvršitelja.

Izvršitelj obrade i bilo koja osoba koja djeluje pod vodstvom voditelja obrade ili izvršitelja obrade koja ima pristup osobnim podacima, *ne smije obrađivati te podatke ako to ne zatraži voditelj obrade, izuzev ako to nalaže pravo EU-a ili države članice* (čl. 29.). Ako izvršitelj obrade protivno Uredbi utvrđuje svrhu i način obrade osobnih podataka koje mu je voditelj obrade povjerio na obradu, *on će se smatrati voditeljem u pogledu te obrade i biti za istu u potpunosti odgovoran prema Uredbi* (čl. 28. st. 10.).

e) Primatelji, treće strane

Definicije primatelja i trećih strana prema Uredbi (čl. 4. točke 9. i 10.) ne razlikuju se od definicija prema ranijem pravnom okviru. Tako je **primatelj** fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo kojem se otkrivaju osobni podaci, neovisno o tome je li on treća strana. Ne smatraju se primateljima tijela javne vlasti koja mogu primiti osobne podatke u okviru određene istrage u skladu s pravom Unije ili države članice.

Treća strana je fizička ili pravna osoba, tijelo javne vlasti, agencija ili drugo tijelo, a koje nije: ispitanik, voditelj obrade, izvršitelj obrade ili bilo koja druga osoba ovlaštena za obradu osobnih podataka pod izravnom nadležnošću voditelja obrade ili izvršitelja obrade (kao što su to, na primjer, osobe zaposlene kod voditelja obrade ili izvršitelja obrade).

f) Izrada profila

„Izrada profila“ prema Uredbi je svaki oblik automatizirane obrade osobnih podataka koji se sastoji od uporabe osobnih podataka za ocjenu određenih osobnih aspekata povezanih s pojedincem, posebno za analizu ili predviđanje aspekata u vezi s radnim učinkom, ekonomskim stanjem, zdravljem, osobnim sklonostima, interesima, pouzdanošću, ponašanjem, lokacijom ili kretanjem tog pojedinca (čl. 4. točka 4.).

g) Privola

Stroži, detaljno propisani uvjeti u vezi s privolom kao jednom od propisanih pravnih osnova za zakonitu obradu osobnih podataka predstavljaju jednu od značajnijih novosti u Uredbi u

odnosu na raniji okvir.[60] Naime, kao i do sada obrada osobnih podataka može se temeljiti na privoli, a koju ispitanik prema Uredbi daje za obradu svojih osobnih podataka u jednu ili više posebnih svrha (čl. 6. st. 1a.). Privola se definira kao *svako dobrovoljno, posebno, informirano i* ***nedvosmisleno*** *izražavanje želja ispitanika kojim on izjavom ili jasnom potvrdnom radnjom daje pristanak za obradu osobnih podataka koji se na njega odnose* (čl. 4. t. 11.). Posebno je važno istaknuti propisano pravilo prema kojem je voditelj obrade taj koji snosi teret dokaza o valjano danoj privoli.

Dobrovoljnost davanja privole u posebnom je fokusu pa se tako propisuje i to da se kod ocjene toga je li privola bila dobrovoljna u najvećoj mogućoj mjeri uzima se u obzir je li, među ostalim, izvršenje ugovora (uključujući pružanje usluge) uvjetovano privolom za obradu osobnih podataka koja nije nužna za izvršenje tog ugovora (čl. 7.). Naime, ne može se smatrati da je privola dana dobrovoljno ako ispitanik nema istinski ili slobodan izbor ili ako nije u mogućnosti odbiti ili povući privolu bez posljedica. Prema dodatnim pojašnjenjima uvjet dobrovoljnog davanja privole nalaže i to da privola ne bi trebala biti valjana pravna osnova za obradu osobnih podataka kada postoji jasna neravnoteža između ispitanika i voditelja obrade, posebno ako je voditelj obrade tijelo javne vlasti i stoga nije vjerojatno da je s obzirom na sve okolnosti te posebne situacije privola dana dobrovoljno (uvodne izjave br. 42.-43.).

Privola se može dati označavanjem polja kvačicom pri posjetu internetskim stranicama, biranjem tehničkih postavaka *online* usluga tj. usluga informacijskog društva ili davanjem druge izjave ili ponašanja koje jasno pokazuje u tom kontekstu da ispitanik prihvaća predloženu obradu svojih osobnih podataka. Prema tome, *šutnja, unaprijed kvačicom označeno polje ili manjak aktivnosti* ne bi se smjeli smatrati privolom (uvodna izjava br. 32.).

Uredba utvrđuje i pravo ispitanika da u svako doba povuče privolu, kao i obvezu da ga se o toj mogućnosti obavijesti prije davanja privole. Što se *oblika davanja privole* tiče, ako je privola dana kao pisana izjava koja se odnosi i na druga pitanja, tada se zahtjev za privolu mora predočiti tako da ga se može jasno razlučiti od drugih pitanja, u razumljivom i lako dostupnom obliku uz korištenje jasnog i jednostavnog jezika. Svaki dio te izjave koji bi predstavljao povredu Uredbe neće bit obvezujuć. Uredbom se propisuje i *način povlačenja privole*, a koji se mora omogućiti na isto toliko jednostavan način za ispitanika kao i samo davanje privole.

h) Privola djeteta u kontekstu korištenja *online* usluga

[60] Detaljna tumačenja privole dostupna su u Smjernicama RS29 o privoli u skladu s Uredbom 2016/679, koje je prihvatio Europski odbor za zaštitu podataka (dalje: EOZP): 17/HR WP259 rev.01, 28.11.2017., zadnje mijenjane te donesene 10.4.2018., http://azop.hr/images/dokumenti/217/smjernice-o-privoli.pdf.

S posebnom pažnjom treba sagledati novosti u Uredbi kada je riječ o zaštiti prava djece, što se opravdava činjenicom da su djeca često manje svjesna rizika, posljedica i predmetnih zaštitnih mjera te svojih prava u vezi s obradom osobnih podataka (uvodna izjava br. 38.).

Države članice danas različito uređuju pitanje dobne granice djeteta kada je riječ o njihovu davanju valjane privole za obradu osobnih podataka, bilo posebno kroz propise o zaštiti osobnih podataka ili u kontekstu propisa koji se odnose na pitanja poslovne sposobnosti djece, najčešće vezano za sklapanje pravnih poslova. Što se tiče uvjeta za dobivanje privola djeteta Uredbom se uređuje pitanje privole samo u situaciji kada se obrada osobnih podataka djeteta temelji na privoli u kontekstu korištenja *online* usluga tj. usluga informacijskog društva (čl. 8.). Prema tome, samo u tom se slučaju Uredbom postavljaju ujednačeni okviri i to na način da se obrada osobnih podataka djeteta smatra zakonitom samo ako je privolu dalo dijete s navršenih najmanje 16 godina. Kada se radi o mlađem djetetu takva će obrada biti zakonita samo po privoli, odnosno odobrenju nositelja roditeljske odgovornosti. Uredba utvrđuje i obvezu voditelja obrade da uloži razumne napore kako bi provjerio je li privolu u navedenom slučaju dao nositelj roditeljske odgovornosti, uzimajući u obzir dostupnu tehnologiju. Prema dodatnim pojašnjenjima, privola nositelja roditeljske odgovornosti ne bi trebala biti nužna u kontekstu preventivnih usluga ili usluga savjetovanja koje su ponuđene izravno djetetu (uvodna izjava br. 38.). Ovim se pravilima ne utječe na opće ugovorno pravo država članica kao što su pravila o valjanosti, sklapanju ili učinku ugovora kada je riječ o djetetu.

Uredba ostavlja državama članicama mogućnost da domaćim zakonom predvide i nižu od postavljene dobne granice od 16 godina, ali zaključno s dobi od 13 godina. Drugim riječima, posebno uređena dob za privolu djeteta za obradu osobnih podataka pri korištenju usluga informacijskog društva ne smije biti niža od 13 godina. Domaćim su Zakonom o provedbi Opće uredbe uvedene posebne odredbe o privoli djeteta (koje ima prebivalište u Republici Hrvatskoj) za obradu osobnih podataka u vezi s njegovim korištenjem usluga informacijskog društva, na način da se za isto potvrdila dobna granica od 16 godina predviđena Uredbom (čl. 19.).

i) Pseudonimizacija

Uredba uvodi pojam pseudonimizacije u europski opći pravni okvir zaštite podataka, potičući primjenu tog postupka tijekom obrade osobnih podataka. Postupak pseudonimizacije podrazumijeva *obradu osobnih podataka na način da se ti podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se te informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi* (čl. 4. t. 5). Iako se u slučaju pseudonimiziranih podataka radi i dalje o osobnim podacima, primjena postupka pseudonimizacije može smanjiti rizike za ispitanike o kojima je riječ, te pomoći voditeljima obrade i izvršiteljima obrade u ispunjavanju njihovih obveza u vezi sa zaštitom podataka, što će se detaljnije pojasniti dalje u tekstu.

5.3.3. Materijalno područje primjene Uredbe[61]

Uredba se primjenjuje na obradu osobnih podataka koja se u cijelosti obavlja automatizirano te na neautomatiziranu obradu osobnih podataka koji čine dio sustava pohrane ili su namijenjeni biti dio sustava pohrane.

U određenim se slučajevima Uredba ne primjenjuje.

Uredba se ne primjenjuje na *obradu koju provode fizičke osobe isključivo tijekom osobnih ili kućnih aktivnosti*. Prema dodatnim pojašnjenjima (uvodnoj izjavi) radi se ovdje o aktivnostima koje nisu povezane s profesionalnom ili komercijalnom djelatnošću, kao npr. korespondencija i posjedovanje adresa. Kako se ovdje radi o odredbi istovjetnoj onoj iz ranijeg okvira, za njezino tumačenje ostaje relevantna ranija praksa Suda EU-a, a prema kojoj, primjerice, korištenje sustava videonadzora koji je fizička osoba ugradila u svoju kuću radi zaštite imovine, zdravlja i života vlasnika kuće, te taj sustav nadzire i javni prostor, *ne bi predstavljalo obradu podataka koja se provodi za obavljanje isključivo osobnih ili domaćih aktivnosti*.[62]

S druge strane, kao novost u odnosu na raniji okvir u dodatnim su pojašnjenjima Uredbe *aktivnosti društvenog umrežavanja te internetske aktivnosti poduzete u kontekstu takvih aktivnosti* nadodani novi primjeri osobnih i kućanskih *online aktivnosti* (na koje se Uredba ne primjenjuje). Međutim, kada je riječ o uslugama društvenih mreža Uredba će se svejedno primjenjivati na *voditelje obrade ili izvršitelje obrade koji pružaju sredstva za obradu osobnih podataka za spomenute osobne ili kućne aktivnosti*.

Nadalje, Uredba se (kao i dosadašnja Direktiva ZOP) ne primjenjuje na obradu osobnih podataka tijekom djelatnosti koja ne spadaju u opseg prava EU-a, kao što su djelatnosti u području zaštite nacionalne sigurnosti, kao ni na obradu koju obavljaju države članice kada obavljaju aktivnosti povezane sa zajedničkom vanjskom i sigurnosnom politikom EU-a (glava V. poglavlje 2. Ugovora o Europskoj uniji).

Osim toga, posebnim pravnim instrumentima EU-a zasebno se uređuju pojedina područja koja, prema tome, izlaze iz područja primjene Uredbe.

To je s jedne strane obrada koju obavljaju nadležna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja. Ovo je područje posebno uređeno novom *Direktivom (EU) 2016/680 o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP*), koja se primjenjuje od 6. svibnja 2018.g.[63]

---

[61] Detaljno vidi u čl. 2. te uvodnim izjavama br. 14-19. Uredbe.
[62] C-212/13, František Ryneš protiv Úřad pro ochranu osobních údajů, EU:C:2014:2428.
[63] SL L 119, 4.5.2016., str. 89-131.

Nadalje, na obradu osobnih podataka od strane institucija, tijela, ureda i agencija EU-a primjenjuje se *Uredba br. 45/2001 o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka*[64]. S obzirom na potrebu usklađivanja Uredbe br. 45/2001 s Općom uredbom, istu će zamijeniti nova uredba koja je trenutno u zakonodavnom postupku.[65] Kada je riječ o Uredbi br. 45/2001 potrebno je skrenuti pažnju na to da je njome uspostavljen *Europski nadzornik zaštite osobnih podataka*, koji je odgovoran za praćenje i osiguravanje primjene te Uredbe kao i drugih akata EU-a koji se odnose na zaštitu temeljnih prava i sloboda fizičkih osoba u vezi s obradom osobnih podataka od strane institucija ili tijela EU-a. Nadzornik savjetuje institucije i tijela EU-a u pogledu svih pitanja koja se tiču obrade osobnih podataka, a ima i pravo posredovanja pred Sudom EU-a. Značaj njegove funkcije očituje se i u obvezi Europske komisije da se s njime savjetuje kod usvajanja zakonodavnih prijedloga koji se odnose na zaštitu prava i sloboda u vezi s obradom osobnih podataka.

Posebna pravila o zaštiti osobnih podataka i privatnosti za sektor elektroničkih komunikacija propisana su *Direktivom 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija* (Direktiva o privatnosti i elektroničkim komunikacijama, dalje i kao: Direktiva o e-privatnosti ili Direktiva 2002/58/EZ).[66] Kada je riječ o obradi u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga u javnim komunikacijskim mrežama u EU-u (što je područje primjene te Direktive), Uredba ne propisuje dodatne obveze fizičkim i pravnim osobama kada su one već podvrgnute posebnim obvezama s istim ciljem sukladno ovoj Direktivi. Drugim riječima, Uredba će se primjenjivati na sva pitanja u vezi sa zaštitom temeljnih prava i sloboda u odnosu na obradu osobnih podataka u mjeri u kojoj ista ne podliježu posebnim obvezama istog cilja sukladno Direktivi o e-privatnosti (čl. 95. i uvodna izjava br. 173. Uredbe). Kako bi se pojasnio odnos između Uredbe i Direktive 2002/58/EZ te osigurala usklađenost s Uredbom, tu je Direktivu trebalo izmijeniti na odgovarajući način nakon donošenja Uredbe. Europska komisija početkom 2017. g. objavila je prijedlog *Uredbe o privatnosti i elektroničkim komunikacijama*, kojim se ova Direktiva stavlja van snage i koji akt je trenutno u zakonodavnom postupku.[67]

Pored svega navedenog treba napomenuti i to da se (u istoj mjeri kao Direktiva ZOP) Uredba ne primjenjuje na obradu *anonimnih informacija*. To su informacije koje se ne odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, odnosno to su podaci koji su učinjeni anonimnima na način da se identitet ispitanika ne može ili više ne može utvrditi (uvodna izjava br. 26.). Osim toga, Uredba se ne primjenjuje na *obradu osobnih podataka preminulih osoba,* iako države članice mogu predvidjeti pravila u vezi s obradom tih podataka (uvodna izjava br. 27.).

---

[64] SL L 8, 12.1.2001., str. 1-22.

[65] Europska komisija, Prijedlog Uredbe o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe br. 45/2001 i Odluke br. 1247/2002/EZ, COM(2017) 8 final, 2017/0002(COD), Bruxelles, 10.1.2017.

[66] Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), SL L 201, 31.7.2002., str. 37-47. - izdanje na hrvatskom jeziku: 13/Sv. 52, str. 111-121.

[67] Europska komisija, Prijedlog Uredbe o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama), COM(2017) 10 final, 2017/0003 (COD).

5.3.4. Teritorijalno područje primjene Uredbe

Uredbom se značajno širi dosadašnje teritorijalno područje primjene europskog pravnog okvira zaštite osobnih podataka.[68]

a) Obrada osobnih podataka u okviru aktivnosti poslovnog nastana voditelja obrade ili izvršitelja obrade u EU-u

Uredba se primjenjuje na *obradu osobnih podataka* ***u okviru aktivnosti poslovnog nastana*** *voditelja obrade ili izvršitelja obrade u EU-u* (neovisno o tome vrši li se obrada u EU-u ili ne).

Prema dodatnim pojašnjenjima u Uredbi (koji su istovjetni onima iz ranije Direktive ZOP), pojam *poslovnog nastana* znači djelotvorno i stvarno obavljanje djelatnosti putem stabilnih aranžmana, s time da pravni oblik aranžmana (podružnica, društvo kćer) nije odlučujući čimbenik u tom pogledu. Za potrebe tumačenja pojma poslovnog nastana te obrade osobnih podataka "u okviru aktivnosti" poslovnog nastana voditelja obrade i dalje se smatra relevantnom praksa Suda EU-a (koji je do sada tumačio odgovarajuće odredbe ranijeg okvira).

Tako je u predmetu *Google Spain* (C-131/12[69]) Sud utvrdio da se obrada osobnih podataka koja se obavlja u svrhu usluge pretraživača Google Search i kojom rukovodi poduzetnik sa sjedištem u trećoj zemlji (Google, Inc. - SAD) kao voditelj obrade, obavlja „u okviru aktivnosti" njegova poslovnog nastana u državi članici EU-a (Španjolskoj) *ako ima za cilj promociju i prodaju oglašivačkog prostora kojeg nudi pretraživač i služi za naplatu te usluge*. U tim su okolnostima aktivnosti pretraživača i njegova poslovnog nastana u Španjolskoj *neodvojivo povezane,* odnosno povezane su s oglašivačkim prostorom na način da usluga pretraživača bude *ekonomski isplativa*, a pretraživač je *istodobno sredstvo kojim se omogućuje ostvarenje tih aktivnos*ti. Nadalje, obradu osobnih podataka predstavljalo bi i samo njihovo prikazivanje na stranici s rezultatima pretraživanja. Kako je to prikazivanje rezultata popraćeno na istoj stranici prikazivanjem reklama povezanih s izrazima za pretraživanje, obrada osobnih podataka o kojoj je riječ smatra se da se obavlja *u okviru oglašivačke i trgovačke aktivnosti poslovnog nastana voditelja obrade na španjolskom teritoriju*. Prema tome, obrada osobnih podataka o kojoj je riječ ne mora se izravno vršiti od strane poslovnog nastana koji se nalazi u državi članici EU-a, već je dovoljno da se obavlja *u okviru aktivnosti* tog poslovnog nastana.

---

[68] Čl. 3., uvodne izjave br. 22-25. Uredbe. Za detaljan pregled u domaćoj literaturi rješenja Uredbe u odnosu na raniji okvir uz pregled bitne prakse Suda EU-a, vidi: Gumzej, Nina, Opća uredba o zaštiti podataka, rad u okviru projekta „Novi hrvatski pravni sustav" Pravnog fakulteta u Zagrebu, 2017, neobjavljeno, https://www.bib.irb.hr/951269.

[69] C-131/12, Google Spain SL, Google Inc. protiv AEPD, Mario Costeja González, EU:C:2014:317.

U kasnijem je predmetu C-230/14[70] Sud utvrdio da pojam „poslovnog nastana“ obuhvaća *svaku, čak i najmanju, učinkovitu i stvarnu aktivnost koja se obavlja putem stabilnih dogovora (aranžmana)*. Tako prisutnost i samo jednog zastupnika može u određenim okolnostima biti dovoljna da predstavlja stabilne aranžmane, ako zastupnik djeluje s dovoljnim stupnjem stabilnosti pomoću resursa potrebnih za pružanje konkretnih usluga o kojima je riječ u predmetnoj državi članici EU-a. Kriterij za utvrđivanje postojanja poslovnog nastana voditelja obrade u drugoj državi članici EU-a u odnosu na onu gdje je on osnovan, s jedne je strane *stupanj stabilnosti dogovora (aranžmana)*, a s druge *učinkovitost provedbe aktivnosti u toj drugoj državi članici*. Oba kriterija se prema Sudu moraju tumačiti *s obzirom na posebnu prirodu gospodarskih djelatnosti i pružanja usluga o kojima je riječ*. Radilo se ovdje o tvrtki osnovanoj u Slovačkoj (Weltimmo) koja je upravljala mrežnom stranicom za posredovanje nekretninama u Mađarskoj i koja je u tom kontekstu obrađivala osobne podatke oglašivača. Sud je utvrdio da je slovačka tvrtka (Weltimmo) ostvarila *stvarnu i učinkovitu aktivnost u Mađarskoj* s obzirom na obradu osobnih podataka u kontekstu aktivnosti njezina poslovnog nastana kao voditelja obrade u toj zemlji. Obrada osobnih podataka o kojoj je riječ tiče se objave osobnih podataka vlasnika nekretnina na Weltimmovim mrežnim stranicama za posredovanje nekretninama, te (u slučaju primjene) korištenja tih podataka radi izdavanja računa za oglase. Aktivnosti Weltimma koje se odnose na obradu osobnih podataka o kojoj je riječ uglavnom jesu bile usmjerene prema Mađarskoj: Weltimmo je upravljao mrežnim stranicama u Mađarskoj i one su bile sastavljene na mađarskom jeziku. Weltimmo je u Mađarskoj imao zastupnika, koji je nastojao pregovarati s oglašivačima ispunjenje neplaćenih tražbina, služio kao kontakt između Weltimma i oglašivača te zastupao Weltimma u upravnim i sudskim postupcima (koji se odnose na obradu osobnih podataka o kojima je riječ). Osim toga, Weltimmo je otvorio bankovni račun u Mađarskoj u svrhu naplate potraživanja i tamo je koristio poštanski pretinac radi upravljanja svakodnevnim poslovima.

b) Primjena Uredbe kada voditelj obrade /izvršitelj obrade nema poslovni nastan u EU-u

Nema li voditelj obrade ili izvršitelj obrade *poslovni nastan u EU-u* Uredba će se također primjenjivati u slučaju aktivnosti obrade osobnih podataka ispitanika u EU-u koje su povezane s *ponudom robe ili usluga tim ispitanicima* (neovisno o tome treba li ispitanik izvršiti plaćanje), *bilo s nadzorom tj. praćenjem njihova ponašanja unutar EU-a*.

Aktivnosti obrade osobnih podataka ispitanika u EU-u koje su povezane s *ponudom robe ili usluga tim ispitanicima* (neovisno o tome treba li ispitanik izvršiti plaćanje), jedna su od dvije moguće okolnosti koje će dovesti do primjene Uredbe kod obrade njihovih osobnih podataka koju vrši voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Uniji.

Dodatna pojašnjenja u Uredbi bitna su za pravilnu ocjenu navedene situacije, prema kojem je potrebno utvrditi *da li je očito namjeravano nuđenje usluga ili robe ispitanicima u Uniji* od strane takvog voditelja obrade ili izvršitelja obrade. Pritom se pojašnjava kako čimbenici kao što su sama dostupnost internetskih stranica (voditelja ili izvršitelja obrade) u EU-u ili dostupnost adresa elektroničke pošte i drugih kontaktnih podataka ili samo korištenje jezikom pojedine države članice a koji se ujedno općenito koristi u trećoj zemlji gdje voditelj obrade

[70] C-230/14, Weltimmo s. r. o. protiv Nemzeti Adatvédelmi és Információszabadság Hatóság, EU:C:2015:639.

ima poslovni nastan, neće sami po sebi dovesti do primjene Uredbe jer nedovoljno ukazuju na namjeravanu ponudu usluga i robe ispitanicima u EU-u. Međutim, prema Uredbi to jesu sljedeći čimbenici:

a) korištenje *jezikom*, odnosno *valutom* koja se inače koriste u jednoj ili više država članica EU-a *iako se ne radi o službenom jeziku, odnosno valuti u zemlji poslovnog nastana*;
b) spominjanje kupaca ili korisnika koji se nalaze u EU-u.

Osim toga, ponovno kada je riječ o voditelju ili izvršitelju obrade bez *poslovnog nastana u EU-u*, Uredba će se primjenjivati i kod aktivnosti obrade osobnih podataka ispitanika u EU-u koje su povezane s *nadzorom, tj. praćenjem njihova ponašanja unutar EU-a*. Kako bi se odredilo može li se aktivnost obrade smatrati praćenjem ponašanja ispitanika, trebalo bi utvrditi prati li se pojedince na internetu među ostalim mogućom naknadnom upotrebom tehnika obrade osobnih podataka koje se sastoje od izrade profila pojedinca, osobito radi donošenja odluka koje se odnose na njega ili radi analize ili predviđanja njegovih osobnih sklonosti, ponašanja i stavova.

U ovdje izloženim slučajevima primjene Uredbe kako na voditelja obrade tako i na izvršitelja obrade koji nemaju poslovni nastan u EU-u, navedeni voditelj obrade, odnosno izvršitelj obrade, dužan je pisanim putem imenovati predstavnika u Uniji (uz određene iznimke).[71]

c) Primjena Uredbe po osnovi međunarodnog javnog prava

Uredba će se primjenjivati i na obradu koju poduzima voditelj obrade koji nema poslovni nastan u EU-u, već na mjestu gdje se pravo države članice primjenjuje temeljem međunarodnog javnog prava (npr. u diplomatskom ili konzularnom predstavništvu države članice).

5.3.5. Zakonitost obrade

a) Osnove za obradu osobnih podataka

Obrada osobnih podataka mora se temeljiti na najmanje jednoj od Uredbom propisanih osnova kako bi bila zakonita (čl. 6., uvodne izjave br. 40-49.). Uz nekoliko manjih izmjena Uredbom propisane osnove odgovaraju onima u Direktivi ZOP. One su, kako slijedi:

1) privola ispitanika za obradu njegovih osobnih podataka u jednu ili više posebnih svrha;
2) nužnost obrade za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora;
3) nužnost obrade radi poštovanja pravnih obveza voditelja obrade;
4) nužnost obrade radi zaštite životno važnih interesa ispitanika ili druge fizičke osobe;

[71] Detaljnije vidi u čl. 27. u vezi s čl. 3. st. 2. Uredbe.

4) nužnost obrade za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;
(6) nužnost obrade za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, *osobito ako je ispitanik dijete*.

Kod obrade koja je nužna radi poštovanja pravnih obveza voditelja obrade (3) kao i kod obrade koja je nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade (5), navedene pravne osnove ili mjere (npr. pravna obveza voditelja obrade) utvrđuju se pravom EU-a ili države članice kojem voditelj obrade podliježe. One trebaju biti jasne i precizne, a njihova primjena predvidljiva osobama na koje se primjenjuju u skladu s praksom Suda EU-a i Europskog suda za ljudska prava.[72]

Legitiman interes kao osnova za obradu osobnih podataka ne smije prevladavati nad interesima, odnosno temeljnim pravima i slobodama ispitanika, pri čemu je potrebno pažljivo razmotriti razumna očekivanja ispitanika koja se temelje na njihovu odnosu s voditeljem obrade. Legitiman interes se kao osnova ne bi smjela primjenjivati kad obradu provode tijela javne vlasti pri izvršavanju svojih zadaća, imajući u vidu ranije navedenu obvezu propisivanja pravne osnove za obradu osobnih podataka koju provode tijela javne vlasti. Primjeri koji bi se prema pojašnjenjima iz Uredbe mogli podvesti pod osnovu legitimnog interesa voditelja obrade bili bi obrada osobnih podataka u svrhu: izravnog marketinga; sprečavanja prijevara; izvješćivanja nadležnog tijela o mogućem kaznenom djelu ili prijetnji javnoj sigurnosti te prijenosa osobnih podataka u tom kontekstu pod uvjetom poštovanja primjenjivih obveza čuvanja tajnosti podataka, te obrada u svrhu prijenosa osobnih podataka (između ostalih klijenata ili radnika) unutar grupe poduzetnika za unutarnje administrativne potrebe. U području elektroničkih komunikacija legitiman interes predstavljala bi obrada podataka radi sprečavanja neovlaštenog pristupa elektroničkim komunikacijskim mrežama i širenja zlonamjernih kodova te zaustavljanja napada „uskraćivanjem usluge", kao i u svrhu sprečavanja štete na računalnim i elektroničkim komunikacijskim sustavima.

b) Osnove za obradu posebnih kategorija osobnih podataka

Kada je riječ o zakonitosti obrade posebnih kategorija osobnih podataka, njihova je obrada načelno zabranjena, kao i prema dosadašnjem okviru. Međutim, Uredbom se proširuje opseg dopuštenih pravnih osnova za obradu tih podataka (čl. 9., uvodne izjave br. 51-56.). Ti se podaci iznimno smiju obrađivati, pod uvjetom ispunjenja koje od sljedećih osnova:

(1) ispitanik je dao izričitu privolu za obradu tih osobnih podataka za jednu ili više određenih svrha (osim ako se pravom Unije ili države članice propisuje da ispitanik ne može ukinuti spomenutu zabranu);
(2) obrada je nužna za potrebe izvršavanja obveza i ostvarivanja posebnih prava voditelja obrade ili ispitanika u području radnog prava i prava o socijalnoj sigurnosti te socijalnoj zaštiti u mjeri u kojoj je to odobreno u okviru prava Unije ili države

[72] Detaljno o uvjetima vidi u čl. 6. st. 2. i 3. te uvodnim izjavama br. 41. i 45. Uredbe.

članice ili kolektivnog ugovora u skladu s pravom države članice koje propisuje odgovarajuće zaštitne mjere za temeljna prava i interese ispitanika;

(3) obrada je nužna za zaštitu životno važnih interesa ispitanika ili drugog pojedinca ako ispitanik fizički ili pravno nije u mogućnosti dati privolu;

(4) obrada se provodi u sklopu legitimnih aktivnosti s odgovarajućim zaštitnim mjerama zaklade, udruženja ili drugog neprofitnog tijela s političkim, filozofskim, vjerskim ili sindikalnim ciljem te pod uvjetom da se obrada odnosi samo na članove ili bivše članove tijela ili na osobe koje imaju redovan kontakt s njom u vezi s njezinim svrhama i da podaci nisu priopćeni nikome izvan tog tijela bez privole ispitanika;

(5) obrada se odnosi na osobne podatke za koje je očito da ih je objavio ispitanik;

(6) obrada je nužna za uspostavu, ostvarivanje ili obranu pravnih zahtjeva ili kad god sudovi djeluju u sudbenom svojstvu;

(7) obrada je nužna za potrebe značajnog javnog interesa na temelju prava Unije ili države članice koje je razmjerno željenom cilju te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika;

(8) obrada je nužna u svrhu preventivne medicine ili medicine rada radi procjene radne sposobnosti zaposlenika, medicinske dijagnoze, pružanja zdravstvene ili socijalne skrbi ili tretmana ili upravljanja zdravstvenim ili socijalnim sustavima i uslugama na temelju prava Unije ili države članice ili u skladu s ugovorom sa zdravstvenim radnikom te u skladu sa sljedećim uvjetima i zaštitnim mjerama: navedene podatke obrađuje stručnjak ili se podaci obrađuju pod odgovornošću stručnjaka koji podliježe obvezi čuvanja profesionalne tajne sukladno pravu Unije ili države članice ili pravilima koja su odredila nadležna nacionalna tijela ili druga osoba koja također podliježe obvezi čuvanja tajne sukladno pravu Unije ili države članice ili pravilima koja su utvrdila nadležna nacionalna tijela;

(9) obrada je nužna u svrhu javnog interesa u području javnog zdravlja, kao što je zaštita od ozbiljnih prekograničnih prijetnji zdravlju ili osiguravanje visokih standarda kvalitete i sigurnosti zdravstvene skrbi te lijekova i medicinskih proizvoda, na temelju prava Unije ili države članice kojim se propisuju odgovarajuće i posebne mjere za zaštitu prava i sloboda ispitanika, posebno čuvanje profesionalne tajne;

(10) obrada je nužna u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe (u skladu s čl. 89. st. 1.) na temelju prava Unije ili države članice koje je razmjerno cilju koji se nastoji postići te kojim se poštuje bit prava na zaštitu podataka i osiguravaju prikladne i posebne mjere za zaštitu temeljnih prava i interesa ispitanika.

Pored navedenog Uredba dopušta državama članicama da zadrže ili uvedu dodatne uvjete, uključujući ograničenja s obzirom na obradu genetskih podataka, biometrijskih podataka ili podataka koji se odnose na zdravlje. Sukladno navedenom domaći je zakonodavac putem Zakona o provedbi Opće uredbe o zaštiti podataka posebno uredio pitanja obrade genetskih podataka i obrade biometrijskih podataka (čl. 20-24.).

c) Obrada osobnih podataka koji se odnose na kaznene osude i kažnjiva djela

Kao i prema Direktivi ZOP (no za razliku od ranijeg Zakona o zaštiti osobnih podataka) osobni podaci koji se odnose na kaznene osude i kažnjiva djela ne spadaju izrijekom u definiciju posebne kategorije osobnih podataka niti prema Uredbi. Njihova obrada jasno se uređuje

Uredbom u okviru zasebne odredbe (čl. 10.), prema kojem se ti podaci obrađuju samo pod nadzorom službenog tijela ili kada je obrada odobrena pravom Unije ili države članice kojim se propisuju odgovarajuće zaštitne mjere za prava i slobode ispitanika. Sveobuhvatni registar kaznenih osuda vodi se samo pod nadzorom službenog tijela vlasti.

5.3.6. Načela obrade osobnih podataka

Načela obrade osobnih podataka jesu:

(1) **zakonitost, poštenost i transparentnost** (engl. *lawfulness, fairness and transparency*): podaci se moraju obrađivati zakonito, pošteno i transparentno s obzirom na ispitanika;
(2) **ograničavanje svrhe** (engl. *purpose limitation*): osobni podaci moraju se prikupljati u posebne, izričite i zakonite svrhe te se dalje ne smiju obrađivati na način koji nije u skladu s tim svrhama (daljnja obrada u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, u skladu s člankom 89. stavkom 1. Uredbe ne smatra se neusklađenom s prvotnim svrhama);
(3) **smanjenje količine podataka** (engl. *data minimisation*): osobni podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe obrade;
(4) **točnost** (engl. *accuracy*): osobni podaci moraju biti točni i po potrebi ažurni. Mora se poduzeti svaka razumna mjera radi osiguravanja da se osobni podaci koji nisu točni, uzimajući u obzir svrhe obrade, izbrišu ili isprave bez odlaganja;
(5) **ograničenje pohrane** (engl. *storage limitation*): osobni podaci moraju se čuvati u obliku koji omogućuje identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se obrađuju. Osobni podaci mogu se pohraniti na dulja razdoblja ako će se oni obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe u skladu s čl. 89. st. 1. Uredbe, što podliježe provedbi primjerenih tehničkih i organizacijskih mjera propisanih Uredbom radi zaštite prava i sloboda ispitanika;
(6) **cjelovitost i povjerljivost** (engl. *integrity and confidentiality*): osobni podaci moraju se obrađivati na način kojim se osigurava njihova odgovarajuća sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera;
(7) **pouzdanost** (engl. *accountability*): voditelj obrade odgovoran je za usklađenost s načelima obrade osobnih podataka te je mora biti u mogućnosti dokazati.

Posebno je važno novouvedeno **načelo pouzdanosti**. I dok se prema ranijem okviru utvrđivala odgovornost voditelja (obrade) za osiguravanje usklađenosti s načelima obrade osobnih podataka, novouvedeno načelo pouzdanosti u Uredbi toj odgovornosti pridodaje i obvezu **dokazivanja te usklađenosti**. Voditelji obrade su tako dužni u skladu s načelom pouzdanosti dužni provoditi odgovarajuće i djelotvorne tehničke i organizacijske mjere kako bi osigurali i mogli dokazati da se obrada provodi u skladu s Uredbom. Te mjere utvrđuju se na način da se uzima u obzir *priroda, opseg, kontekst i svrha obrade osobnih podataka, kao i rizici različitih razina vjerojatnosti i ozbiljnosti za prava i slobode fizičkih osoba* (na koja obrada osobnih podataka utječe). Mjere mogu uključivati provedbu odgovarajućih politika zaštite podataka

(ako su razmjerne u odnosu na aktivnosti obrade) i one se moraju prema potrebi preispitivati i ažurirati. [73]

a) Obrada osobnih podataka u druge svrhe u odnosu na svrhu za koju su prvotno prikupljeni

Iako ranije navedeno načelo ograničenja svrhe nalaže da se osobni podaci prikupljeni u posebne, izričite i zakonite svrhe ne smiju dalje obrađivati na način koji nije u skladu s tim svrhama (uz iznimku daljnje obrade u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, u skladu s čl. 89. st. 1. Uredbe, a koja se ne smatra neusklađenom s prvotnim svrhama), Uredbom se posebno utvrđuje *postupak određivanja sukladnosti daljnje svrhe obrade podataka s prvom svrhom u koju su podaci prvotno prikupljeni* (čl. 6. st. 4., uvodna izjava br. 50.).

U tom će postupku voditelj obrade između ostalog trebati utvrditi: (1) svaku vezu između svrha prikupljanja osobnih podataka i svrha namjeravanog nastavka obrade; (2) kontekst u kojem su prikupljeni osobni podaci, posebno u pogledu odnosa između ispitanika i voditelja obrade; (3) prirodu osobnih podataka; (4) moguće posljedice namjeravanog nastavka obrade za ispitanike; (5) postojanje odgovarajućih zaštitnih mjera, koje mogu uključivati enkripciju ili pseudonimizaciju. Iznimke kada se utvrđivanje sukladnosti svrha neće trebati provoditi i kada će se obrada u drugu svrhu smatrati zakonitom jesu ako se obrada u drugu svrhu temelji na *privoli* ispitanika, ili na *pravu EU-a / pravu države članice*, no sve sukladno Uredbom propisanim uvjetima.

5.3.7. Prava ispitanika

Omogućavanje kontrole ispitanika nad njihovim osobnim podacima, kao što je između ostalog provjera obrađuju li se njihovi osobni podaci i ako da je li ta obrada zakonita, nužan su dio uređenog i učinkovitog sustava zaštite osobnih podataka. Relevantna prava ispitanika Uredbom se dodatno proširuju i razrađuju u odnosu na raniji pravni okvir.

a) Obavještavanje ispitanika o obradi osobnih podataka

U skladu s načelom poštenosti i transparentnosti, prema kojem se osobni podaci moraju obrađivati pošteno i transparentno s obzirom na ispitanika, Uredba utvrđuje detaljan opseg informacija koje se moraju pružiti ispitaniku u vezi s obradom njegovih osobnih podataka, osim ako i u mjeri u kojoj ispitanik tim informacijama već ne raspolaže.

[73] Detaljnije vidi u čl. 24. st. 1.-2. te uvodnim izjavama br. 74-76. Uredbe.

Opseg potrebnih informacija razlikuje se u odnosu na to prikupljaju li se informacije izravno od ispitanika (čl. 13.) ili ne (čl. 14.), te se uz iznimku ranije navedene prethodne raspoloživosti informacija u slučaju informiranja ispitanika od kojeg se podaci izravno ne prikupljaju utvrđuju i druge iznimke kada se propisane informacije iznimno ne trebaju dostaviti.

U nastavku se izlaže popis informacija koje je voditelj obrade dužan pružiti ispitaniku, s primjerima kako ih je objavilo domaće nadzorno tijelo – AZOP:

A. *Voditelj obrade dužan je ispitaniku pružiti sljedeće informacije u trenutku prikupljanja osobnih podataka (ako se podaci prikupljaju od njega)*:

1) o svom identitetu (kontakt podaci voditelja obrade;
2) o službeniku za zaštitu podataka (kontakt podaci službenika);
3) o svrsi i pravnoj osnovi za obradu osobnih podataka;
4) o primateljima ili kategorijama primatelja osobnih podataka (npr. HZZO, HZMO);
5) o prijenosu osobnih podataka 3. zemlji ili međunarodnoj organizaciji (izvan EU-a[74]; napomena: podaci se mogu kao i do sada slobodno prenositi unutar EU-a);
6) ako se obrada temelji na privoli: o pravu da se u bilo kojem trenutku povuče privola, a da to ne utječe na zakonitost obrade koja se temeljila na privoli prije povlačenja;
7) ako se obrada temelji na legitimnom interesu: o legitimnom interesu (npr. slanje *newslettera* korisnicima usluga, praćenje rada zaposlenika putem GPS sustava ukoliko se rad obavlja izvan poslovnih prostorija poslodavca);
8) o roku pohrane osobnih podataka, odnosno ako to nije moguće o kriterijima kojima se utvrđuje razdoblje pohrane (npr. evidenciju o radnicima poslodavac čuva trajno, dok je organizator nagradne igre osobne podatke sudionika dužan brisati/uništiti nakon završetka iste - protek svrhe);
9) o postojanju prava da se od voditelja obrade zatraži pristup osobnim podacima, ispravak, brisanje osobnih podataka ili ograničavanje obrade koja se na njega odnose, prava na ulaganje prigovora na obradu takvih podataka te na prenosivost njegovih podataka drugom voditelju obrade;
10) o pravu na podnošenje prigovora nadzornom tijelu;
11) o tome je li pružanje osobnih podataka zakonska ili ugovorna obveza ili zahtjev nužan za sklapanje ugovora te ima li ispitanik obvezu njihova pružanja i koje su moguće posljedice ako se takvi podaci ne pruže (npr. sklapanje ugovora o radu), te
12) o postojanju automatiziranog donošenja odluka, što uključuje izradu profila te smislene informacije o tome o kojoj je logici riječ, kao i važnost i predviđene posljedice takve obrade za ispitanika (npr.: izrada profila klijenata od strane kreditnih institucija u svrhu utvrđivanje njihove kreditne sposobnosti ili praćenje navika kupaca i izrade profila u svrhu marketinških ponuda).

[74] Taj prijenos dopušta se na prvome mjestu temeljem odluke Europske komisije o primjerenoj razini zaštite. Nema li je, prijenos je moguć uz ispunjenjenje posebnih zaštitnih mjera i ako su ispitanicima osigurana provediva prava te učinkovita sudska zaštita. Kao zadnja mjera Uredbom se utvrđuju pojedine druge mogućnosti (iznimke) koje omogućuju prijenos. Detaljno vidi u poglavlju 5. Uredbe, a za analizu u domaćoj literaturi vidi: Gumzej, Nina, Europski okvir zaštite osobnih podataka: aktualnosti, rad u okviru projekta „Novi hrvatski pravni sustav" Pravnog fakulteta u Zagrebu, neobjavljen, 2016., https://www.bib.irb.hr/951272, str. 10. *et seq*. Dodatno, u vezi čl. 49. Uredbe vidi smjernice EOZP-a: Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25.5.2018., https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

B. Ako osobni podaci nisu dobiveni od ispitanika, voditelj obrade dužan je ispitaniku pružiti osim gore navedenih informacija i *informacije o izvoru osobnih podataka*.[75]

b) Pravo na pristup

Ispitanik ima pravo dobiti od voditelja obrade potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi podaci obrađuju, pristup tim podacima i informacijama o: (1) svrsi njihove obrade; (2) kategorijama osobnih podataka; (3) primateljima ili kategorijama primatelja kojima su ti podaci otkriveni ili će im biti otkriveni, osobito primateljima u trećim zemljama ili međunarodnim organizacijama; (4) odgovarajućim zaštitnim mjerama ukoliko se njihovi podaci prenose u treću zemlju ili međunarodnu organizaciju (čl. 46.); (5) predviđenom razdoblju u kojem će podaci biti pohranjeni ili, ako to nije moguće, o kriterijima korištenima za utvrđivanje tog razdoblja; (6) postojanju prava da se od voditelja obrade zatraži ispravak ili brisanje osobnih podataka ili ograničavanje obrade osobnih podataka koji se odnose na ispitanika ili prava na prigovor na takvu obradu; (7) pravu na podnošenje pritužbe nadzornom tijelu; (8) postojanju automatiziranog donošenja odluka, što uključuje izradu profila te, barem u tim slučajevima, smislenim informacijama o tome o kojoj je logici riječ, kao i važnosti i predviđenim posljedicama takve obrade za ispitanika. Ukoliko se osobni podaci *ne prikupljaju od ispitanika*, on ima pravo dobiti i (9) svaku dostupnu informaciju o njihovu izvoru.[76]

c) Pravo na prigovor

Obrada osobnih podataka u svrhe izravnog marketinga

Obrađuju li se osobni podaci u svrhe izravnog marketinga, ispitanik ima pravo prigovora na takvu obradu u svakom trenutku i u tom se slučaju njegovi podaci više ne smiju obrađivati u tu svrhe. Radi se o pravu koji su ispitanici imali do sada prema ranijem okviru. Ispitanika se mora upoznati s ovim pravom najkasnije u trenutku prve komunikacije s istim, i to na jasan način i odvojeno od bilo koje druge informacije.

Obrada osobnih podataka koja se temelji na osnovi javnog interesa/izvršavanju službene ovlasti voditelja obrade, odnosno na osnovi legitimnog interesa voditelja obrade ili treće strane

---

[75] Važne napomene voditeljima obrade i izvršiteljima obrade vezano za primjenu Opće uredbe o zaštiti podataka, http://azop.hr/aktualno/detaljnije/obavijest-za-voditelje-i-izvrsitelje-obrade-ukidanje-sredisnjeg-registra.
Detaljno o obavještavanju i načelu transparentnosti prema Uredbi vidi u čl. 12.-14. i uvodnim izjavama br. 58-62., te smjernicama koje je potvrdio EOZP: Guidelines on transparency under Regulation 2016/679, 17/EN WP260 rev.01, 29.11.2017, zadnje mijenjane te usvojene 11.4.2018., https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

[76] Detaljnije vidi u čl. 15. te uvodnim izjavama br. 63-64. Uredbe.

U sljedeća dva slučaja ispitanik ima pravo uložiti prigovor na obradu s obzirom na osnovu koju voditelj obrade koristiti za obradu njegovih osobnih podataka. To se dopušta samo u dva slučaja i to ukoliko voditelj obrade obrađuje osobne podatke jer je:

(1) obrada nužna za izvršavanje zadaće od javnog interesa ili pri izvršavanju službene ovlasti voditelja obrade;
(2) obrada nužna za potrebe legitimnih interesa voditelja obrade ili treće strane, osim kada su od tih interesa jači interesi ili temeljna prava i slobode ispitanika koji zahtijevaju zaštitu osobnih podataka, osobito ako je ispitanik dijete.

Za razliku od situacije kada se podaci obrađuju u svrhe marketinga, a kada se smjesta po uloženom prigovoru podaci moraju prestati obrađivati u tu svrhu, u navedena dva slučaja voditelj obrade će ipak moći može nastaviti vršiti obradu, unatoč prigovoru, ali samo ako dokaže *uvjerljive legitimne razloge za obradu koji nadilaze interese, prava i slobode ispitanika ili radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva*. U suprotnom mora prestati s obradom. Ispitanika se mora upoznati s ovim pravom najkasnije u trenutku prve komunikacije s istim, i to na jasan način i odvojeno od bilo koje druge informacije.

Za razliku od rješenja prema ranijem okviru prema kojem bi obrada u takvom slučaju trebala prestati samo ako bi ispitanik koji je prigovor uložio ujedno i dokazao opravdanost svog prigovora, Uredba to više ne zahtijeva već prebacuje na voditelja obrade teret dokaza (u svrhu nastavka takve obrade unatoč prigovoru).

Obrada osobnih podataka u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe

U slučaju obrade osobnih podataka u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, ispitanik ima pravo prigovora na tu obradu na temelju svoje posebne situacije, osim ako je obrada nužna za provođenje zadaće koja se obavlja zbog javnog interesa. Radi se o posve novoj osnovi za prigovor u odnosu na dosadašnji pravni okvir.

U kontekstu služenja *online* uslugama tj. uslugama informacijskog društva ispitanik može ostvariti svoje pravo na prigovor automatiziranim putem koji se koristi tehničkim specifikacijama.[77]

d) Pravo na ispravak

Kada se o njima vode netočni osobni podaci, ispitanici imaju pravo na njihov ispravak od voditelja obrade, bez nepotrebnog odgađanja.[78]

[77] Detaljno o pravu na prigovor vidi u čl. 21. i uvodnim izjavama br. 69-70. Uredbe.
[78] Detaljno vidi u čl. 16. i uvodnoj izjavi br. 65. Uredbe.

e) Pravo na brisanje podataka

Pravo na brisanje osobnih podataka posljednjih je godina osobito aktualna tema s obzirom na sve intenzivniju obradu osobnih podataka na internetu, odnosno u digitalnom i globaliziranom okruženju. U tom je kontekstu kao preteču pojedinih novih rješenja u pogledu ovog prava prema Uredbi bitno ukratko prikazati presudu Suda EU-a u predmetu C-131/12 (Google Spain SL, Google Inc. protiv AEPD, Mario Costeja González, EU:C:2014:31), a koja je dovela do nove prakse internetskih pretraživača u kontekstu tzv. europskog *prava biti zaboravljen*. Iako se u ovom predmetu tumačila Direktiva ZOP i on se odnosio samo na praksu internetskih pretraživača, Uredba nadograđuje rješenja Direktive u vezi s pravom na brisanje osobnih podataka također u određenoj mjeri uzimajući u obzir navedenu presudu, a praksa internetskih pretraživača u pogledu ostvarivanja tzv. „prava na zaborav" sukladno istoj aktualna je i po stupanju na snagu Uredbe.[79]

Pravo na zaborav i internetski pretraživači

Naime, u G*oogle Spain* predmetu Sud EU-a tumačio je *inter alia* pitanje postojanja te opsega i uvjeta prava ispitanika da zatraži i ishodi brisanje svojih osobnih podataka iz indeksa, odnosno rezultata pretraživanja internet pretraživača. Presudio je da je davatelj usluge internet pretraživanja (konkretno Google) pod određenim uvjetima u svojstvu voditelja obrade osobnih podataka dužan poštovati pravo ispitanika na brisanje njegovih osobnih podataka na način da obriše poveznice prema internetskim stranicama trećih koje sadrže osobne podatke o kojima je riječ i to sve također pod pretpostavkama da ti podaci nisu prethodno ili istodobno izbrisani sa spomenutih internetskih stranica i da je njihovo objavljivanje na navedenim stranicama samo po sebi zakonito. To pravo ispitanik ima neovisno o postojanju štete za njega s obzirom na uključivanje informacije o kojoj je riječ u popis rezultata. Vrlo je važno imati na umu da se ovaj slučaj i presuda odnosi *isključivo na pretrage koje su povezane s imenom ispitanika*. Postavi li ispitanik zahtjev za brisanje njegovih osobnih podataka, a utvrdi se da *u ovom vremenskom trenutku* uključivanje poveznica prema internetskim stranicama s istinitim informacijama o njemu (koje su treće osobe zakonito objavile) nije u skladu s pravnim okvirom zaštite osobnih podataka, jer se s obzirom na sve okolnosti slučaja o kojem je riječ pokazuje da su te informacije neodgovarajuće ili da one nisu relevantne ili nisu više relevantne, odnosno da su suvišne u odnosu na svrhu obrade koju provodi davatelj usluge internet pretraživanja, te se informacije i poveznice trebaju obrisati iz popisa rezultata pretraživanja. Kod sagledavanja odnosa između prava ispitanika na poštovanje privatnog života i na zaštitu osobnih podataka, s jedne strane, te s druge, legitimnog interesa korisnika interneta koje moguće zanima pristup tim podacima (na temelju pretrage po imenu ispitanika), između njih je potrebno pronaći pravednu ravnotežu. Ta ravnoteža može se razlikovati od slučaja do slučaja s obzirom na prirodu informacija o kojima je riječ i njihovu osjetljivost za privatan život ispitanika, te interes javnosti za tu informaciju koji može varirati, osobito s obzirom na ulogu ispitanika u javnom životu.[80]

---

[79] Vidi npr. upute AZOP-a u vezi s pravom na zaborav u odnosu na pretraživač Google: http://azop.hr/zahtjevi-za-uklanjanje-osobnih-podataka/detaljnije/google-pravo-na-zaborav.

[80] Za detaljnu analizu u domaćoj znanstvenoj literaturi, vidi: Gumzej, Nina, Pravo na zaborav i globalni internet: izvršavanje zahtjeva za uklanjanje poveznica na pretraživačima, Društvo i tehnologija 2015, Opatija, Zbornik radova, str. 224-244., https://www.bib.irb.hr/786062.

Pravo na brisanje osobnih podataka – rješenja Uredbe

Slučajevi kada je obvezno brisanje

Ispitanik ima pravo od voditelja obrade ishoditi brisanje osobnih podataka koji se na njega odnose bez nepotrebnog odgađanja te voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako je ispunjen jedan od sljedećih uvjeta:

(1) osobni podaci više nisu nužni u odnosu na svrhe za koje su prikupljeni ili na drugi način obrađeni;

(2) ispitanik je povukao privolu na kojoj se obrada temelji, a ne postoji druga pravna osnova za obradu (također i kada je riječ o osobnim podacima djeteta prikupljenih u vezi s ponudom usluga informacijskog društva);

(3) ispitanik je sukladno Uredbi uložio prigovor: a) na obradu koja se temelji na osnovi javnog interesa/izvršavanja službene ovlasti voditelja obrade, odnosno na osnovi legitimnog interesa voditelja obrade ili treće strane (čl. 21. st. 1. Uredbe), a ne postoje jači legitimni razlozi za obradu, odnosno ispitanik je sukladno Uredbi uložio prigovor: b) na obradu u svrhe izravnog marketinga (čl. 21. st. 2. Uredbe);

(4) osobni podaci nezakonito su obrađeni;

(5) osobni podaci moraju se brisati radi poštovanja pravne obveze iz prava Unije ili države članice kojem podliježe voditelj obrade.

Pravo na brisanje posebno je bitno ako je ispitanik dao svoju privolu dok je bio dijete i nije bio u potpunosti svjestan rizika obrade, a kasnije želi ukloniti takve osobne podatke, osobito na internetu.

Brisanje javno objavljenih osobnih podataka

Ukoliko voditelj obrade mora obrisati osobne podatke koje je javno objavio (osobito na Internetu), on je dužan poduzeti razumne mjere, uključujući tehničke mjere, uzimajući u obzir dostupnu tehnologiju i trošak provedbe, kako bi obavijestio voditelje obrade koji obrađuju te osobne podatke da je ispitanik zatražio od tih voditelja obrade da izbrišu sve poveznice do njih ili kopiju ili rekonstrukciju tih podataka.

Iznimke

Bez obzira na ranije navedeno osobni podaci ne trebaju se brisati ako je njihova obrada nužna za ostvarivanje prava na slobodu izražavanja i na slobodu informiranja, radi poštovanja pravnih obveza, za izvršavanje zadaće od javnog interesa ili izvršavanje službene ovlasti voditelja obrade, na temelju javnog interesa u području javnog zdravlja, u svrhe arhiviranja od javnog

interesa, u svrhe znanstvenih ili povijesnih istraživanja, u statističke svrhe ili za postavljanje, ostvarivanje ili obranu pravnih zahtjeva.[81]

f) Pravo na ograničenje obrade

U praksi se mogu javiti situacije kada je potrebno privremeno ograničiti obradu osobnih podataka, primjerice do i u svrhu utvrđenja potrebnih činjenica u vezi sa zahtjevom ispitanika da se oni obrišu, ili zato što te podatke koji bi se inače trebali obrisati ipak treba iz određenih razloga pohraniti, no ne i dalje aktivno obrađivati. Radi se o institutu tzv. blokiranja koji je ranije već bio predviđen Direktivom ZOP (ne i domaćim okvirom), kao pravo koje je ispitanik mogao izvršavati u odnosu na voditelja obrade. Međutim, Direktiva nije definirala taj pojam niti odredila svrhe tj. odnosno okolnosti kada je blokiranje obrade potrebno i/ili opravdano. Stoga je bilo važno ovaj institut cjelovito i jednoznačno urediti na razini EU-a. Pojam koji se koristi u Uredbi je „*ograničenje obrade osobnih podataka*“, a definira se kao označavanje pohranjenih osobnih podataka s ciljem ograničavanja njihove buduće obrade (čl. 4. t. 3.). Ispitanik ima prema Uredbi pravo ishoditi od voditelja obrade ograničenje obrade njegovih osobnih podataka, u slučaju kada:

> (1) ispitanik osporava točnost osobnih podataka, na razdoblje kojim se voditelju obrade omogućuje provjera točnosti osobnih podataka;
> (2) obrada je nezakonita i ispitanik se protivi brisanju osobnih podataka te umjesto toga traži ograničenje njihove uporabe;
> (3) voditelj obrade više ne treba osobne podatke za potrebe obrade, ali ih ispitanik traži radi postavljanja, ostvarivanja ili obrane pravnih zahtjeva;
> (4) ispitanik je sukladno Uredbi uložio prigovor na obradu koja se temelji na osnovi javnog interesa/izvršavanju službene ovlasti voditelja obrade, odnosno na osnovi legitimnog interesa voditelja obrade ili treće strane (čl. 21. stavak 1. Uredbe), očekujući potvrdu nadilaze li legitimni razlozi voditelja obrade razloge ispitanika.

Kada se postigne ograničenje obrade osobnih podataka, ti se podaci smiju obrađivati samo*:*

(1) uz privolu ispitanika (uz iznimku pohrane), ili (2) za postavljanje, ostvarivanje ili obranu pravnih zahtjeva ili (3) zaštitu prava druge fizičke ili pravne osobe, ili (4) zbog važnog javnog interesa Unije ili države članice.

Metode kojima se ograničava obrada osobnih podataka mogle bi, među ostalim, uključivati privremeno premještanje odabranih osobnih podataka u drugi sustav obrade, činjenje odabranih podataka nedostupnima za korisnike ili privremeno uklanjanje objavljenih podataka s internetske stranice. U automatiziranim sustavima pohrane ograničavanje obrade u načelu bi trebalo osigurati tehničkim sredstvima na način da osobni podaci nisu predmet daljnjih obrada i da se ne mogu mijenjati. Činjenicu da je obrada osobnih podataka ograničena trebalo bi jasno navesti u sustavu.[82]

---

[81] Detaljno o rješenjima Uredbe vidi u članku 17. i 19. te uvodnim izjavama br. 65-66.
[82] Detaljnije vidi u čl. 4. t. 3., čl. 18. te uvodnoj izjavi br. 67. Uredbe.

g) Izvješćivanje primatelja u vezi s ispravkom ili brisanjem osobnih podataka ili ograničenjem obrade

Voditelj obrade dužan je priopćiti svaki ispravak ili brisanje osobnih podataka ili ograničenje obrade svakom primatelju kojem su otkriveni osobni podaci, osim ako se to pokaže nemogućim ili zahtijeva nerazmjeran napor. Pored navedenog, ukoliko ispitanik to zatraži, voditelj obrade dužan ga je izvijestiti o tim primateljima (čl. 19.).

h) Pravo na prenosivost podataka

Uredbom se utvrđuje pravo ispitanika na prenosivost podataka kao sasvim novo pravo u odnosu na dosadašnji pravni okvir, koje je namijenjeno jačanju nadzora ispitanika nad njihovim osobnim podacima. To se pravo ostvaruje samo ako se osobni podaci obrađuju automatizirano i ako se njihova obrada temelji bilo na privoli ispitanika, bilo na ugovoru (obrada je nužna za izvršavanje ugovora u kojem je ispitanik stranka ili kako bi se poduzele radnje na zahtjev ispitanika prije sklapanja ugovora). Sadržaj prava na prenosivost je s jedne strane zaprimanje osobnih podataka koje je ispitanik bio pružio voditelju obrade u strukturiranom, uobičajeno upotrebljavanom i strojno čitljivom formatu, te s druge, prijenos tih podataka drugom voditelju obrade bez ometanja od strane prvog voditelja obrade. Štoviše, ako je tehnički izvedivo ispitanik ima pravo i na izravni prijenos predmetnih podataka od jednog voditelja obrade drugome. Međutim, pravo na prenosivost ne smije negativno utjecati na prava i slobode drugih niti dovoditi u pitanje pravo na brisanje osobnih podataka sukladno Uredbi, a osobito ne bi smjelo podrazumijevati brisanje osobnih podataka koji se odnose na ispitanika, koje je on dostavio u svrhu izvršavanja ugovora, u mjeri u kojoj su ti osobni podaci potrebni za izvršavanje tog ugovora i koliko god su potrebni. Voditelje obrade trebalo bi poticati na razvijanje interoperabilnih formata koji omogućuju prenosivost podataka.[83]

i) Pravo ne biti podvrgnut automatiziranom pojedinačnom donošenju odluka, uključujući izradu profila

U sličnoj mjeri kao i u dosadašnjoj Direktivi ZOP Uredba utvrđuje pravo ispitanika da se na njega ne odnosi odluka koja se temelji isključivo na automatiziranoj obradi, uključujući „izradu profila“, koja proizvodi pravne učinke koji se na njega odnose ili na sličan način značajno na njega utječu (npr. automatsko odbijanje zahtjeva za kreditom putem interneta ili prakse zapošljavanja putem interneta bez ikakve ljudske intervencije). To uključuje „izradu profila” (čl. 4. t. 4.) kroz obradu kojom se procjenjuju osobni aspekti u vezi s pojedincem, osobito analizu i predviđanje aspekata ispitanikovog učinka na poslu, ekonomskog stanja, zdravlja, osobnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja kada ona proizvodi pravne učinke koji se odnose na ispitanika ili na njega snažno utječu.

[83] Detaljnije vidi u čl. 20. i uvodnoj izjavi br. 68. te Smjernicama RS29 o pravu na prenosivost podataka, koje je potvrdio EOZP, 16/EN WP 242 rev.01, 13.12.2016., zadnje mijenjane te donesene 05.4.2017., http://azop.hr/info-servis/detaljnije/smjernice.

U određenim će slučajevima automatizirane pojedinačne odluke ipak biti dopuštene, a to ukoliko je odluka u pitanju: (1) temeljena na izričitoj privoli ispitanika, odnosno (2) potrebna za sklapanje ili izvršenje ugovora između ispitanika i voditelja obrade podataka; u oba slučaja voditelj obrade mora provesti odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika, a to barem prava na ljudsku intervenciju voditelja obrade, prava izražavanja vlastitog stajališta te prava na osporavanje odluke. Treća okolnost koja omogućuje takve odluke je kada su one (3) dopuštene pravom Unije ili države članice kojem podliježe voditelj obrade (npr. u svrhe praćenja i sprečavanja prijevare i porezne utaje), a koje pravo također propisuje odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika.

Automatizirane pojedinačne odluke ne smiju se temeljiti na posebnim kategorijama osobnih podataka, osim ako: (1) za takvu obradu postoji izričita privola ispitanika ili ako je (2) ta obrada nužna za potrebe značajnog javnog interesa na temelju prava Unije ili države članice. s time da u oba navedena iznimna slučaja moraju bit uspostavljene odgovarajuće mjere zaštite prava i sloboda te legitimnih interesa ispitanika.

U svakom slučaju, automatizirane pojedinačne odluke ne bi se trebale odnositi na djecu.[84]

5.3.8. Transparentne informacije, komunikacija i modaliteti za ostvarivanje prava ispitanika

Sve informacije o obradi osobnih podataka te sva komunikacija voditelja obrade prema ispitanicima u odnosu na ostvarivanje njihovih prava (pristup, ispravak, brisanje, ograničenje obrade, prenosivost podataka, prigovor na obradu, prava s obzirom na automatizirano pojedinačno donošenje odluka, obavješćivanje o povredi osobnih podataka) mora biti pružena u *sažetom, transparentnom, razumljivom i lako dostupnom obliku, uz uporabu jasnog i jednostavnog jezika, osobito za svaku informaciju koja je posebno namijenjena djetetu*.

Uz iznimku informacija koje se ispitaniku pružaju kod povrede osobnih podataka (za koje je propisan poseban postupak), ovdje navedene informacije u vezi s pravima voditelj obrade ispitaniku na zahtjev pruža najkasnije u roku od mjesec dana od zaprimanja zahtjeva. Iznimno se taj rok može produljiti za dodatna dva mjeseca (uzimajući u obzir složenost i broj zahtjeva).

Informacije se ispitaniku pružaju pisano ili drugim sredstvima, među ostalim, ako je prikladno, elektroničkim putem, a prednost u Uredbi se uvijek daje preferencijama ispitanika u tom kontekstu uz uvažavanje mogućnosti voditelja obrade. Tako, podnese li ispitanik zahtjev elektroničkim putem te bi se informacije ako je moguće trebale dati na isti način (osim ako ispitanik zatraži drugačije). Zatraži li ispitanik da se informacije daju usmeno to bi trebalo omogućiti, ali samo pod uvjetom da je voditelj obrade utvrdio identitet ispitanika drugim sredstvima. Naime, kako bi se izbjegao rizik toga da neovlaštene treće osobe neovlašteno dobiju pristup osobnim podacima ispitanika, odnosno ostvaruju druga ranije spomenuta prava

[84] Detaljnije vidi u čl. 22. i uvodnim izjavama br. 71-72., te Smjernicama RS29., koje je potvrdio EOZP: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 3.10.2017, zadnje mijenjane te usvojene 06.2.2018., https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

ispitanika u vezi s njegovim osobnim podacima, Uredba izričito utvrđuje pravo voditelja obrade da kod opravdane sumnje oko identiteta pojedinca u tim slučajevima zatraži dodatne nužne podatke za potvrđivanje identiteta ispitanika.[85]

5.3.9. Obrada osobnih podataka koja ne zahtijeva identifikaciju

Osobito relevantna u *online* uvjetima je propisana iznimka od primjene propisanih obveza voditelja obrade radi udovoljavanja zahtjevima ispitanika odnosno ispunjavanja njihovih prava (pravo na pristup, brisanje, ispravak, ograničenje obrade osobnih podataka i pravo na prenosivost podataka), u slučajevima kada voditelj obrade (više) ne treba identificirati ispitanika gledano u odnosu na svrhu obrade njegovih osobnih podataka. To uključuje i digitalnu identifikaciju (npr. autentifikacijske podatke za prijavu na internetske usluge dotičnog voditelja obrade). Naime, u tim slučajevima onaj voditelj obrade koji je takvu nemogućnost identifikacije dokazao, *nije dužan čuvati, odnosno prikupljati ili obrađivati dodatne informacije kako bi utvrdio identitet ispitanika* u svrhu pridržavanja s Uredbom. Iako kod prava na pristup osobnim podacima voditelj obrade treba koristiti razumne mjere kako bi utvrdio identitet ispitanika koji traži pristup (osobito u okviru internetskih usluga i mrežnih identifikatora), on ne bi smio pohranjivati osobne podatke samo i isključivo u svrhu toga da bi mogao udovoljiti mogućim takvim zahtjevima ispitanika. Sve ovdje izloženo neće, međutim, vrijediti ako ispitanik sam pruži dodatne informacije u svrhu identifikacije, a kako bi mogao ostvariti gore navedena svoja prava.[86]

5.3.10. Evidencije aktivnosti obrade

Iako Uredba ukida raniju opću obvezu voditelja obrade na izvješćivanje nadzornih tijela o obradi osobnih podataka (u domaćem Zakonu o zaštiti osobnih podataka radilo se o dostavi evidencija o zbirkama podataka AZOP-u te objavi istih u Središnjem registru) te se umjesto toga usredotočuje na određene visokorizične postupke u vezi s obradom podataka, to se ne odnosi i na *obvezu internog vođenja evidencija o aktivnostima obrade osobnih podataka* (čl. 30., uvodne izjave br. 13 i 82.). Takvo se vođenje evidencija Uredbom propisuje kao obveza i to ne samo voditelja obrade nego i izvršitelja obrade. Evidencije se na zahtjev trebaju dati na uvid nadzornom tijelu.

Vođenje evidencija olakšava činjeničnu procjenu rizika postupaka obrade na prava ispitanika, te utvrđivanje i provedbu odgovarajućih sigurnosnih mjera da se zaštite osobni podaci, što su ključne sastavnice načela pouzdanosti prema Uredbi.[87] Propisani oblik evidencije je pisan, a to uključuje i elektronički oblik. Sadržaj evidencije razlikuje se ovisno o tome vodi li evidenciju

[85] Čl. 12. i uvodne izjave br. 58.-59. Uredbe.
[86] Čl. 11. u vezi s čl. 15.-20. Uredbe; uvodne izjave br. 57. i 64.
[87] Pozicijski papir RS29 o iznimkama od obveze vođenja evidencija aktivnosti obrade prema članku 30(5) Opće uredbe o zaštiti podataka, prihvaćen od strane Europskog odbora za zaštitu podataka, 19.4.2018., https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

voditelj ili izvršitelj obrade pa tako, na primjer, voditelj obrade mora uključiti u evidenciju sljedeće informacije:

(1) ime i kontaktne podatke voditelja obrade (i, ako je primjenjivo, zajedničkog voditelja obrade, predstavnika voditelja obrade i službenika za zaštitu podataka); (2) svrhe obrade; (3) opis kategorija ispitanika i kategorija osobnih podataka; (4) kategorije primatelja kojima su osobni podaci otkriveni ili će im biti otkriveni, uključujući primatelje u trećim zemljama ili međunarodne organizacije; (5) ako je primjenjivo, prijenose osobnih podataka u treću zemlju ili međunarodnu organizaciju, uključujući identificiranje te treće zemlje ili međunarodne organizacije te, u slučaju prijenosa u izvanrednim okolnostima (čl. 49. st. 1. drugi podstavak Uredbe), dokumentaciju o odgovarajućim zaštitnim mjerama; (6) ako je to moguće, predviđene rokove za brisanje različitih kategorija podataka; te (7) ako je moguće, opći opis tehničkih i organizacijskih sigurnosnih mjera koje provode kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik (sukladno obvezi iz čl. 32. st. 1. Uredbe).

Kako bi se izbjegle pretjerane otegotnosti za *mikropoduzeća, mala i srednja poduzeća* ta se obveza ne odnosi na njih kada zapošljavaju manje od 250 osoba. To neće, međutim, biti slučaj kada takva poduzeća vrše obradu koja će vjerojatno prouzročiti visok rizik za prava i slobode ispitanika, ili kada vrše obradu koja nije povremena, odnosno ako obrađuju posebnu kategoriju osobnih podataka ili osobne podatke u vezi s kaznenim osudama i kažnjivim djelima. Ipak, kako se tumači i takva manja poduzeća će u pravilu morati voditi evidenciju aktivnosti obrade osobnih podataka svojih radnika, jer ona u pravilu redovito obrađuju te osobne podatke tj. ta obrada u pravilu nije povremena.[88]

5.3.11. Kodeksi ponašanja i certifikacija

Iako je izrada tzv. kodeksa ponašanja i ranije bila predviđena Direktivom ZOP (ne i Zakonom o zaštiti osobnih podataka), Uredbom se osobito podržava značaj kodeksa kroz uspostavljeni mehanizam nadzora nad njihovim pridržavanjem i činjenicu da poštovanje odobrenih kodeksa ponašanja može poslužiti radi dokazivanja usklađenog postupanja s Uredbom.

Radi se ovdje o pravilima zaštite osobnih podataka koja mogu izraditi *udruženja i druga tijela koja predstavljaju kategorije voditelja obrade ili izvršitelja obrade, s ciljem olakšavanja primjene Uredbe, a pritom se trebaju uzeti u obzir posebna obilježja različitih sektora obrade i posebne potrebe mikro, malih i srednjih poduzeća*. Tako kodeksi ponašanja mogu primjerice biti namijenjeni za primjenu u pojedinim sektorima gdje se posebnije izražavaju pojedina pitanja zaštite osobnih podataka (npr. za sektor marketinga i prodaje, u farmaceutskoj industriji i dr.). Osim toga, pomoću kodeksa se mogu pobliže urediti pitanja u vezi s primjenom pojedinih odredbi Uredbe i na općenitoj razini (npr. u vezi s legitimnim interesom, pseudonimizacijom, informiranjem i zaštitom djece te načinom pribavljanja privole nositelja roditeljske odgovornosti nad djetetom i dr.). Kodekse odobravaju nadležna nadzorna tijela za zaštitu osobnih podataka, odnosno Europski odbor za zaštitu podataka (EOZP) ako se aktivnosti obrade odvijaju u više država članica ili čitavoj Uniji. Osim toga, Europska je komisija

[88] *Ibid.*

ovlaštena je proglasiti opću valjanost kodeksa unutar EU-a u slučaju prethodnog pozitivnog mišljenja EOZP-a o tome da je kodeks sukladan s Uredbom. Konačno, kako poštovanje odobrenih kodeksa ponašanja može poslužiti radi dokazivanja usklađenog postupanja s Uredbom, važnu novost predstavlja obveza osiguravanja odgovarajućeg mehanizma nadzora nad njihovim pridržavanjem. Taj nadzor moraju vršiti stručna i neovisna, akreditirana treća tijela. Odobreni kodeksi ponašanja javno se objavljuju.[89]

Kada je riječ o certificiranju, Uredbom predviđeno *dobrovoljno certificiranje zaštite osobnih podataka te pečata i oznaka za zaštitu osobnih podataka* u potpunosti je novouvedeni mehanizam koregulacije u općem okviru zaštite osobnih podataka EU-a. Osim što takvo certificiranje omogućuje ispitanicima brzu procjenu razine zaštite podataka za proizvode i usluge o kojima je riječ (transparentnost), ono može pomoći pri dokazivanju usklađenosti postupaka obrade osobnih podataka (voditelja ili izvršitelja obrade) o kojima je riječ, s Uredbom. Uredba predviđa poticanje uspostave mehanizama certificiranja zaštite osobnih podataka te pečata i oznaka za zaštitu osobnih podataka, osobito na razini EU-a, i to od strane država članica i nadzornih tijela za zaštitu podataka, EOZP-a i Europske komisije. Pritom treba uzeti u obzir posebne potrebe mikro, malih i srednjih poduzeća. Certifikate će izdavati nadležna nadzorna tijela za zaštitu osobnih podataka, odnosno akreditirana certifikacijska tijela na najviše tri godine, uz mogućnost obnove. Kada je riječ o domaćem okviru, ovdje je bitno istaknuti da se Zakonom o provedbi Opće uredbe o zaštiti podataka kao nadležno tijelo za akreditiranje certifikacijskih tijela u Republici Hrvatskoj utvrđuje *Hrvatska akreditacijska agencija* (čl. 5. Zakona u vezi s čl. 43. st. 1. Uredbe).

Kriterije za certifikaciju prema Uredbi određuje nadležno nadzorno tijelo, odnosno EOZP. EOZP može izraditi kriterije i za zajednički certifikat, tzv. *Europski pečat za zaštitu osobnih podataka*. Europska komisija ovlaštena je donositi provedbene akte kojima propisuje tehničke standarde za mehanizme certificiranja, pečate i oznake za zaštitu podataka te mehanizme promicanja i priznavanja tih mehanizama certificiranja, pečata i oznaka.[90]

Činjenici poštovanja odobrenih kodeksa ponašanja ili mehanizama certificiranja daje se posebna vrijednost kroz Uredbu. Ista je, primjerice, element za moguće dokazivanje prikladnosti poduzetih mjera zaštite podataka i provedbu načela pouzdanosti[91] kao i za odluku o tome hoće li se u slučaju povrede izreći upravna novčana kazna i ako da, o njezinu iznosu[92],

[89] Detaljnije vidi u čl. 40-41; čl. 57. st. 1m, 1p, 1q i čl. 58. st. 3d (zadaci, ovlasti nadzornih tijela); čl. 64. st. 1b (konzistentnost - mišljenja EOZP-a); čl. 70. st. 1n i 1x (zadaće EOZP-a) te u uvodnim izjavama br. 98.-99, 168.
[90] Detaljnije vidi u čl. 42-43; čl. 57. st. 1n, 1o, 1p i 1q; čl. 58. st. 1c, 2 h, 3e-f (zadaci, ovlasti nadzornih tijela); čl. 64. st. 1c (konzistentnost), čl. 70. st. 1n – 1q (zadaće EOZP-a) te u uvodnim izjavama br. 100, 168.
[91] Detaljnije vidi u čl. 24. st. 3. (obveze voditelja obrade), čl. 25. st. 3 (odobreni mehanizam certificiranja što se tiče tehničke i integrirane zaštite podataka); čl. 28. st. 5. (tehničke i organizacijske mjere – izvršitelji obrade), čl. 32. st. 3. (sigurnost obrade), čl. 35. st. 8. (kodeksi i procjene učinka), te općenito u čl. 40-43. Uredbe.
[92] Čl. 83. st. 2j Uredbe.

zatim propisana osnova za međunarodni prijenos osobnih podataka u pojedinim slučajevima[93], i dr.

5.3.12. Upravljanje rizicima i sigurnost obrade

Uredbom uspostavljen sustav upravljanja rizicima temelji se na prepoznavanju vjerojatnosti i ozbiljnosti rizika koje pojedina obrada ima, s obzirom na njezinu prirodu, opseg, kontekst i svrhe, na prava i slobode pojedinaca. Te bi rizike trebalo procjenjivati na temelju objektivne procjene, kojom se utvrđuje uključuju li postupci obrade podataka rizik ili visoki rizik. Pojašnjenja rizika različitih vjerojatnosti i ozbiljnosti, uključuju situacije:

1) obrade osobnih podataka koja bi mogla prouzročiti fizičku, materijalnu ili nematerijalnu štetu, posebno ako ta obrada može dovesti do diskriminacije, krađe identiteta ili prijevare, financijskog gubitka, štete za ugled, gubitka povjerljivosti osobnih podataka zaštićenih poslovnom tajnom, neovlaštenog obrnutog postupka pseudonimizacije, ili bilo koje druge znatne gospodarske ili društvene štete;
2) ako bi ispitanici mogli biti uskraćeni za svoja prava i slobode ili spriječeni u obavljanju nadzora nad svojim osobnim podacima;
3) ako se obrađuju osobni podaci koji odaju rasno ili etničko podrijetlo, politička mišljenja, vjerska ili filozofska uvjerenja, članstvo u sindikatu i ako je riječ o obradi genetičkih podataka, podataka koji se odnose na zdravlje ili spolni život ili kaznene osude i kažnjiva djela ili povezane sigurnosne mjere;
4) ako se procjenjuju osobni aspekti, osobito analiza ili predviđanje aspekata u vezi s učinkom na poslu, ekonomskim stanjem, zdravljem, osobnim preferencijama ili interesima, pouzdanošću ili ponašanjem, lokacijom ili kretanjem kako bi se izradili ili upotrebljavali osobni profili;
5) ako se obrađuju osobni podaci osjetljivih pojedinaca, osobito djece;
6) ako obrada uključuje veliku količinu osobnih podataka i utječe na velik broj ispitanika.

Nadograđujući se na raniji okvir Uredba dodatno osnažuje pristup procjene rizika kada je riječ o odabiru odgovarajućih mjera radi osiguravanja *sigurnosti obrade osobnih podataka*. Osim toga, provedba mjera radi osiguravanja sigurnosti osobnih podataka utvrđuje se kao jedno od temeljnih načela obrade osobnih podataka i to *načelo cjelovitosti i povjerljivosti*, te se izričito utvrđuje odgovornost voditelja obrade ne samo da osigura usklađenost postupanja u skladu s tim načelom već i da tu usklađenost dokaže (*načelo pouzdanosti*).

U glavnoj odredbi koja nosi naslov „Sigurnost obrade“ (čl. 32.) propisuje se obveza kako voditelja obrade, tako i izvršitelja obrade da provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik, uzimajući u obzir najnovija dostignuća, troškove provedbe te prirodu, opseg, kontekst i svrhe obrade, kao i rizik različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca.

Kod procjene odgovarajuće razine sigurnosti u obzir se posebno uzimaju rizici koje predstavlja obrada, posebno rizici od slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog

[93] Detaljnije vidi u čl. 40. st. 3., čl. 42. st.2. i čl. 46. st. 2e-2f Uredbe.

otkrivanja ili neovlaštenog pristupa podacima koji su preneseni, pohranjeni ili na drugi način obrađivani (a što osobito može dovesti do fizičke, materijalne ili nematerijalne štete).

Uredba izričito utvrđuje i primjere odgovarajućih mjera sigurnosti, a to su, prema potrebi:

(1) pseudonimizacija i enkripcija osobnih podataka;

(2) sposobnost osiguravanja trajne povjerljivosti, cjelovitosti, dostupnosti i otpornosti sustava i usluga obrade;

(3) sposobnost pravodobne ponovne uspostave dostupnosti osobnih podataka i pristupa njima u slučaju fizičkog ili tehničkog incidenta;

(4) proces za redovno testiranje, ocjenjivanje i procjenjivanje učinkovitosti tehničkih i organizacijskih mjera za osiguravanje sigurnosti obrade.

Kako je ranije pokazano, dodanu vrijednost poštovanja odobrenog kodeksa ponašanja ili mehanizma certificiranja i u ovome kontekstu može poslužiti voditeljima ili izvršiteljima obrade kod dokazivanja usklađenosti postupanja s navedenim zahtjevima sigurnosti obrade.

Što se tiče samog *načela povjerljivosti*, u sličnoj mjeri kao i dosadašnji okvir Uredba utvrđuje obvezu i voditelja obrade i izvršitelja obrade da primjenjuju mjere osiguravanja toga da osobe koje imaju pristup osobnim podacima, a koje djeluju pod njihovom odgovornošću, te podatke obrađuju samo prema uputama voditelja obrade. Iznimka je u tom pogledu dopušten pristup podacima na temelju prava EU-a ili prava države članice.[94]

Domaće nadzorno tijelo – AZOP objavilo je sljedeće preporuke u svrhu provedbe odgovarajućih tehničkih i organizacijskih mjera zaštite u skladu s Uredbom:

(1) potrebno je pohranjivati svu dokumentaciju u papirnatom obliku koja sadrži osobne podatke (npr. u ormare ili ladice pod ključem) i držati istu pod nadzorom ovlaštenih osoba voditelja obrade;
(2) potrebno je koristiti korisnička imena i lozinke u svrhu omogućavanja pristupa osobnim podacima pohranjenim u elektroničkom obliku;
(3) potrebno je izrađivati sigurnosne kopije;
(4) potrebno je provoditi pseudonimizaciju ili enkripciju osobnih podataka, osobito ako se radi o posebnim kategorijama, poput podataka o zdravlju;
(5) potrebno je bilježiti pristup podacima; i
(6) potrebno je potpisivati izjave o povjerljivosti (kada je riječ o osobama koje rade u obradi osobnih podataka).[95]

5.3.13. Načela tehničke zaštite podataka i integrirane zaštite podataka

Pojam *privatnost po dizajnu* (engl. *privacy by design*) poznat je na globalnoj razini već dulji niz godina, a označava filozofiju i pristup ugrađivanja zaštite prava na privatnost u vezi s obradom osobnih podataka u specifikacije dizajna različitih tehnologija.[96]

[94] Čl. 32. i uvodne izjave br. 74.-77., 83. Uredbe.

[95] Važne napomene voditeljima obrade i izvršiteljima obrade vezano za primjenu Opće uredbe o zaštiti podataka, http://azop.hr/aktualno/detaljnije/obavijest-za-voditelje-i-izvrsitelje-obrade-ukidanje-sredisnjeg-registra.

[96] Cavoukian, Ann, Privacy by design … take the challenge, Information and Privacy Commissioner of Ontario, Canada, 2009., str. 3., https://www.ipc.on.ca/wp-content/uploads/Resources/PrivacybyDesignBook.pdf.

Privatnost po dizajnu uz korištenje naprednih tehnologija za zaštitu privatnosti smatra se pravim sredstvom za osiguravanje između ostalog toga da se već u samoj fazi planiranja i oblikovanja sustava za obradu osobnih podataka predvide, odnosno u sustav ugrade sve potrebne mjere i/ili kontrole za učinkovitu provedbu temeljnih načela zaštite osobnih podataka (kao što su to poglavito načela minimalizacije i određenosti svrhe obrade osobnih podataka). Prepoznajući važnost i koristi ugradnje tog načela u sustave za obradu osobnih podataka, u Uredbi se kao značajni pomak u odnosu na raniji okvir uvodi obveza provedbe tog načela kao tzv. zaštite podataka po dizajnu (izravan prijevod s engleskog jezika - *data protection by design*), tj. „*tehničke zaštite podataka*" prema službenoj domaćoj terminologiji.

Uredba tako propisuje u čl. 25. da se provedba mjera kojima se osigurava i dokazuje usklađenost s istom treba osigurati usvajanjem odgovarajućih internih politika i provedbom mjera, kojima se osobito ispunjavaju (1) načelo tehničke zaštite podataka i (2) načelo integrirane zaštite podataka (potonje se načelo pojašnjava malo niže u tekstu).

Obveza učinkovite provedbe *načela tehničke zaštite podataka* za voditelja obrade znači da isti mora osigurati provedbu odgovarajućih tehničkih i organizacijskih mjera *kako u vrijeme određivanja sredstava obrade tako i u vrijeme same obrade*, u svrhu osiguravanja usklađenosti s Uredbom, uključujući zaštitu prava ispitanika. Pritom se uzimaju u obzir *najnovija dostignuća, trošak provedbe, priroda, opseg, kontekst i svrhe obrade, te rizici različitih razina vjerojatnosti i ozbiljnosti za prava i slobode pojedinaca koji proizlaze iz obrade*. Uredba navodi izričito primjer mjere *pseudonimizacije* (kako bi se ispunilo načelo smanjenja količine podataka - osobni podaci moraju biti primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju). Nadalje, u dodatnim se pojašnjenjima pored mjera smanjenja količine osobnih podataka i njihove pseudonimizacije što je prije moguće utvrđuju kao primjeri mjera i *transparentnost u vezi s funkcijama i obradom osobnih podataka, omogućavanje ispitaniku da prati obradu podataka te omogućavanje voditelju obrade da stvara i poboljšava sigurnosne značajke*.

Što se tiče *načela integrirane zaštite podataka* (engl. *data protection by default*), ono nalaže da voditelj obrade osigura kroz odgovarajuće tehničke i organizacijske mjere to da se integriranim načinom (tj. kao početna, zadana vrijednost) obrađuju samo osobni podaci koji su nužni za svaku posebnu svrhu obrade. Odnosi se ta obveza i na količinu prikupljenih osobnih podataka, opseg njihove obrade, razdoblje pohrane te njihovu dostupnost. Osobni podaci koji se obrađuju ne mogu automatski (dakle bez intervencije pojedinca) biti dostupni neograničenom broju osoba.

Provedba ova dva načela uzima se u obzir kod razmatranja stupnja odgovornosti voditelja obrade (odnosno izvršitelja obrade, ako ih ima) u kontekstu odluka o izricanju upravnih novčanih kazni i njihovu iznosu. Valja ovdje imati na umu i odgovarajuću certifikaciju voditelja ili izvršitelja obrade, budući da se odobreni mehanizmi certificiranja mogu

koristiti kao element za dokazivanje sukladnosti s propisanim zahtjevima primjene navedenih načela tehničke i integrirane zaštite podataka (čl. 25. st. 3., čl. 83. st. 2d i 2j Uredbe).

Kako su voditelji obrade (i izvršitelji obrade po njihovu nalogu, ako ih ima) dužni primijeniti načela tehničke i integrirane zaštite podataka, postavlja se pitanje mjere do koje oni mogu na isto utjecati ako se npr. radi o njihovu korištenju „gotovih" usluga i proizvoda treće strane (putem kojih se obrađuju osobni podaci o kojima je riječ). Od posebne su važnosti stoga dodatna pojašnjenja, prema kojima treba poticati *proizvođače proizvoda, usluga i aplikacija* da uzmu u obzir pravo na zaštitu podataka prilikom razvoja i osmišljavanja relevantnih proizvoda, usluga i aplikacija, te da osiguraju da voditelji obrade i izvršitelji obrade mogu ispuniti svoje obveze u pogledu zaštite podataka, uzimajući u obzir najnovija dostignuća. Osim toga, načela tehničke i integrirane zaštite podataka trebalo bi uzeti u obzir i u kontekstu javnih natječaja (uvodna izjava br. 78.).

5.3.14. Povreda osobnih podataka

U Uredbi se po prvi puta na razini općeg pravnog okvira zaštite osobnih podataka EU-a uređuju postupci u slučaju tzv. povreda osobnih podataka. Ti postupci su do tada bili uređeni samo posebnim okvirom zaštite podataka i privatnosti u području elektroničkih komunikacija u EU-u (Direktivom o e-privatnosti i Uredbom Komisije br. 611/2013 o mjerama koje se primjenjuju na obavješćivanje o povredama osobnih podataka u skladu s Direktivom 2002/58/EZ[97]), kao i u Republici Hrvatskoj (čl. 99. Zakona o elektroničkim komunikacijama).

Povredu osobnih podataka prema Uredbi predstavlja kršenje sigurnosti koje dovodi do slučajnog ili nezakonitog uništenja, gubitka, izmjene, neovlaštenog otkrivanja ili pristupa osobnim podacima koji su preneseni, pohranjeni ili na drugi način obrađivani (čl. 4. t. 12.). Propisani su postupci u Uredbi u vezi s izvješćivanjem nadzornog tijela za zaštitu osobnih podataka o povredi, te u vezi s izvješćivanjem samih ispitanika.[98]

Šteta koja ispitanicima može prouzročiti povreda osobnih podataka može biti fizička, materijalna i nematerijalna šteta, a njihovi su konkretni primjeri, kako slijedi: gubitak nadzora nad osobnim podacima ili ograničavanje prava ispitanika, diskriminacija, krađa identiteta ili prijevara, financijski gubici, neovlašteni obrnuti postupci pseudonimizacije, šteta za ugled, gubitak povjerljivosti osobnih podataka zaštićenih profesionalnom tajnom ili bilo koja druga ekonomska ili društvena šteta za ispitanika.

Izvješćivanje nadzornog tijela

[97] SL L 173, 26. 6. 2013., str. 2–8.; izdanje na hrv. jeziku: 13/Sv. 66, str. 159-165.
[98] Čl. 25. i uvodna izjava br. 78. Uredbe.

Uredbom se utvrđuje obveza voditelja obrade da bez nepotrebnog odgađanja i, ako je izvedivo, najkasnije 72 sata nakon saznanja o povredi obavijesti o tome nadzorno tijelo, osim ako nije vjerojatno da će povreda prouzročiti rizik za prava i slobode pojedinaca. Ako to izvješćivanje nije učinjeno unutar 72 sata, ono mora biti popraćeno s razlozima za kašnjenje. Kada voditelj obrade angažira izvršitelja, on mora bez nepotrebnog odgađanja izvijestiti voditelja obrade nakon što sazna za povredu. Propisani minimalni sadržaj obavijesti uključuje:

(1) opis prirode povrede, uključujući, ako je moguće, kategorije i približan broj dotičnih ispitanika te kategorije i približan broj dotičnih evidencija osobnih podataka;

(2) ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija;

(3) opis vjerojatnih posljedica povrede; i

(4) opis mjera koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje povrede, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.

Kako bi se nadzornom tijelu omogućila provjera poštovanja ovdje navedenih obveza voditelj obrade dužan je dokumentirati sve povrede osobnih podataka, uključujući činjenice vezane za povredu, njezine posljedice i mjere poduzete za popravljanje štete.

Obavješćivanje ispitanika

Voditelj obrade mora obavijestiti ispitanika o povredi koja će vjerojatno prouzročiti visok rizik za njegova prava i slobode, i to bez nepotrebnog odgađanja. Obavijest mora sadržavati barem:

(1) opis prirode povrede, uz korištenje jasnog i jednostavnog jezika;

(2) ime i kontaktne podatke službenika za zaštitu podataka ili druge kontaktne točke od koje se može dobiti još informacija;

(3) opis vjerojatnih posljedica povrede, i

(4) opis mjera koje je voditelj obrade poduzeo ili predložio poduzeti za rješavanje povrede, uključujući prema potrebi mjere umanjivanja njezinih mogućih štetnih posljedica.

Obavješćivanje ispitanika nije obvezno:

(1) ako je voditelj obrade poduzeo odgovarajuće tehničke i organizacijske mjere zaštite i te su mjere primijenjene na osobne podatke pogođene povredom, posebno one koje te podatke čine nerazumljivima neovlaštenim osobama, kao što je enkripcija; ili

(2) ako je voditelj obrade poduzeo naknadne mjere kojima se osigurava da više nije vjerojatno da će doći do visokog rizika za prava i slobode ispitanika; ili

(3) ako bi se time zahtijevao nerazmjeran napor (tada mora postojati javno obavješćivanje ili slična mjera kojom se ispitanici obavješćuju na jednako djelotvoran način).

Ako voditelj obrade nije do tog trenutka obavijestio ispitanika, ovo od njega može tražiti nadzorno tijelo nakon što je razmotrilo razinu vjerojatnosti da će povreda prouzročiti visok rizik, odnosno to tijelo može zaključiti da je ispunjen jedan od propisanih uvjeta (1-3 gore) kada nije obvezno izvješćivanje ispitanika.[99]

5.3.15. Pseudonimizacija

Kako je ranije pojašnjeno, Uredbom se pojam pseudonimizacije uvodi u europski opći pravni okvir zaštite podataka kao postupak obrade osobnih podataka na način da se ti podaci više ne mogu pripisati određenom ispitaniku bez uporabe dodatnih informacija, pod uvjetom da se te informacije drže odvojeno te da podliježu tehničkim i organizacijskim mjerama kako bi se osiguralo da se osobni podaci ne mogu pripisati pojedincu čiji je identitet utvrđen ili se može utvrditi (čl. 4. t. 5.). Iako se u slučaju pseudonimiziranih podataka radi i dalje o osobnim podacima, primjena pseudonimizacije na osobne podatke može smanjiti rizike za ispitanike o kojima je riječ, te pomoći voditeljima obrade i izvršiteljima obrade u ispunjavanju njihovih obveza u vezi sa zaštitom podataka (uvodna izjave br. 26, 28). Uredba u nizu primjera potiče primjenu tog postupka tijekom obrade osobnih podataka.

Pseudonimizacijom se osobito može postići načelo smanjenja količine osobnih podataka, a s time je u vezi i utvrđivanje pseudonimizacije kao jedne od zaštitnih mjera putem koje se (posebice ako se provede čim je moguće prije u postupu obrade) može osigurati provedba načela tehničke zaštite podataka (čl. 25. st. 1., uvodna izjava br. 78).

Uz enkripciju pseudonimizacija se utvrđuje kao jedna od mjera putem kojih voditelji obrade i izvršitelji obrade mogu ispuniti svoju obvezu provedbe odgovarajućih tehničkih i organizacijskih mjera kako bi osigurali odgovarajuću razinu sigurnosti s obzirom na rizik (čl. 32. st. 1. t. a).

Prihvati li se teza, ovisno o okolnostima pojedinog slučaja, da kod povrede osobnih podataka koji su pseudonimizirani nije vjerojatno da će povreda osobnih podataka prouzročiti rizik za prava i slobode pojedinaca, voditelji obrade mogli bi izbjeći propisanu obvezu izvješćivanja (nadzornog tijela, odnosno pojedinaca o kojima je riječ).

Provedba pseudonimizacije kao zaštitne mjere prilikom obrade osobnih podataka utvrđuje se kao čimbenik kojim se može osigurati dopuštena daljnja obrada osobnih podataka u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe (takve daljnje obrade osobnih podataka neće se u tom slučaju smatrati neusklađenima s prvotnim svrhama obrade tih podataka) i kao jedan od čimbenika, uz enkripciju osobnih podataka, na temelju kojeg se može utvrditi je li u posebnim slučajevima daljnja obrada osobnih podataka različita u odnosu na svrhu u koju su ti podaci prvotno prikupljeni. Drugim

[99] Detaljnije o povredi osobnih podataka vidi u čl. 33-34., uvodnim izjavama br. 75., 85.-88. te Smjernicama RS29 koje je potvrdio EOZP: Guidelines on Personal data breach notification under Regulation 2016/679, 18/EN WP250 rev.01, 3.10.2017, zadnje mijenjane i usvojene 06.2.2018., https://edpb.europa. eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

riječima, iako se daljnjom obradom osobnih podataka, neusklađenom s prvotnom svrhom njihova prikupljanja, krši načelo ograničenja svrhe obrade podataka, uspješno provedena pseudonimizacija kao zaštitna mjera može doprinijeti utvrđenju toga da daljnja obrada podataka o kojima je riječ ne bi bila protivna prvotnoj svrsi njihove obrade tj. prikupljanja.[100]

5.3.16. Procjena učinka na zaštitu osobnih podataka i prethodno savjetovanje

Kako je ranije pojašnjeno, Uredba ukida prijašnju opću obvezu voditelja obrade na izvješćivanje nadzornih tijela o obradi podataka (u ranijem Zakonu o zaštiti osobnih podataka provedenu na način da su voditelji bili dužni dostavljati evidencije o zbirkama podataka, koje su se objavljivale u Središnjem registru AZOP-a). Za tu se obvezu, naime, utvrdilo da je administrativno i financijski suviše otegotna gledano u odnosu na koristi koje su se kroz njezinu provedbu predviđale. Umjesto toga Uredba se usredotočuje na određene postupke u svrhu prepoznavanja i minimalizacije rizika kod tzv. visokorizičnih aktivnosti obrade za prava i slobode pojedinaca. Tim se novim postupcima ujedno nadograđuju odredbe ranijeg okvira o tzv. prethodnim provjerama aktivnosti obrade koje bi mogle predstavljati posebne rizike za prava i slobode ispitanika.

Uredba tako predviđa obvezu voditelja obrade da poduzima *procjenu učinka na zaštitu podataka* u slučaju vjerojatne visokorizične aktivnosti obrade osobnih podataka. Rizici o kojima je riječ odnose se na (utjecaj te obrade na) prava i slobode pojedinaca. Pritom se razmatra *vrsta obrade*, osobito ako se provodi putem novih tehnologija, kao i *priroda, opseg, kontekst i svrhe* obrade. Procjena učinka obvezna je samo ako je vjerojatno da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visok rizik za prava i slobode pojedinaca.

Propisani slučajevi kada se osobito mora provoditi obvezna procjena jesu, kako slijedi:

(1) sustavna i opsežna procjena osobnih aspekata u vezi s pojedincima koja se temelji na automatiziranoj obradi, uključujući izradu profila, i na temelju koje se donose odluke koje proizvode pravne učinke koji se odnose na pojedinca ili koje na njega slično utječu;

(2) opsežna obrada posebnih kategorija osobnih podataka ili podataka u vezi s kaznenim osudama i kažnjivim djelima; ili

(3) sustavno praćenje javno dostupnog područja u velikoj mjeri (posebno ako se koriste optičko-elektronički uređaji).

[100] Detaljnije vidi u čl. 5. st. 1b, 5. st. 1e i čl. 89. Uredbe, čl. 6. st. 4e., te uvodnim izjavama br. 50. i 156. Uredbe

Tako je npr. obvezna procjena u slučaju bolnica koje obrađuju genetske i zdravstvene podatke pacijenata (bolnički informacijski sustav), dok ona to nije (nema opsežne obrade) ako se odnosi na osobne podatke pacijenata ili klijenata liječnika, zdravstvenih djelatnika ili odvjetnika.[101]

Uredba propisuje *minimalan sadržaj* procjene učinka, kako slijedi: sustavan opis predviđenih postupaka i svrha obrade; procjena nužnosti i proporcionalnosti postupaka obrade povezanih s njihovim svrhama; procjena rizika za prava i slobode ispitanika, te predviđene mjere za ublažavanje rizika, pri čemu se uzima u obzir i poštovanje odobrenih kodeksa ponašanja.[102]

Pokaže li procjena učinka da bi obrada dovela do visokog rizika za prava i slobode ispitanika za slučaj da voditelj obrade ne donese mjere za ublažavanje rizika, isti je dužan savjetovati se s nadzornim tijelom prije obrade (*prethodno savjetovanje*), u vezi s čime Uredba propisuje daljnja postupanja.[103]

Pored ranije navedenih slučajeva kada se mora provoditi procjena učinka prema Uredbi, nadzorna tijela u državama članicama ovlaštena su utvrđivati i daljnje postupke koji podliježu obveznoj procjeni učinka.[104] Agencija za zaštitu osobnih podataka objavila je cjeloviti popis postupaka koji podliježu procjeni učinka putem *Odluke o uspostavi i javnoj objavi popisa vrsta postupaka obrade koje podliježu zahtjevu za procjenu učinka na zaštitu podataka* (popis može biti mijenjan te je nužno redoviti pratiti relevantne objave tog tijela):

1) obrada osobnih podataka radi sustavnog i opsežnog profiliranja ili automatiziranog odlučivanja kako bi se donijeli zaključci koji u značajnijoj mjeri utječu ili mogu utjecati na pojedinca i/ili više osoba ili koji služe kao pomoć u donošenju odluka o nečijem pristupu nekoj usluzi ili servisu ili pogodnosti (npr. obrada podataka odnosnih na ekonomski ili financijski status, zdravlje, osobne preferencije, interese, pouzdanost, ponašanje, podatke o lokaciji i dr.);

2) obrada posebnih kategorija podataka u svrhu profiliranja ili automatiziranog odlučivanja;

3) obrada osobnih podataka djece u svrhu profiliranja ili automatiziranog odlučivanja ili za marketinške svrhe, ili za izravnu ponudu usluga namijenjenu njima;

4) obrada osobnih podatka prikupljenih od trećih koji se uzimaju u obzir za donošenje odluke oko sklapanja, raskida, odbijanja ili produženja ugovora o pružanju usluga fizičkim osobama;

5) obrada posebnih kategorija osobnih podataka ili osobnih podataka o kaznenoj ili prekršajnoj odgovornosti u velikom opsegu;

---

[101] Uvodna izjava br. 91. Uredbe; AZOP, Važne napomene voditeljima obrade i izvršiteljima obrade vezano za primjenu Opće uredbe, http://azop.hr/aktualno/detaljnije/obavijest-za-voditelje-i-izvrsitelje-obrade-ukidanje-sredisnjeg-registra.

[102] Detaljnije o procjeni učinka vidi u čl. 35. i uvodnim izjavama br. 75, 84, 89, 90-93. Uredbe, te Smjernicama RS29 o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik" u smislu Uredbe 2016/679, koje je potvrdio EOZP, 17/HR WP48 rev.01,04.4.2017., zadnje mijenjane te usvojene 4.10.2017., http://azop.hr/info-servis/detaljnije/smjernice.

[103] Detaljno o prethodnom savjetovanju vidi u čl. 36. te uvodnim izjavama br. 94-96. Uredbe.

[104] Ako popis nadzornog tijela obuhvaća aktivnosti obrade povezane s ponudom robe ili usluga ispitanicima ili s praćenjem njihova ponašanja u više država članica ili bi mogle znatno utjecati na slobodno kretanje osobnih podataka unutar EU-a, prije njihova usvajanja nadležno nadzorno tijelo primjenjuje mehanizam konzistentnosti. Vidi čl. 35. st. 4-6. u vezi s čl. 63. Uredbe.

6) obrada osobnih podataka uz sustavni nadzor javno dostupnih mjesta u velikom opsegu;

7) uporaba novih tehnologija ili tehnoloških rješenja za obradu osobnih podataka ili s mogućnošću obrade osobnih podataka (npr. primjena „interneta stvari“ poput pametnih televizora, pametnih kućanskih aparata, komunikacijski povezanih igračaka, sustava „pametni gradovi“, pametnih mjerača energije, itd.) koji služe za analizu ili predviđanje ekonomske situacije, zdravlja, osobnih preferencija ili interesa, pouzdanosti ili ponašanja, lokacije ili kretanja fizičkih osoba;

8) obrada osobnih podataka generiranih pomoću uređaja sa senzorima koji šalju podatke putem interneta ili drugim tehnologijama za prijenos informacija;

9) obrada biometrijskih ili genetskih podataka;

10) obrada povezivanjem, usporedbom ili provjerom podudarnosti iz više izvora;

11) obrada osobnih podataka na način koji uključuje praćenje lokacije ili ponašanja pojedinca, u slučaju sustavne obrade komunikacijskih podataka (metapodaci) nastalih uporabom telefona, interneta ili drugih komunikacijskih kanala, kao što je GSM, GPS, Wi Fi, praćenje ili obrada podataka o lokaciji;

12) obrada osobnih podataka korištenjem uređaja i tehnologija kod kojih incidentni događaj može ugroziti zdravlje pojedinca ili više osoba;

13) obrada osobnih podataka u drugu/e svrhu/e od one za koju su prvobitno prikupljeni;

14) obrada osobnih podataka radnik uporabom aplikacija ili sustava za praćenje (npr. kao što je obrada osobnih podatka za praćenje rada, kretanja, komunikacije i sl.).[105]

Valja ovdje skrenuti pažnju i na *Zakonom o provedbi Opće uredbe* utvrđenu obvezu AZOP-a (čl. 18.) da na svojim mrežnim stranicama objavljuje anonimizirana ili pseudonimizirana rješenja i mišljenja u pogledu vrsta obrada koje mogu prouzročiti visoki rizik za prava i slobode (ako se ista odnose na maloljetnike bit će anonimizirana radi njihove zaštite).

5.3.17. Neovisna nadzorna tijela

U pravu EU-a se uvjet *neovisnosti* nadzornih tijela za zaštitu osobnih podataka izričito utvrđuje Ugovorom o funkcioniranju EU-a (čl. 16. st. 2.) te Poveljom o temeljnim pravima EU-a (čl. 8. st. 3.). O tom je uvjetu odlučivao i Sud EU-a u presudama donesenim protiv nekoliko država članica (SR Njemačke, Austrije i Mađarske) kod kojih je utvrđena povreda neovisnosti nadzornih tijela. U svojim je presudama Sud među ostalim utvrdio kako zahtjev potpune neovisnosti zahtijeva da nadzorna tijela budu slobodna od bilo kojeg utjecaja, bilo izravnog ili neizravnog, u svojem radu i odlučivanju, kao i to da sam rizik od političkog utjecaja na odluke koje donose zadire u njihovo neovisno obavljanje zadataka. Prema Sudu neovisnost nije uspostavljena s funkcionalnom neovisnošću nadzornih tijela, ukoliko još uvijek postoji

[105] Kl.: 004-04/18-01/01, ur.br. 567-01/01-18-01, Zagreb, 25.5.2018.

mogućnost vanjskog (političkog) utjecaja na ta tijela.[106] Tumačenja Suda u kontekstu navedenih izvora te ranije Direktive ZOP relevantna su i u kontekstu danas važeće Uredbe.

Svaka država članica dužna je prema Uredbi osigurati neovisno nadzorno tijelo odgovorno za praćenje njezine primjene, kako bi se zaštitila temeljna prava i slobode pojedinaca u pogledu obrade i olakšao slobodan protok osobnih podataka unutar EU-a. Kada je riječ o neovisnosti, utvrđuje se da nadzorno tijelo mora djelovati potpuno neovisno pri obavljanju svojih dužnosti i izvršavanju svojih ovlasti. Članovi nadzornog tijela moraju biti slobodni od vanjskog utjecaja, bilo izravnog bilo neizravnog, pri obavljanju svojih dužnosti i izvršavanju svojih ovlasti u skladu s Uredbom te ne smiju tražiti ni primati upute ni od koga.

Svako je nadzorno tijelo zaduženo za doprinos dosljednoj primjeni Uredbe u EU-u i u tu svrhu nadzorna tijela surađuju međusobno, kao i s Europskom komisijom, te u određenim slučajevima s Europskim odborom za zaštitu podataka („suradnja i konzistentnost“).[107]

Uredbom se detaljno uređuju i uvjeti za članove nadzornog tijela, pravila za osnivanje nadzornog tijela, te njegova nadležnost, zadaće i ovlasti.[108]

Pored (1) praćenja i provedbe primjene Opće uredbe, tim aktom propisane zadaće nadzornih tijela su, među ostalim: 2) promicanje javne svijesti o rizicima, pravilima, zaštitnim mjerama i pravima u vezi s obradom te njihovo razumijevanje – pri čemu naročitu pozornost dobivaju aktivnosti posebno namijenjene djeci; (3) promicanje osviještenosti voditelja obrade i izvršitelja obrade o njihovim obvezama; (4) praćenje bitnih razvoja u onoj mjeri u kojoj utječu na zaštitu osobnih podataka, osobito razvoj informacijskih i komunikacijskih tehnologija i komercijalnih praksi; (5) pružanje na zahtjev informacije bilo kojem ispitaniku u vezi s ostvarivanjem njihovih prava iz Uredbe; (6) rješavanje podnesenih pritužbi; (7) suradnja s drugim nadzornim tijelima; (8) provedba istraga o primjeni Uredbe; 9) savjetovanje parlamenta, vlade i drugih institucija i tijela o zakonodavnim i administrativnim mjerama u vezi sa zaštitom prava i sloboda pojedinaca u pogledu obrade i dr.

Ovlasti nadzornih tijela prema Uredbi mogu se podijeliti u (1) *istražne*, (2) *korektivne*, te u (3) *ovlasti u vezi s odobravanjem i savjetodavne ovlasti*. Pored navedenih ovlasti prema Uredbi svaka država članica domaćim zakonom može predvidjeti dodatne ovlasti nadzornog tijela.

U skladu sa svojim *istražnim ovlastima* nadzorna tijela mogu, među ostalim: (1) narediti voditelju i izvršitelju obrade da pruže sve informacije potrebne za obavljanje njihovih zadaća; (2) ishoditi od voditelja i izvršitelja obrade pristup svim osobnim podacima i svim informacijama potrebnim za obavljanje svojih zadaća; kao i ishoditi pristup njihovim prostorijama, u skladu s pravom EU-a ili postupovnim pravom države članice; (3) provoditi istrage u obliku revizije zaštite podataka; 4) provoditi preispitivanja izdanih certifikata, i dr.

[106] C-518/07, EU:C:2010:125; C-614/10, EU:C:2012:631 i C-288/12, EU:C:2014:237.

[107] Detaljno vidi u poglavlju VII., te uvodnim izjavama br. 124-128, 130-131 i 133-140. Uredbe. Vidi i čl. 15. Zakona o provedbi Opće uredbe o suradnji AZOP-a s nadzornim tijelima za zaštitu podataka drugih država.

[108] Detaljno vidi u poglavlju VI. te uvodnim izjavama br. 117-129. Uredbe.

Korektivne ovlasti nadzornih tijela jesu, među ostalim: (1) izdati upozorenja voditelju ili izvršitelju obrade da bi namjeravani postupci obrade lako mogli prouzročiti kršenje Uredbe; (2) izdati službene opomene voditelju ili izvršitelju obrade ako se obradom krši Uredba; (3) narediti voditelju ili izvršitelju obrade da poštuje zahtjeve ispitanika za ostvarivanje njegovih prava u skladu s Uredbom; (4) narediti voditelju ili izvršitelju obrade da postupke obrade uskladi s Uredbom; (5) narediti voditelju obrade da ispitanika obavijesti o povredi osobnih podataka; (6) privremeno ili konačno ograničiti, među ostalim zabraniti, obradu; (7) narediti ispravak, brisanje ili ograničavanje obrade podataka; (8) povući certifikat ili certifikacijskom tijelu narediti da povuče izdani certifikat, odnosno certifikacijskom tijelu narediti da ne izda certifikat ako nisu ili više nisu ispunjeni kriteriji za certificiranje; (9) izreći upravnu novčanu kaznu uz mjere, ili umjesto ovdje navedenih mjera, ovisno o okolnostima slučaja; (10) narediti suspenziju protoka podataka primatelju u trećoj zemlji ili međunarodnoj organizaciji, i dr.

Ovlasti u vezi s odobravanjem te savjetodavne ovlasti uključuju, među ostalim: (1) izdati parlamentu, vladi države članice ili, u skladu s pravom države članice, drugim institucijama i tijelima, te javnosti, mišljenje o svakom pitanju u vezi sa zaštitom osobnih podataka, na vlastitu inicijativu ili na zahtjev; (2) savjetovati voditelja obrade u skladu s prethodnim postupkom savjetovanja, (3) izdati mišljenje i odobriti nacrte kodeksa ponašanja; (4) akreditirati certifikacijska tijela; (5) izdati certifikate i odobriti kriterije certificiranja, i dr.

Nadzorna su tijela u pravilu nadležna na državnom području vlastite države članice, uz iznimku u slučaju *prekogranične obrade* osobnih podataka.[109]

5.3.18. Službenici za zaštitu osobnih podataka

Funkcija službenika za zaštitu podataka već je bila predviđena Direktivom ZOP, koja je ostavila mogućnost njihova imenovanja na izbor državama članicama, a što je u Hrvatskoj po ranijem okviru bilo provedeno na način da su voditelji obrade s 20 ili više radnika morali imenovati službenike. Priznajući važnost te funkcije u skladu sa zahtjevima novog pravnog okvira, Uredba izričito uređuje obvezu imenovanja ovih službenika u određenim slučajevima te bitno nadograđuje raniji okvir s detaljnim pravilima o njihovu imenovanju, položaju i zadacima (čl. 37.-39., uvodna izjava br. 97.). Nova detaljna pravila u Uredbi napose su rezultat dosadašnjeg iskustva u radu ovih službenika diljem EU-a.

[109] Prekogranična obrada je ili: (1) obrada osobnih podataka u EU-u u kontekstu aktivnosti poslovnih nastana u više država članica voditelja ili izvršitelja obrade, kada voditelj ili izvršitelj obrade ima poslovni nastan u više država članica; ili (2) obrada podataka u EU-u u kontekstu aktivnosti jedinog poslovnog nastana voditelja ili izvršitelja obrade, ali koja bitno utječe ili je izgledno da će bitno utjecati na ispitanike u više država članica (čl. 4. t. 23.). Tada nadzorno tijelo za glavni poslovni nastan (čl. 4. t. 16.) ili za jedini poslovni nastan voditelja ili izvršitelja obrade treba djelovati kao vodeće nadzorno tijelo po propisanim postupcima. Detaljnije vidi u čl. 55-56, 60. i uvodnim izjavama br. 122, 124-128, 130-131., te u Smjernicama RS29 za identifikaciju voditelja obrade ili vodećeg nadzornog tijela izvršitelja obrade, koje je potvrdio EOZP, 16/HR WP244 rev.01, 03.12.2016., zadnje mijenjane i donesene 05.4.2017., http://azop.hr/info-servis/detaljnije/smjernice.

Obveza imenovanja službenika prema Uredbi zahvaća kako voditelje obrade, tako i izvršitelje obrade, i to u slučajevima, kako slijedi:

(1) ako obradu provodi tijelo javne vlasti ili javno tijelo (uz iznimku sudova koji djeluju u okviru svoje sudske nadležnosti),

(2) ako se osnovne djelatnosti voditelja ili izvršitelja obrade sastoje od postupaka obrade koji zbog svoje prirode, opsega i/ili svrha iziskuju redovito i sustavno praćenje ispitanika u velikoj mjeri, ili

(3) ako se osnovne djelatnosti voditelja ili izvršitelja obrade sastoje od opsežne obrade posebnih kategorija podataka ili osobnih podataka u vezi s kaznenim osudama i kažnjivim djelima.

Poslovi službenika obavljaju se u okviru njegova radnopravnog odnosa kod voditelja ili izvršitelja obrade, odnosno u okviru njegova ugovora o djelu kao „vanjskog" službenika. Službenik se imenuje temeljem stručnih kvalifikacija, osobito stručnog znanja o pravu i praksama u području zaštite podataka, kao i na temelju sposobnosti izvršavanja minimalno propisanih zadaća, u čemu ga je voditelj / izvršitelj obrade dužan podržavati osiguravanjem potrebnih sredstava za njihovo izvršavanje (kao i za održavanje njegova stručnog znanja) te pristupa osobnim podacima i postupcima obrade. Propisana je obveza voditelja i izvršitelja obrade da osiguraju to da službenik bude na primjeren način i pravodobno uključen u sva pitanja u pogledu zaštite osobnih podataka, te on mora izravno odgovarati najvišoj rukovodećoj razini. Pohvalna je u Uredbi predviđena, inače česta situacija u praksi gdje službenik za zaštitu podataka ispunjava i druge zadaće i dužnosti kod voditelja ili izvršitelja obrade, a u kojem slučaju ne smije doći do sukoba interesa. Moglo bi se tumačiti da bi nesukladni s položajem službenika bili svi položaji koji podrazumijevaju sudjelovanje u donošenju odluka o utvrđivanju svrha i načina obrade osobnih podataka (npr. ako je riječ o višem rukovodstvu: predsjednik uprave, direktor poslovanja, direktor financija, voditelj odjela za marketing, voditelj ljudskih resursa, voditelj odjela za informacijsku tehnologiju, i dr.).[110] Važna je i propisana obveza voditelja i izvršitelja obrade da osiguravaju to da službenik ne prima ikakve upute u pogledu izvršenja njegovih zadaća, kao i zabrana razrješenja dužnosti ili kažnjavanja ovog službenika zbog izvršavanja njegovih zadaća.

Minimalno propisane zadaće službenika za zaštitu podataka u Uredbi jesu, kako slijedi:

(1) obavještavanje i savjetovanje voditelja ili izvršitelja obrade te radnika koji obavljaju obradu o njihovim obvezama iz Uredbe te drugim odredbama prava EU-a ili države članice o zaštiti podataka;

(2) praćenje poštovanja Uredbe te drugih odredaba prava EU-a ili države članice o zaštiti podataka i politika voditelja ili izvršitelja obrade u odnosu na zaštitu osobnih podataka,

[110] Smjernice RS29 o službenicima za zaštitu podataka, koje je potvrdio EOZP; 16/HR WP 243 rev.01, 13.12. 2016., zadnje mijenjane i donesene 05.4.2017., http://azop.hr/images/dokumenti/217/wp243rev01_hr.pdf, str. 19.

uključujući raspodjelu odgovornosti, podizanje svijesti i osposobljavanje osoblja koje sudjeluje u postupcima obrade te povezane revizije;

(3) pružanje savjeta, kada to zatraži voditelj obrade, u pogledu procjene učinka na zaštitu podataka i praćenje njezina izvršavanja;

(4) suradnja s nadzornim tijelom; te

(5) djelovanje kao kontaktna točka za nadzorno tijelo o pitanjima u pogledu obrade, što uključuje i prethodno savjetovanje, te savjetovanje, prema potrebi, o svim drugim pitanjima.

Pristup zaštiti podataka prema Uredbi temeljen na procjeni rizika očituje se i u propisanoj obvezi službenika da kod obavljanja svojih zadaća vodi računa o riziku povezanom s postupcima obrade i uzima u obzir prirodu, opseg, kontekst i svrhe obrade.

Kontaktni podaci službenika objavljuju se i dostavljaju nadzornom tijelu. Osobito radi olakšavanja pretjeranog opterećenja resursa za voditelje i izvršitelje obrade u vezi s ovom funkcijom, Uredbom se predviđa mogućnost imenovanja jednog službenika od strane grupe poduzetnika (ako je isti lako dostupan iz svakog poslovnog nastana), odnosno od strane tijela javne vlasti ili javnog tijela koje ga može imenovati za nekoliko takvih vlasti ili tijela (uzimajući u obzir njihovu organizacijsku strukturu i veličinu).

5.3.19. Sankcije i pravni lijekovi

Posebna ozbiljnost nove Uredbe očituje se u propisanim najvišim upravnim novčanim kaznama koje se mogu izreći za povrede Uredbe, te čije izricanje mora u svakom pojedinačnom slučaju biti učinkovito, proporcionalno i odvraćajuće. One, naime, mogu iznositi: 1) do 10 mil. EUR, ili u slučaju poduzetnika do 2 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće; odnosno 2) do 20 mil. EUR, ili u slučaju poduzetnika do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome što je veće. Kod odlučivanja hoće li izreći upravnu novčanu kaznu, te pri određivanju visine takve kazne, nadzorna tijela (za zaštitu podataka) moraju uzeti u obzir niz Uredbom propisanih čimbenika.

Nadalje, pored mjera i novčanih upravnih kazni koje se izriču sukladno Uredbi, države članice utvrđuju pravila o ostalim sankcijama (kaznenopravnim, upravnim) koje se primjenjuju na kršenja Uredbe, posebno na ona kršenja koja ne podliježu upravnim novčanim kaznama po Uredbi, ali i na kršenja domaćih propisa donesenih u skladu s Uredbom. Te sankcije moraju biti učinkovite, proporcionalne i odvraćajuće.[111]

U slučajevima povreda prava predviđenih Uredbom raspoloživi su pravni lijekovi:

[111] Detaljnije o upravnim novčanim kaznama vidi u čl. 83.-84. i uvodnim izjavama br. 148.-150. i 152., te u Smjernicama RS29 o primjeni i određivanju upravnih novčanih kazni, koje je potvrdio EOZP, 17/HR RS253, 03.10.2017., http://azop.hr/images/dokumenti/217/wp253_hr_novcane_kazne.pdf.

(1) pravo na pritužbu nadzornom tijelu, (2) pravo na učinkoviti sudski pravni lijek protiv nadzornog tijela, (3) pravo na učinkoviti sudski pravni lijek protiv voditelja obrade ili izvršitelja obrade, te (4) pravo na naknadu štete.

Tako svaki ispitanik ima pravo (ne dovodeći u pitanje nijedan drugi upravni ili sudski pravni lijek) *podnijeti pritužbu nadzornom tijelu*, osobito u državi članici u kojoj ima uobičajeno boravište, u kojoj je njegovo radno mjesto ili mjesto navodnog kršenja, ako smatra da obrada osobnih podataka koja se odnosi na njega krši Uredbu.

Nadalje, svaki ispitanik ima pravo na učinkoviti sudski pravni lijek (ne dovodeći u pitanje nijedan drugi upravni ili izvansudski pravni lijek) *ako nadležno nadzorno tijelo ne riješi pritužbu ili ne izvijesti ispitanika u roku od tri mjeseca o napretku ili ishodu podnesene pritužbe nadzornom tijelu*. Postupci protiv nadzornog tijela vode se pred sudovima države članice u kojoj nadzorno tijelo ima poslovni nastan.

Isto tako, ne dovodeći u pitanje nijedan dostupan upravni ili izvansudski pravni lijek, ispitanik ima pravo na učinkoviti sudski pravni lijek *ako smatra da su mu zbog obrade njegovih osobnih podataka protivno Uredbi prekršena njegova prava iz Uredbe*. Postupci protiv voditelja obrade ili izvršitelja obrade vode se *pred sudovima države članice u kojoj voditelj obrade ili izvršitelj obrade ima poslovni nastan*. Osim toga, takvi se postupci mogu voditi pred sudovima države članice u kojoj ispitanik ima uobičajeno boravište, osim ako je voditelj obrade ili izvršitelj obrade tijelo javne vlasti neke države članice koje djeluje izvršavajući svoje javne ovlasti.

Pored navedenog, ne dovodeći u pitanje nijedan drugi upravni ili izvansudski pravni lijek, *svaka fizička ili pravna osoba* ima *pravo na učinkoviti sudski pravni lijek protiv pravno obvezujuće odluke nekog nadzornog tijela koja se na nju odnosi*. Postupci protiv nadzornog tijela vode se, kako je ranije navedeno, pred sudovima države članice u kojoj nadzorno tijelo ima poslovni nastan.

Kada je riječ o naknadi štete, svaka osoba koja je pretrpjela materijalnu ili nematerijalnu štetu zbog kršenja Uredbe ima *pravo na naknadu od voditelja obrade ili izvršitelja obrade za pretrpljenu štetu*. Ti se postupci vode pred istim sudovima koji su nadležni u postupcima protiv voditelja obrade ili izvršitelja obrade.[112]

5.3.20. Ograničenja od primjene pojedinih odredbi Uredbi i iznimke od primjene Uredbe (posebne situacije obrade osobnih podataka)

[112] Detaljnije o pravnim lijekovima vidi u čl. 77-82. te uvodnim izjavama br. 141-147. Uredbe.

Države članice mogu pod određenim uvjetima propisati ograničenja od primjene pojedinih odredbi Uredbe u domaćem pravu (čl. 23., uvodna izjava br. 73.).[113] Tim se ograničenjem mora poštovati bit temeljnih prava i sloboda te ono mora predstavljati nužnu i razmjernu mjeru u demokratskom društvu u neku od propisanih svrha, poput zaštite nacionalne kao i javne sigurnosti.[114] Uredbom se propisuje i minimalni sadržaj svake od tih zakonodavnih mjera/propisa.[115] Pored navedenih ograničenja koja države članice mogu uvesti u svoj zakonodavni okvir, Uredba ostavlja mogućnost državama članicama da ograniče primjenu pojedinih odredbi Uredbe, odnosno da donose posebne propise u pojedinim posebnim situacijama obrade osobnih podataka (poglavlje IX. Uredbe), konkretno u vezi s:

a) obradom osobnih podataka i slobodom izražavanja i informiranja (uklj. obradu u novinarske svrhe i svrhe akademskog, umjetničkog ili književnog izražavanja);
b) obradom osobnih podataka i javnim pristupom službenim dokumentima;
c) obradom nacionalnog identifikacijskog broja;
d) obradom osobnih podataka u kontekstu zaposlenja;
e) obradom osobnih podataka u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe;
f) obradom osobnih podataka i obvezama tajnosti, te
g) postojećim pravilima o zaštiti podataka crkava i vjerskih udruženja.

5.4. Zakon o provedbi Opće uredbe o zaštiti podataka (NN br. 42/18)

U Republici Hrvatskoj je nastavno na Uredbu donesen *Zakon o provedbi opće Uredbe o zaštiti podataka* (dalje i kao: Zakon), koji je stupio na snagu 25.5.2018. g. i kojim je stavljen izvan snage Zakon o zaštiti osobnih podataka te podzakonski propisi doneseni na temelju tog zakona.

5.4.1. Isključeno područje primjene Zakona

U skladu s materijalnim područjem primjene Uredbe u Zakonu se izričito utvrđuje da se isti ne odnosi se na obradu osobnih podataka koju obavljaju nadležna tijela u svrhu sprečavanja,

[113] Ograničenje opsega obveza i prava iz poglavlja III. Uredbe (čl. 12.-22. u poglavlju III. Uredbe: odjeljak 2. - informacije i pristup osobnim podacima; odjeljak 3. - ispravak i brisanje; odjeljak 4. - pravo na prigovor i automatizirano pojedinačno donošenje odluka), poglavlja IV. odjeljka 2 (obavješćivanje ispitanika o povredi osobnih podataka), te poglavlja II. čl. 5. (načela obrade osobnih podataka).

[114] Daljnje su propisane svrhe radi kojih se mogu utvrditi ograničenja pod ovim uvjetima: zaštita obrane; sprečavanje, istraga, otkrivanje ili progon kaznenih djela ili izvršavanje kaznenopravnih sankcija; zaštita drugih važnih ciljeva od općeg javnog interesa EU-a ili države članice; zaštita neovisnosti pravosuđa i sudskih postupaka; sprečavanje, istraga, otkrivanje i progon kršenja etike za regulirane struke; funkcija praćenja, inspekcije ili regulatorna funkcija makar povremeno povezana s izvršavanjem službene ovlasti u pojedinim ovdje propisanim slučajevima; zaštita ispitanika ili prava i sloboda drugih; te ostvarivanje potraživanja u građanskim sporovima.

[115] Voditelj obrade; svrha/kategorije obrade; kategorije osobnih podataka; opseg ograničenja; zaštitne mjere za sprečavanje zlouporabe ili nezakonitog pristupa ili prijenosa; rok pohrane i zaštitne mjere koje se mogu primijeniti uzimajući u obzir prirodu, opseg i svrhe/kategorije obrade; rizici za prava i slobode ispitanika, te pravo ispitanika da budu obaviješteni o ograničenju, osim ako može biti štetno za svrhu tog ograničenja.

istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja, kao ni na područje nacionalne sigurnosti i obrane (čl. 1. st. 2.). Naime, kako je ranije pojašnjeno, Uredba se *među ostalim* ne primjenjuje na obradu osobnih podataka tijekom djelatnosti koja ne spadaju u opseg prava EU-a, kao što su djelatnosti u području zaštite nacionalne sigurnosti, kao ni na obradu koju obavljaju nadležna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja, a što je uređeno *Direktivom (EU) 2016/680 o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP*).

5.4.2. Definicija tijela javne vlasti u smislu Zakona

Pojam tijela javne vlasti nije definiran Uredbom te je domaći zakonodavac odlučio taj pojam definirati za potrebe tumačenja i primjene ovog Zakona. Propisuje se tako da će u smislu ovog Zakona pojam tijela javne vlasti uključivati tijela državne uprave i druga državna tijela, jedinice lokalne i područne (regionalne) samouprave (čl. 3. st. 2.). Opseg tijela koja spadaju u pojam tijela javne vlasti za potrebe ovog Zakona bitno je uži u odnosu na opseg tijela javne vlasti kako su ista definirana drugim zakonima, napose Zakonom o pravu na pristup informacijama (NN br. 25/13 i 85/15, čl. 5. točka 2.).

5.4.3. Nadležno tijelo za akreditiranje certifikacijskih tijela u RH

Zakon utvrđuje, u skladu s čl. 43. Uredbe, *Hrvatsku akreditacijsku agenciju* kao nadležno tijelo za akreditiranje certifikacijskih tijela u Republici Hrvatskoj (čl. 5.).

5.4.4. AZOP: uspostava, zadaci, ovlasti

Agencija za zaštitu osobnih podataka (AZOP) osnovana je 2004. g. kao pravna osoba s javnim ovlastima na temelju ranijeg Zakona o zaštiti osobnih podataka. Zakonom o provedbi Opće uredbe ta se Agencija potvrđuje kao neovisno *državno* nadzorno tijelo u smislu Uredbe (ono prestaje biti pravna osoba s javnim ovlastima), koje je u svom radu samostalno i neovisno i za svoj rad odgovara Hrvatskome saboru.

Agencijom rukovodi ravnatelj, koji ima zamjenika, a oboje imenuje Hrvatski sabor na prijedlog Vlade RH temeljem javnog poziva za dostavu kandidatura. Ravnatelj, zamjenik ravnatelja i službenici AZOP-a ne smiju obavljati poslove službenika za zaštitu podataka za drugog voditelja ili izvršitelja obrade.

Sredstva za rad AZOP-a osiguravaju se u državnom proračunu. AZOP je dužan podnijeti godišnje izvješće o radu Hrvatskome saboru, propisanog sadržaja i to najkasnije do 31.3. tekuće godine za prethodnu godinu.

Osim što obavlja nadzor nad provedbom Uredbe i Zakona o provedbi Opće uredbe, AZOP obavlja nadzor i nad primjenom, u Republici Hrvatskoj, *Direktive (EU) 2016/680 o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP*), osim ako posebnim propisima nije drugačije određeno.

Dodatno na ovlasti nadzornih tijela utvrđene Uredbom, AZOP se Zakonom ovlašćuje na pokretanje i sudjelovanje u kaznenim, prekršajnim, upravnim i drugim sudskim i izvansudskim postupcima zbog povrede Uredbe i Zakona o provedbi Opće uredbe (kada je propisano posebnim zakonom), kao i na pokretanje i vođenje postupaka protiv odgovornih osoba, također zbog povrede Uredbe i Zakona. Pored navedenog utvrđuje se njegova nadležnost da u određenim posebnim slučajevima vezano za međunarodni prijenos osobnih podataka obustavi upravni postupak i predmet uputi Visokom upravnom sudu RH, a također i nadležnost Visokog upravnog suda da se tim povodom sukladno pravu EU-a obrati Sudu EU-a.[116]

Na pisani zahtjev fizičkih ili pravnih osoba AZOP izdaje stručna mišljenja iz područja zaštite osobnih podataka, koje ovo tijelo mora ovisno o složenosti zahtjeva izdati najkasnije u roku od 30 dana od dana podnošenja zahtjeva, a u iznimnim slučajevima se taj rok produljuje za dodatnih 30 dana.

Zakonom se utvrđuje i obveza središnjih tijela državne uprave i drugih državnih tijela na dostavu AZOP-u nacrta prijedloga zakona i prijedloga drugih propisa kojima se uređuju pitanja vezana uz obradu osobnih podataka, kako bi AZOP mogao izdati stručna mišljenja.

AZOP mora na svojim mrežnim stranicama objavljivati anonimizirana ili pseudonimizirana rješenja i mišljenja u pogledu vrsta obrada koje mogu prouzročiti visoki rizik za prava i slobode. Ako se ista odnose na maloljetnike, bit će anonimizirana radi njihove zaštite (čl. 18.)

U Zakonu se utvrđuje i ovlast AZOP-a da donosi odluke kojima se izriču upravne novčane kazne, kako za povrede Uredbe tako i Zakona. Međutim, to se neće odnositi na tijela javne vlasti (definiranih, kako je ranije pokazano, za potrebe ovog Zakona), budući da su ista tijela Zakonom isključena od primjene upravnih novčanih kazni.

[116] Posumnja li u valjanost odluke Europske komisije o primjerenosti i o standardnim ugovornim klauzulama, obustavit će upravni postupak i ustupiti predmet Visokom upravnom sudu RH na rješavanje upravne stvari. Ako Visoki upravni sud utvrdi da odluka Komisije nije valjana, uputit će zahtjev o ocjeni valjanosti te odluke Sudu EU-a. S ovime u vezi vidi i presudu Suda EU-a u predmetu C-362/14, Schrems protiv Data Protection Commissioner, EU:C:2015:650, t. 55-66; kao i Provedbenu odluku Komisije (EU) 2016/2297 od 16.12.2016. o izmjeni odluka 2001/497/EZ i 2010/87/EU o standardnim ugovornim klauzulama za prijenos osobnih podataka u treće zemlje i obrađivačima u tim zemljama u skladu s Direktivom 95/46/EZ, SL L 344, 17.12.2016, str. 100–101.

Osim toga, izriče li se upravna novčana kazna protiv pravne osobe s javnim ovlastima ili protiv pravne osobe koja obavlja javnu službu, ta kazna ne smije ugroziti obavljanje takve javne ovlasti ili javne službe. Protiv odluke AZOP-a o kazni nije dopuštena žalba, ali se može pokrenuti upravni spor pred nadležnim upravnim sudom.

Zakon posebno propisuje nekoliko prekršajnih odredbi, kao i vlastitih upravnih novčanih kazni za pojedine povrede tog Zakona. Prekršajne odredbe propisane su za ravnatelja i zamjenika ravnatelja AZOP-a, odnosno službenike AZOP-a u slučaju povreda Zakona kroz otkrivanje neovlaštenim osobama povjerljivih podataka za koje su doznali obavljanjem svoje funkcije, tj. radnog mjesta u AZOP-u.

Upravne se novčane kazne propisuju za slučaj povreda nekoliko Zakonom propisanih odredbi u vezi s provedbom videonadzora, na koje će se ukazati pri njihovu pregledu u nastavku teksta.

Pravomoćna rješenja AZOP-a objavljuju se na njegovim mrežnim stranicama bez anonimiziranja podataka o počinitelju, ako: (1) je tim rješenjem utvrđena povreda Zakona ili Uredbe u vezi s (a) obradom osobnih podataka maloljetnika, (b) obradom posebnih kategorija osobnih podataka, (c) automatiziranim pojedinačnim donošenjem odluka, profiliranjem; ili (2) ako je povredu počinio voditelj obrade ili izvršitelj obrade koji je već bio prekršio odredbe Zakona ili Uredbe, ili (3) kod izrečene pravomoćne odluke o upravnoj novčanoj kazni u iznosu od najmanje 100.000,00 kuna.[117]

5.4.5. Postupak u nadležnosti AZOP-a i prava ispitanika u vezi s pravnim lijekovima

Vezano za Uredbom predviđeno pravo na pritužbu nadzornom tijelu, Zakonom se posebno utvrđuje (u istoj mjeri kao i ranijim Zakonom o zaštiti osobnih podataka) pravo osobe da podnese AZOP-u *zahtjev za utvrđivanje povrede prava*, ako smatra da joj je povrijeđeno pravo zajamčeno kako Zakonom tako i Uredbom. O povredi prava AZOP odlučuje rješenjem, koje je upravni akt. Protiv tog rješenja žalba nije dopuštena, ali je tužbom moguće pokrenuti upravni spor pred nadležnim upravnim sudom (čl. 34. Zakona)

Nadalje, kada je riječ o *zastupanju ispitanika*, u skladu s mogućnostima predviđenim Uredbom Zakon utvrđuje pravo ispitanika da ovlasti neprofitno tijelo, organizaciju ili udruženje koje je osnovano u skladu sa zakonom, a u čijem se statutu navode ciljevi od javnog interesa te je aktivno u području zaštite prava i sloboda ispitanika s obzirom na zaštitu njegovih osobnih podataka, da podnese pritužbu u njegovo ime i da u njegovo ime ostvaruje sve Uredbom predviđene pravne lijekove (čl. 41. Zakona).[118]

5.4.6. Obrada osobnih podataka u posebnim slučajevima

[117] Detaljnije o uspostavi, zadacima, ovlastima AZOP-a vidi u poglavljima II-III, VI-VIII. Zakona.
[118] Detaljnije o postupku u nadležnosti AZOP-a i pravnim lijekovima vidi u poglavlju V. Zakona.

Materijalnopravni uvjeti za *obradu osobnih podataka putem videonadzora* čine najveći dio odredbi Zakona kojima se uređuje obrada osobnih podataka u posebnim slučajevima (čl. 25-32.). Inače ta materija nije posebno uređena Uredbom, budući da ista sadrži tehnološki neutralna pravila koja ne ovise o korištenim tehnologijama. Nadalje, kako je ranije pokazano, Uredba ostavlja mogućnost državama članicama da donose posebne propise u pojedinim posebnim situacijama obrade osobnih podataka, među ostalim obrade osobnih podataka u statističke svrhe.[119] Zakon koristi navedenu mogućnost kada je riječ o *obradi osobnih podataka u svrhu izrade službene statistike*. Pored navedenog, sukladno drugim relevantnim odredbama Uredbe Zakon posebno uređuje uvjete obrade osobnih podataka u vezi s *privolom djeteta u odnosu na usluge informacijskog društva* te s *obradom genetskih i biometrijskih podataka.*

a) Obrada osobnih podataka putem videonadzora

U općim odredbama o videonadzoru (čl. 25-29.) utvrđuje se kako videonadzor u smislu Zakona podrazumijeva *prikupljanje i daljnju obradu osobnih podataka koja obuhvaća stvaranje snimke koja čini ili je namijenjena da čini dio sustava pohrane*. Ako drugi zakon drugačije ne propisuje, na obradu osobnih podataka putem videonadzora primjenjuju se odredbe ovog Zakona. Nadalje, utvrđuje se da se obrada osobnih podataka putem videonadzora smije provoditi *samo u svrhu koja je nužna i opravdana za zaštitu osoba i imovine te pod uvjetom da ne prevladavaju interesi ispitanika koji su u suprotnosti s takvom obradom*. Zakon uređuje i područja koja videonadzor smije obuhvatiti, a to su isključivo prostorije, dijelovi prostorija, vanjska površina objekta, kao i unutarnji prostor u sredstvima javnog prometa, čiji je nadzor nužan radi postizanja gore navedene svrhe. Propisuje se i rok od 6 mjeseci kao najdulji rok čuvanja snimki dobivenih videonadzorom, osim ako je drugim zakonom propisan duži rok ili ako su iste dokaz u sudskom, upravnom, arbitražnom ili drugom istovrijednom postupku.

Zakon predviđa mogućnost izricanja najviše upravne novčane kazne do 50.000,00 kuna u slučaju pojedinih povreda općih pravila o videonadzoru (čl. 51.).

Prva povreda o kojoj je riječ, jest: *neoznačavanje objekta, prostorija, dijelova prostorija te vanjske površine objekte u skladu sa Zakonom*. Naime, voditelj ili izvršitelj obrade dužan je označiti da je objekt odnosno pojedina prostorija u njemu te vanjska površina objekta pod videonadzorom, a oznaka treba biti vidljiva najkasnije prilikom ulaska u perimetar snimanja. Ta obavijest treba sadržavati sve relevantne informacije sukladno Uredbi (čl. 13.), a posebno jednostavnu i lako razumljivu sliku uz tekst kojim se ispitanicima pružaju sljedeće informacije: (1) da je prostor pod videonadzorom; (2) podatke o voditelju obrade i (3) podatke za kontakt putem kojih ispitanik može ostvariti svoja prava.

Druga povreda Zakona za koju se može izreći spomenuta kazna sastoji se od nepostupanja voditelja i izvršitelja obrade po njihovoj obvezi *uspostave automatiziranog sustava zapisa za*

[119] Čl. 89. st. 1, 2 i 4..; vidi i dodatna pojašnjenja u uvodnim izjavama br. 156, 162-163. Uredbe.

evidentiranje pristupa snimkama videonadzora s obveznim podacima (vremenom i mjestom pristupa te oznakom osoba koje su pristupale podacima prikupljenim putem videonadzora). Sustav videonadzora, naime, prema Zakonu mora biti zaštićen od pristupa neovlaštenih osoba.

Treća i zadnja povreda za koju se može izreći upravna kazna propisana ovim Zakonom zahvaća osobe koje su prema tom propisu ovlaštene pristupiti podacima prikupljenim putem videonadzoru (odgovorne osobe voditelja obrade odnosno izvršitelja obrade i/ili osobe koje isti ovlasti), ukoliko te osobe koriste snimke iz sustava videonadzora suprotno propisanoj svrsi. S ovime u vezi valja napomenuti i to da se Zakonom izričito dopušta pristup podacima prikupljenim putem videonadzora za nadležna državna tijela, kada to čine u okviru obavljanja poslova iz svog zakonom utvrđenog djelokruga.

Pored navedenih općih odredbi Zakonom se utvrđuju i pravila o videonadzoru radnih prostorija (čl. 30.), videonadzoru stambenih i poslovno-stambenih zgrada (čl. 31.) te videonadzoru javnih površina (čl. 32.).

Kada je riječ o *videonadzoru radnih prostorija*, Zakon propisuje da se obrada osobnih podataka radnika putem videonadzora može provoditi samo ako su uz uvjete utvrđene tim Zakonom ispunjeni i uvjeti utvrđeni propisima kojima se regulira zaštita na radu[120] i ako su radnici bili na primjeren način unaprijed obaviješteni o takvoj mjeri te ako ih je poslodavac obavijestio prije donošenja odluke o postavljanju sustava videonadzora. Zabranjen je nadzor nad prostorijama za odmor, osobnu higijenu i presvlačenje. U kontekstu poslodavčeve odluke o uvođenju videonadzora i povezanih postupaka obrade osobnih podataka radnika potrebno je paziti i na primjenu relevantnih odredbi *Zakona o radu.*[121]

U pogledu *videonadzora stambenih,* odnosno *poslovno-stambenih zgrada* Zakon propisuje kao uvjet za uvođenje tog nadzora ishodovanje suglasnosti suvlasnika koji čine najmanje 2/3 suvlasničkih dijelova.[122] Osim toga utvrđuje se da videonadzor može zahvatiti samo pristup ulascima i izlascima iz stambenih zgrada te zajedničke prostorije u stambenim zgradama, te se zabranjuje korištenje videonadzora za praćenje radne učinkovitosti domara, spremačica i drugih osoba koje rade u stambenoj zgradi.

Kada je riječ o *videonadzoru na javnim površinama*, isti se Zakonom dopušta samo za tijela javne vlasti, pravne osobe s javnim ovlastima i pravne osobe koje obavljaju javnu službu, i to

[120] Vidi čl. 43. Zakona o zaštiti na radu (NN br. 71/14, 118/14 i 154/14).

[121] Vidi osobito čl. 29., čl. 150. st. 1. i 3. te čl. 151. st. 1. t. 7. Zakona o radu (NN br. 93/14 i 127/17).

[122] Do uređenja ove materije Zakonom AZOP je tumačio uvođenje videonazora u stambenim zgradama kao posao izvanrednog upravljanja zgradom, za koji je prema čl. 41. Zakona o vlasništvu i drugim stvarnim pravima bila potrebna suglasnost svih suvlasnika (rješenje od 13.7.2016., Kl.: UP/I-041-02/16-01/63; Ur.br.: 567-02/03-16-01, http://azop.hr/images/dokumenti/492/rjesenje-zastita_privatnosti_stanara.pdf.

samo ako je propisano zakonom, ako je nužno za izvršenje poslova i zadaća tijela javne vlasti ili radi zaštite života i zdravlja ljudi te imovine.[123]

a) Privola djeteta u kontekstu korištenja *online* usluga

Zakonom se uvode odredbe o privoli djeteta za obradu osobnih podataka u vezi s njegovim korištenjem usluga informacijskog društva (čl. 19.). Kako je ranije pokazano, Uredba je ostavila državama članicama mogućnost da zakonom predvide i nižu od postavljene dobne granice od 16 godina, zaključno s dobi od 13 godina. Međutim, Zakon ne propisuju nižu dobnu granicu, već izričito potvrđuje najvišu granicu predviđenu Uredbom. Drugim riječima, kada je riječ o djetetu s prebivalištem u Republici Hrvatskoj, obrada osobnih podataka djeteta u vezi s njegovim korištenjem usluga informacijskog društva, a koja se temelji na njegovoj privoli, zakonita je ako dijete ima najmanje 16 godina.

b) Obrada genetskih podataka

Zakon utvrđuje zabranu obrade genetskih podataka radi izračuna izgleda bolesti i drugih zdravstvenih aspekata ispitanika u okviru radnji za sklapanje ili izvršavanje ugovora o životnom osiguranju i ugovora s klauzulama o doživljenju, ako je riječ o *genetskim podacima ispitanika koji u Hrvatskoj sklapaju ugovore o životnom osiguranju i ugovore s klauzulama o doživljenju ako obradu provodi voditelj obrade s poslovnim nastanom u Hrvatskoj ili koji pruža usluge u Hrvatskoj*. Ta se zabrana ne ukida ni danom privolom ispitanika (čl. 20.).

c) Obrada biometrijskih podataka

Zakon utvrđuje više pravila (čl. 21-24.) kada je riječ o biometrijskim podacima ispitanika u Hrvatskoj gdje obradu provodi voditelj obrade s poslovnim nastanom u Hrvatskoj ili koji pruža usluge u Hrvatskoj, odnosno tijelo javne vlasti. Ta se pravila neće primjenjivati u područjima obrane, nacionalne sigurnosti i sigurnosno-obavještajnog sustava.

Posebno se propisuju pravila za obradu navedenih podataka: (1) u privatnom sektoru, (2) u tijelima javne vlastima i (3) kada je riječ o podacima zaposlenika u svrhu evidentiranja radnog vremena i radi ulaska i izlaska iz službenih prostorija.

Tako se, kada je riječ o *obradi biometrijskih podataka u privatnom sektoru* utvrđuje da je takva obrada dopuštena samo ako je propisana zakonom ili ako je nužna za zaštitu osoba, imovine, klasificiranih podataka, poslovnih tajni ili za pojedinačno i sigurno identificiranje korisnika

[123] Za primjere domaćih propisa koji uređuju materiju videonadzora na javnim površinama vidi: Pravilnik o načinu i uvjetima obavljanja poslova privatne zaštite na javnim površinama (NN br. 36/12) i Zakon o sprječavanju nereda na športskim natjecanjima (NN br. 117/03, 71/06, 43/09 i 34/11).

usluga, uzimajući u obzir da ne prevladavaju interesi ispitanika koji su u suprotnosti s ovim zakonom propisanom obradom tih podataka. Kada je riječ o obradi biometrijskih podataka ispitanika radi sigurnog identificiranja korisnika usluga, Zakon utvrđuje pravni temelj za takvu obradu, a to je njihova *izričita privola* (koja se, dakako, mora dati sukladno uvjetima propisanima Uredbom).

Obrađuju li se biometrijski podaci *u tijelima javne vlasti*, to je dopušteno pod uvjetom da je takva obrada određena zakonom i ako je nužna za zaštitu osoba, imovine, klasificiranih podataka ili poslovnih tajni, uzimajući u obzir da ne prevladavaju interesi ispitanika koji su u suprotnosti s ovim zakonom propisanom obradom tih podataka. Zakonom je propisana i presumpcija zakonite obrade tih podataka ukoliko je ista potrebna za ispunjenje obveza iz međunarodnih ugovora u vezi s identificiranjem pojedinca u prelasku državne granice.

Naposljetku, kada je riječ o *obradi biometrijskih podataka zaposlenika u svrhu evidentiranja radnog vremena i radi ulaska i izlaska iz službenih prostorija*, ista se dopušta samo ako je propisana zakonom ili ako se takva obrada provodi kao alternativa drugom rješenju za evidentiranje radnog vremena ili ulaska i izlaska iz službenih prostorija, uz uvjet da je za to zaposlenik dao izričitu privolu (sukladno Uredbi).

d) Obrada osobnih podataka u svrhu izrade službene statistike

Zakon sukladno uvjetima utvrđenima Uredbom[124] propisuje da u okviru obrade osobnih podataka u svrhu proizvodnje službene statistike (u skladu s posebnim propisima iz područja službene statistike), tijela koja proizvode službenu statistiku nisu dužna osigurati ispitanicima pojedina prava (pristup, ispravak, ograničenje obrade osobnih podataka, pravo na prigovor), a to radi osiguravanja uvjeta nužnih za ostvarivanje svrhe službene statistike u mjeri u kojoj je vjerojatno da bi se takvim pravima moglo onemogućiti ili ozbiljno ugroziti postizanje tih svrha, te kada su takva odstupanja od prava prijeko potrebna za postizanje tih svrha. Osim toga, propisana je obveza tijela nadležnih za proizvodnju službene statistike da primjenjuju tehničke i organizacijske mjere zaštite podataka prikupljenih za potrebe službene statistike. Voditelji obrade nisu prilikom prijenosa osobnih podataka tijelima nadležnima za službenu statistiku dužni obavještavati ispitanike o prijenosu tih podataka u statističke svrhe. Nadalje, obrada osobnih podataka u statističke svrhe smatra se podudarnom svrsi za koju su podaci prikupljeni, pod uvjetom da se poduzmu odgovarajuće zaštitne mjere. Osobni podaci obrađeni u statističke svrhe ne smiju omogućiti identifikaciju osobe na koju se podaci odnose (čl. 33.)

5.5. Kazneno djelo nedozvoljene uporabe osobnih podataka

Kako je ranije pokazano, države članice dužne su prema Uredbi utvrditi, pored mjera i novčanih upravnih kazni koje se izriču sukladno Uredbi, pravila o ostalim sankcijama

[124] Čl. 89. st. 1, 2 i 4. i uvodne izjave br. 156., 162.-163. Uredbe.

(kaznenopravnim, upravnim) koje se primjenjuju na kršenja Uredbe, posebno na ona kršenja koja ne podliježu upravnim novčanim kaznama po Uredbi, ali i na kršenja domaćih propisa donesenih u skladu s Uredbom. Te sankcije moraju biti učinkovite, proporcionalne i odvraćajuće (čl. 84. i uvodne izjave 149. i 152. Uredbe).

Kada je riječ o kaznenopravnim sankcijama u domaćem pravnom okviru potrebno je na prvome mjestu istaknuti sankcije propisane Kaznenim zakonom RH (NN br. 125/11, 144/12, 56/15, 61/15 i 101/17) za slučaj počinjenja *kaznenog djela nedozvoljene uporabe osobnih podataka* (čl. 146.), a koje pripada djelima protiv privatnosti.[125]

Kazneno djelo nedozvoljene uporabe osobnih podataka čini bilo tko tko protivno uvjetima određenima u zakonu prikuplja, obrađuje ili koristi osobne podatke fizičkih osoba. Ovo se kazneno djelo pokreće po službenoj dužnosti te se kao sankcija predviđa isključivo kazna zatvora koja u osnovnom obliku ovog djela može biti izrečena u najduljem trajanju od godine dana zatvora. Nadalje, predviđaju se kao kvalificirani oblici toga djela obrada osobnih podataka protivno zakonu čime je pribavljena znatna imovinska korist ili prouzročena znatna šteta (vrijednost imovinske koristi, tj. štete koja prelazi 60.000,00 kn prema čl. 87. st. 29. Kaznenog zakona), izvoz osobnih podataka iz RH radi daljnje obrade protivno zakonu, odnosno objava podataka ili njihovo činjenje dostupnima drugima na koji drugi način protivno zakonu, za što se predviđa kazna zatvora do tri godine. Kvalificirani oblik predviđa se i u slučaju prikupljanja, obrade odnosno korištenja osobnih podataka djeteta kao i posebne kategorije osobnih podataka protivno zakonu. U vezi sa svim navedenim se kao daljnji kvalificirani oblik djela propisuje počinjenje tih djela od strane službene osobe u obavljanju službe ili odgovorne osobe u obavljanju javne ovlasti, za što je zapriječena kazna zatvora od najmanje šest mjeseci do najviše pet godina zatvora.

5.6. Zaštita osobnih podataka i privatnost u području elektroničkih komunikacija

Posebna pravila zaštite osobnih podataka i privatnosti u području elektroničkih komunikacija na razini prava EU-a sadržana su u *Direktivi 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u elektroničkom komunikacijskom sektoru* (dalje: Direktiva o e-privatnosti), čije su odredbe provedene u odgovarajuće odredbe našeg *Zakona o elektroničkim komunikacijama* (ZEK-a).[126]

Nove digitalne mreže imaju značajno velike kapacitete i mogućnosti obrade osobnih podataka. Važan razlog za donošenje Direktive o e-privatnosti poglavito je razvoj Interneta, koji daje zajedničku infrastrukturu za pružanje niza različitih elektroničkih komunikacijskih usluga. Bitno je osigurati uspješan prekogranični razvoj ovih novih usluga kao temelja razvoja informacijskog društva, što u svakom slučaju ovisi i o povjerenju korisnika u pogledu jamstava zaštite njihovih sloboda i prava, osobito prava privatnosti.

[125] Ostala su kaznena djela protiv privatnosti (Glava XIV.): narušavanje nepovredivosti doma i poslovnog prostora (čl. 141.), povreda tajnosti pisama i drugih pošiljaka (čl. 142.), neovlašteno zvučno snimanje i prisluškivanje (čl. 143.), neovlašteno slikovno snimanje (čl. 144.) te neovlašteno otkrivanje profesionalne tajne (čl. 145.).

[126] NN 73/08, 90/11, 133/12, 80/13, 71/14 i 72/17.

Drugim riječima, pored niza prednosti koje korisnicima i društvu donosi opisani razvoj tehnologije, mreža i usluga, njime se također otvaraju novi rizici za privatnost korisnika.

5.6.1. Hrvatska regulatorna agencija za mrežne djelatnosti

Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM) domaći je regulator tržišta elektroničkih komunikacija, poštanskih usluga i željezničkih usluga. U nadležnost HAKOM-a spada i davanje stručnih mišljenja i objašnjenja u primjeni ZEK-a i propisa donesenih na temelju tog zakona.

Dio njegovih usluga čini promicanje interesa korisnika usluga i kroz osiguravanje visoke razine zaštite osobnih podataka i privatnosti, kao i kroz osiguravanje održavanja cjelovitosti i sigurnosti javnih komunikacijskih mreža (čl. 5. st. 4. t. 3. i 6.). Nadzor nad provedbom usklađenosti poslovanja operatora elektroničkih komunikacijskih mreža i/ili usluga s odredbama zakona o sigurnosti i cjelovitosti elektroničkih komunikacijskih mreža i usluga te zaštiti osobnih podataka izričito se utvrđuje kao jedan od poslova u nadležnosti HAKOM-a, koji se obavlja kao javna ovlast (čl. 12. st. 1. t. 13).

U provedbi odredbi Zakona o elektroničkim komunikacijama, HAKOM surađuje između ostalog s AZOP-om, kao i s tijelima nadležnim za usklađivanje prevencije i zaštitu od računalnih ugroza sigurnosti informacijskih sustava, u skladu s posebnim zakonom kojim je uređena informacijska sigurnost te u skladu s preporukama Europske agencije za sigurnost mreža i podataka, engl. *European Network and Information Security Agency*, skraćeno: ENISA (čl. 6. st. 4.).

HAKOM i AZOP međusobno surađuju u provedbi odredbi Zakona o elektroničkim komunikacijama u kojima je implementirana Direktiva o e-privatnosti. Naime, u zakonu se propisuje da oba navedena tijela mogu *u skladu sa svojim ovlastima*, po službenoj dužnosti ili na zahtjev zainteresirane strane, odlukom narediti prestanak povreda pojedinih odredaba tog zakona (čl. 99. – 107). Tu odluku ona mogu donijeti po službenoj dužnosti ili na zahtjev zainteresirane strane (čl. 107a). Radi se ovdje o odredbama koje su pretežito, *ali ne isključivo* donesene u skladu s odgovarajućim odredbama Direktive. Tako na primjer, rješenja o zlonamjernim ili uznemiravajućim pozivima u čl. 105. i o pojedinim posebnim obvezama operatora usluga elektroničke pošte kao što je *inter alia* filtriranje dolazne elektroničke pošte s neželjenim elektroničkim porukama ili štetnim sadržajem (čl. 107. st. 5-10) nisu uvedena u zakon sukladno Direktivi. Prema tome, AZOP ne bi bio nadležan za slučaj povreda takvih odredbi, kao i u svim slučajevima kada se relevantnim odredbama štite legitimni interesi pravnih osoba. To se odnosi i na pojedine odredbe o sigurnosti i cjelovitosti elektroničkih komunikacijskih mreža i usluga koje nisu u izravnoj vezi s mjerama i postupcima za slučaj povreda osobnih podataka (samo potonji su regulirani Direktivom o e-privatnosti.).

HAKOM obavlja inspekcijski nadzor (tj. inspektori elektroničkih komunikacija kao ovlašteni radnici HAKOM-a) nad primjenom Zakona o elektroničkim komunikacijama i propisa donesenih na temelju tog zakona, te međunarodnih ugovora i sporazuma iz područja elektroničkih komunikacija koji obvezuju RH. Inspektori su ovlašteni izdati prekršajni nalog kojim izriču novčane kazne i zaštitne mjere propisane ZEK-om ili predložiti

HAKOM-u podnošenje optužnog prijedloga radi pokretanja prekršajnog postupka. Protiv rješenja inspektora nije dopuštena žalba, ali se protiv njega može pokrenuti upravni spor pred mjesno nadležnim upravnim sudom. Iznimno, protiv rješenja inspektora u vezi s osobito teškim i teškim povredama Zakona o elektroničkim komunikacijama može se pokrenuti upravni spor pred Visokim upravnim sudom RH (čl. 111. st. 1-2 i čl. 116.).

5.6.2. Tajnost elektroničkih komunikacija i pripadajućih prometnih podataka

U Zakonu o elektroničkim komunikacijama utvrđuju se sukladno Direktivi o e-privatnosti (čl. 5.) pojedine posebne obveze radi osiguravanja tajnosti elektroničkih komunikacija i pripadajućih prometnih podataka u javnim komunikacijskim mrežama i javno dostupnim komunikacijskim uslugama (čl. 100.).

Ta je obveza u izravnoj vezi s čl. 36. Ustava Republike Hrvatske zajamčenom slobodom i tajnošću dopisivanja te svih drugih oblika općenja osobe te s jamstvom prava na poštovanje privatnog života i dopisivanja prema članku 8. Konvencije o zaštiti ljudskih prava i temeljnih sloboda.

Temeljno je pravilo propisano u čl. 100. Zakona o elektroničkim komunikacijama, zabrana slušanja, prisluškivanja, pohranjivanja te svakog (drugog) oblika presretanja ili nadzora elektroničkih komunikacija i pripadajućih prometnih podataka. Međutim, ta zabrana nije apsolutna. Osim u slučaju primjene posebnih nadzornih mjera (na primjer, u kontekstu kaznenog postupka i u svrhu zaštite nacionalne sigurnosti), postoje i druge okolnosti radi kojih je pojedini oblik nadzora komunikacija nužan. Određene aktivnosti nisu obuhvaćene spomenutom zabranom - tehnička pohrana podataka koja je nužna za prijenos komunikacije te zakonski ovlašteno bilježenje komunikacija i pripadajućih prometnih podataka tijekom zakonitih poslovnih radnja u svrhu pružanja dokaza o trgovačkim transakcijama ili drugim poslovnim komunikacijama.

Predmet zaštite sukladno izloženoj odredbi jesu komunikacija i pripadajući prometni podaci, koji su definirani u čl. 2. Zakona o elektroničkim komunikacijama. *Komunikacija* se definira kao svaka obavijest razmijenjena ili prenesena između konačnog broja sudionika putem javno dostupne elektroničke komunikacijske usluge. Ona ne obuhvaća obavijesti koje se prenose javnosti elektroničkom komunikacijskom mrežom u sklopu djelatnosti radija i televizije, osim obavijesti koje se mogu povezati s odredivim pretplatnikom ili korisnikom usluga koji ih prima.

Prometni su podaci bilo koji podaci koji se obrađuju u svrhu prijenosa komunikacije elektroničkom komunikacijskom mrežom ili u svrhu obračuna i naplate troškova.

5.6.3. Obrada prometnih podataka

U pravnom okviru EU-a se u kontekstu korištenja javno dostupnih elektroničkih komunikacijskih usluga jamči posebna zaštita prava korisnika tih usluga u vezi s prikupljanjem i daljnjom obradom *prometnih podataka koji se na njih odnose*.

Ti podaci, naime, sadrže informacije o privatnom životu fizičkih osoba i tiču se prava na poštovanje dopisivanja (komunikacije) fizičkih osoba, ali i određenih legitimnih interesa

pravnih osoba.[127] Kako je ranije navedeno, prometne podatke čine svi podaci koji se obrađuju u svrhu prijenosa komunikacije elektroničkom komunikacijskom mrežom ili u svrhu obračuna i naplate troškova. Tipični su primjeri tih podataka u telefoniji, na primjer, podaci o tome kada je tko koga zvao i koliko dugo je poziv trajao. U prometne podatke može između ostalog spadati oblik u kojem se komunikacija prenosi putem mreže, kao i podaci koji se odnose na usmjeravanje, trajanje, vrijeme ili volumen komunikacije, na korišteni protokol, na lokaciju terminalne opreme pošiljatelja odnosno primatelja, na mrežu u kojoj komunikacija započinje ili završava, kao i podaci koji se odnose na početak, kraj ili trajanje veze.[128]

Potreba osiguravanja posebnije zaštite prometnih podataka ukazuje se prvenstveno u kontekstu prava svake osobe na poštovanje njezinog privatnog života. Naime, na temelju ovih se podataka može dobiti uvid u, odnosno mogu se donositi zaključci o nizu različitih aspekata privatnog života osobe na koju se ti podaci odnose, kao što su to njezine aktivnosti i interesi pa i njezina lokacija, to jest kretanje u određenom vremenskom razdoblju (kada se radi o mobilnoj telefoniji).

Analiza podataka o upućivanim pozivima može omogućiti, na primjer, utvrđivanje detalja o društvenom životu pozivatelja, kao što je to krug osoba s kojima je on u bliskom društvenom odnosu (pored podataka o pozivanim brojevima, dodatni se detalji mogu otkriti analizom drugih podataka u vezi s pozivima, kao što je to vrijeme pozivanja i učestalost pozivanja pojedinih brojeva, te duljina trajanja razgovora). Na temelju prometnih se podataka može dobiti uvid u različite interese i sklonosti pozivatelja, kao što bi to na primjer bila potrošačka sklonost, sklonost sudjelovanju u igrama na sreću, traženju savjeta određenih vrsta (na primjer, učestalo korištenje linija za tarot, horoskop) i dr. Kontaktiranje pojedinih specijaliziranih linija koje, na primjer, daju savjetovanja o pojedinim zdravstvenim pitanjima, ili pak psiholoških i bračnih savjetovališta, omogućuje profiliranje pozivatelja i u odnosu na najintimnije aspekte njegove ličnosti.

U kontekstu izloženih posebnih obzira odnosno veze koju prometni podaci imaju s osobom na koju se oni odnose u našem su Zakonu o elektroničkim komunikacijama sukladno Direktivi o e-privatnosti (čl. 6.) utvrđene posebne obveze operatora javno dostupnih elektroničkih komunikacijskih usluga, odnosno javnih komunikacijskih mreža, prilikom njihovog prikupljanja odnosno obrade (čl. 102.).

Tako je temeljna obveza tih operatora da prometne podatke koji se odnose na pretplatnike ili korisnike usluga, a koje je taj operator obradio i pohranio, *obriše ili anonimizira (učini neimenovanima) čim oni više nisu potrebni u svrhu prijenosa komunikacije.*

Međutim, postoji i niz potreba odnosno okolnosti radi kojih će navedeni operatori trebati koristiti prometne podatke koji se odnose na pretplatnike ili korisnike usluga, a koji nisu anonimizirani. To će značiti da se izloženo osnovno pravilo brisanja ili anonimizacije prometnih podataka kada više nisu potrebni radi prijenosa komunikacije, u takvim slučajevima neće primjenjivati. No da bi se ovo realiziralo, potrebno je da su prethodno zadovoljena određena posebna pravila. Kako ćemo vidjeti, pravila koja su u tom smislu propisana tiču se obrade prometnih podataka u određene svrhe i ona u osnovi odražavaju temeljna načela zaštite osobnih podataka, kao što su to, između ostalog, načelo određenosti svrhe obrade podataka i načelo razmjernosti (proporcionalnosti).

---

[127] Uvodna izjava br. 26. Direktive o e-privatnosti.
[128] Uvodna izjava br. 15. Direktive o e-privatnosti.

Prometni podaci koji se odnose na pretplatnike, odnosno korisnike usluga moraju se obrađivati *radi obračuna i naplate troškova* pružene usluge. U našem se zakonu tako propisuje da operatori smiju obrađivati *one prometne podatke koji su potrebni za* obračun troškova elektroničkih komunikacijskih usluga pretplatnika ili korisnika usluga te troškova međupovezivanja, ali samo do zastare tražbina u skladu s općim propisima o obveznopravnim odnosima (drugim riječima, do kraja razdoblja tijekom kojega se račun može zakonski osporiti ili tijekom kojega se plaćanje može izvršiti).

Operatori su dužni obavijestiti pretplatnike, odnosno korisnike usluga o vrstama prometnih podataka koji se obrađuju i o trajanju obrade podataka u svrhe obračuna troškova elektroničkih komunikacijskih usluga, te troškova međupovezivanja. Obavještavanje je moguće, na primjer, putem općih uvjeta poslovanja operatora, odnosno u okviru pretplatničkog ugovora. Nadalje, pristup obradi prometnih podataka u takvim je slučajevima dopušten isključivo ovlaštenim osobama operatora koje rade na poslovima obračuna troškova, te se isti mora ograničiti na najnužnije radnje u vezi s obavljanjem tih poslova. Pristup obradi prometnih podataka mora se ograničiti na najnužnije radnje u vezi s obavljanjem ranije spomenutih poslova. Intencija je ovog pravila sprečavanje nastupa rizika od toga da neovlaštene osobe obrađuju prometne podatke na bilo koji način, kao i osiguravanje toga da osobe koje jesu ovlaštene obrađivati ove podatke ne obavljaju takve aktivnosti obrade podataka, koje bi bile nepotrebne odnosno suvišne.

Operatori javnih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga, osim što trebaju obrađivati prometne podatke i kada je u pojedinim slučajevima potrebno da bi se otkrile tehničke neispravnosti ili greške u prijenosu komunikacija, te podatke trebaju obrađivati i radi *otkrivanja te zaustavljanja prijevara u vidu neplaćenog korištenja elektroničke komunikacijske usluge*.

U našem se zakonu propisuje, naime, da je pristup obradi prometnih podataka (u okviru zakonom propisanih uvjeta propisanih za dopuštenu obradu) dopušten isključivo *ovlaštenim osobama* operatora koje između ostalog rade na poslovima upravljanja elektroničkom komunikacijskom mrežom, obrade pritužbi potrošača i otkrivanja prijevara.

Pored navedene svrhe, prometni podaci koji se odnose na korisnike usluga mogu se obrađivati u druge zakonom izričito propisane svrhe i pod posebno propisanim uvjetima. Valja ovdje istaknuti svrhu *promidžbe* (i prodaje) elektroničkih komunikacijskih usluga, kao i *svrhu pružanja pojedinih posebnih usluga*.

Što se potonjih usluga tiče, prema Direktivi o e-privatnosti ovdje se radi o tzv. *uslugama s dodanom vrijednosti* (engl. *value-added services*). Radi se o uslugama radi čijeg se pružanja prometni podaci (ili podaci o lokaciji bez prometnih podataka) trebaju obrađivati u širem opsegu, odnosno izvan opsega koji je nužan za realizaciju samog prijenosa komunikacije ili obračuna te naplatu njezinih troškova, kao što bi na primjer bile usluge koje bi uključivale davanje informacija o stanju na cestama, o prometu, vremenskoj prognozi i turističke informacije.[129]

Iako je u našem zakonu definicija usluga s dodanom vrijednosti pa prema tome i korištenje tog pojma bilo u skladu s odgovarajućim odredbama Direktive o e-privatnosti, s izmjenama tog zakona 2011. g. u njemu se koristi drugačiji pojam (tzv. *usluge s posebnom tarifom*).

[129] Čl. 2. st. 2 g i uvodna izjava br. 18. Direktive o e-privatnosti.

Posebno treba istaknuti uvjet propisani uvjet *prethodne privole* pretplatnika ili korisnika usluga, a koja se daje nakon što je korisnik obaviješten o vrstama podataka i trajanju obrade u svrhu promidžbe (i prodaje) elektroničkih komunikacijskih usluga te u svrhu pružanja usluga s dodanom vrijednosti. Podaci se i u ovdje navedene svrhe smiju obrađivati samo na način i u *razdoblju potrebnom za* obavljanje tih radnji. Osim toga i ovdje vrijedi pravilo ograničenog pristupa podacima pa je tako pristup obradi dopušten isključivo ovlaštenim osobama operatora koje rade na navedenim poslovima. Također, pristup obradi mora se ograničiti na najnužnije radnje u vezi s obavljanjem tih poslova.

5.6.4. Obrada podataka o lokaciji bez prometnih podataka

Prema definiciji u čl. 2. Zakona o elektroničkim komunikacijama podaci o lokaciji označavaju bilo koje podatke obrađene u elektroničkoj komunikacijskoj mreži ili putem elektroničke komunikacijske usluge, koji označavaju zemljopisni položaj terminalne opreme korisnika javno dostupne elektroničke komunikacijske usluge.

Ti se podaci mogu odnositi na geografsku širinu, duljinu i visinu korisnikove terminalne opreme (kao što je to, na primjer, mobilni uređaj), smjer putovanja, razinu preciznosti informacije o lokaciji, identifikaciju mrežne ćelije u kojoj je terminalna oprema smještena u određenom trenutku u vremenu, kao i na vrijeme kada je podatak o lokaciji zabilježen.

U pravilu se podaci o lokaciji obrađuju zajedno s prometnim podacima kako bi se realizirao prijenos komunikacije (kao i obračun troškova komunikacije). U digitalnim će mobilnim mrežama tako, na primjer, podatak o zemljopisnom položaju terminalne opreme korisnika, kao što je to mobilni uređaj, biti obrađivan kako bi se komunikacija mogla prenijeti između pozivatelja i pozvane strane.[130] Gledano iz aspekta propisa o zaštiti podataka u elektroničkim komunikacijama, u navedenim će se slučajevima podaci o lokaciji smatrati prometnim podacima, te će se i na njih primjenjivati posebno propisana pravila o dopuštenom prikupljanju i daljnjoj obradi prometnih podataka u pojedine svrhe, kao i o njihovoj zaštiti. No s druge su se strane, uslijed tehnološkog razvoja te u kontekstu sve rasprostranjenijeg korištenja mobilnih komunikacijskih mreža javila i određena posebna pitanja prikupljanja i daljnje obrade podataka koji se tiču lokacije korisnika mobilnih uređaja. Tako je već u *Preporuci Vijeća Europe br. R (95) 4 o zaštiti osobnih podataka u području telekomunikacijskih usluga, s posebnim osvrtom na telefonske usluge* iz 1995. g. izražena potreba da se podaci o lokaciji korisnika mobilnih uređaja koji se bilježe radi obračuna i naplate troškova komunikacije, ne bi smjeli koristiti radi praćenja kretanja korisnika uređaja i utvrđivanja njihovih identiteta, kao niti radi utvrđivanja identiteta osoba s kojima oni komuniciraju. Sukladno tome u Preporuci se utvrđuje načelo, prema kojem bi se sustav naplate troškova korištenja mobilnih uređaja trebao temeljiti na podacima o lokaciji koji nisu toliko precizni da bi se na temelju njih mogla utvrditi točna lokacija i pretplatnika i pozivanih osoba u trenutku korištenja uređaja. S time je u vezi primjenjivo posebno pravilo, prema kojem je dopuštena obrada podataka o lokaciji bez prometnih podataka, ako je to potrebno da bi se omogućilo pružanje usluga s dodanom vrijednosti.

Temeljno je pravilo u našem zakonu (čl. 104.) da se podaci o lokaciji bez prometnih podataka, koji se odnose na pretplatnike ili korisnike javnih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga, smiju obrađivati samo ako su anonimizirani (učinjeni

[130] Uvodne izjave br. 14., 15. i 35. Direktive o e-privatnosti.

neimenovanima), a u suprotnom samo na temelju prethodne privole pretplatnika ili korisnika usluga.

Kada se, naime, podaci o lokaciji bez prometnih podataka obrađuju u neanonimiziranom obliku, a izvan opsega koji je nužan za prijenos komunikacije ili za obračun i naplatu troškova prijenosa komunikacije, podrazumijeva se da se oni obrađuju radi pružanja *usluga s dodanom vrijednosti*, što se dopušta samo uz prethodnu privolu pretplatnika odnosno korisnika koji je takvu uslugu zatražio. Prije pribavljanja privole obvezno je obavještavanje pretplatnika ili korisnika usluga, o vrsti podataka o lokaciji bez prometnih podataka, koji će se obrađivati, o svrhama i trajanju obrade, kao i o tome hoće li ti podaci biti dostavljeni trećoj strani radi pružanja usluge s dodanom vrijednosti. Pretplatniku ili korisniku usluga treba se u svako doba *omogućiti da uskrati* svoju privolu za obradu podataka o lokaciji bez prometnih podataka radi pružanja navedene usluge. Pretplatniku i korisniku usluga mora se *i nakon što je pribavljena privola omogućiti privremeno odbijanja obrade* tih podataka. To se korisniku mora omogućiti na jednostavan i besplatan način, a to prilikom svakog priključivanja na elektroničku komunikacijsku mrežu ili prilikom svakog prijenosa komunikacije.

Prikupljeni i dalje obrađivani podaci o lokaciji bez prometnih podataka također se moraju zaštiti od svake neovlaštene obrade. U tom je smislu nužno poduzimati potrebne zaštitne mjere, kako bi se poštovalo pravilo da je obrada dopuštena samo ovlaštenim osobama operatora javnih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga, odnosno ovlaštenim osobama treće strane koja pruža usluge s dodanom vrijednosti. Osim toga, obrada tih podataka mora se ograničiti na najnužnije radnje u vezi s pružanjem navedenih usluga.

Određene posebne okolnosti opravdavaju potrebu obrade podataka o lokaciji bez prometnih podataka i kada za to nema privole pretplatnika i korisnika usluga, ili ako su isti privremeno odbili obradu ovih podataka. To će svakako biti potrebno kako bi se omogućilo nadležnim državnim tijelima i hitnoj službi, da se odazovu na pozive u hitnim slučajevima. U Zakonu o elektroničkim komunikacijama se, prema tome, u navedenu svrhu propisuje obveza *operatora javno dostupnih telefonskih usluga* da onemoguće privremeno odbijanje ili izostanak spomenute privole i to za svaki pozivni broj nadležnih državnih tijela i hitnih službi, u skladu s njihovim pisanim zahtjevom (čl. 106.).

U drugu propisanu iznimku spadaju posebni slučajevi kada operatori javnih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga (kao i pravne i fizičke osobe, koje na temelju posebnih propisa obavljaju djelatnost elektroničkih komunikacijskih mreža i usluga na području RH) moraju ispunjavati propisane obveze prema operativno-tehničkom tijelu nadležnom za nadzor elektroničkih komunikacija i prema tijelima koja su ovlaštena za primjenu mjera tajnog nadzora elektroničkih komunikacijskih mreža i usluga, u skladu s posebnim zakonima iz područja nacionalne sigurnosti i kaznenog postupka (čl. 108. st. 4.).

5.6.5. Obvezno zadržavanje podataka u elektroničkim komunikacijama

Zahtjevi nadležnih tijela da se uvede obveza prikupljanja i pohrane podataka o elektroničkim komunikacijama radi učinkovitije borbe protiv kriminala i zaštite nacionalne sigurnosti osobito su postali izraženi nakon terorističkih napada u SAD-u i Europi početkom prošlog desetljeća. Uskoro nakon toga u pojedinim državama EU-a uslijedile su zakonodavne aktivnosti usmjerene na propisivanje mjera obveznog zadržavanja podataka u elektroničkim komunikacijama.
Potreba usklađivanja takvih mjera na razini prava EU-a dovela je do usvajanja *Direktive 2006/24/EZ o zadržavanju podataka generiranih ili obrađenih u vezi s pružanjem javno*

dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža (dalje u tekstu: Direktiva o zadržavanju podataka).[131] Obvezno zadržavanje podataka, budući da podrazumijeva praćenje i pohranu za dulji rok podataka koji se odnose na korištenje elektroničkih komunikacijskih usluga svih pretplatnika i korisnika usluga (bez obzira na sumnju u počinjenje relevantnih kaznenih djela), već samo po sebi predstavlja vrlo invazivno zadiranje u njihova temeljna prava i slobode te otvara brojna pitanja o mogućim zlouporabama. Tijekom godina provedba Direktive o zadržavanju podataka nailazila je na niz prepreka u pojedinim državama članicama EU-a, a Sud EU-a je istu proglasio 2014. g. nevaljanom te ona danas više nije na snazi.[132] Iako preventivno obvezno zadržavanje podataka, kada je riječ o cilju borbe protiv teških kaznenih djela, nije zabranjeno *per se*, kada je riječ o pravu EU-a, to se područje mora temeljito i vrlo pažljivo urediti propisima odgovarajuće kvalitete te osigurati jamstva odgovarajućih zaštitnih mjera kako bi se izbjegle (brojne) mogućnosti zlouporaba tih osjetljivih podataka pretplatnika i korisnika elektroničkih komunikacijskih usluga.[133]

Obvezno zadržavanje podataka u elektroničkim komunikacijama za rok od dvanaest mjeseci u domaćem je pravu uređeno *Zakonom o elektroničkim komunikacijama* (čl. 109. – 110.), odnosno za rok od godine dana *Zakonom o sigurnosno-obavještajnom sustavu Republike Hrvatske* (NN br. 79/2006 i 105/2006), te *Uredbom Vlade RH o obvezama iz područja nacionalne sigurnosti Republike Hrvatske za pravne i fizičke osobe u telekomunikacijama* (NN br. 64/08 i 76/13).

Utvrđena je svrha zadržavanja prema Zakonu o elektroničkim komunikacijama omogućavanje provedbe istrage, otkrivanja i kaznenog progona kaznenih djela u skladu s posebnim zakonom iz područja kaznenog postupka te u svrhu zaštite obrane i nacionalne sigurnosti u skladu s posebnim zakonima iz područja obrane i nacionalne sigurnosti. Zadržavaju se podaci potrebni za: 1) praćenje i utvrđivanje izvora komunikacije, 2) utvrđivanje odredišta komunikacije, 3) utvrđivanje nadnevka, vremena i trajanja komunikacije, 4) utvrđivanje vrste komunikacije, 5) utvrđivanje korisničke komunikacijske opreme, te 6) utvrđivanje lokacije pokretne komunikacijske opreme. Zabranjeno je zadržavanje podataka koji otkrivaju sadržaj komunikacije.

Izmjenama i dopunama Zakona o elektroničkim komunikacijama 2017. g. (NN br. 72/17) uklonjeno je ranije pozivanje na Direktivu o zadržavanju podataka kao osnovu za implementaciju pojedinih odredbi o zadržavanju podataka u taj zakon, s time da je većina tako propisanih pravila ostala na snazi, uz pozivanje isključivo na gore navedeni domaći okvir kao osnovu za zadržavanje podataka.[134]

---

[131] SL L 105, 13.4.2006., str. 54 – 63.

[132] Spojeni predmeti C–293/12 i C–594/12, Digital Rights Ireland Ltd protiv Minister for Communications , Marine and Natural Resources i dr. i Kärntner Landesregierung i dr., EU:C:2014:238. Za pregled u domaćoj literaturi vidi Gumzej, Nina, Izazovi digitalnog okruženja za privatnost i sigurnost osobnih podataka, Zbornik radova DIT 2014, https://bib.irb.hr/datoteka/721522.NGumzej.pdf, str. 719-720.

[133] Detaljnije vidi u presudi Suda EU-a, *ibid*, te kasnijoj presudi u spojenim predmetima C-203/15 i C-698/15, Tele2 Sverige AB i dr. protiv Post- och telestyrelsen i dr., EU:C:2016:970.

[134] U domaćoj se literaturi i prije ukidanja Direktive i kasnije presude Suda EU-a u predmetima C-203/15 i C-698/15 ukazivalo na potrebu temeljitog preispitivanja domaćih odredbi o zadržavanju, osobito vodeći računa o osiguravanju primjene načela nužnosti i razmjernosti, tj. nužnih jamstava zaštite relevantnih temeljnih prava svih korisnika usluga – građana RH. Vidi: Dragičević, Dražen, Gumzej, Nina, Obvezno zadržavanje podataka i privatnost, Zbornik Pravnog fakulteta u Zagrebu, 64, 2014., 1, str. 39-79.

5.6.6. Pohrana i pristupanje podacima u terminalnoj opremi

Iako se smatra da terminalna oprema (kao što je to, na primjer, tvrdi disk osobnog računala) korisnika elektroničke komunikacijske mreže odnosno u njoj pohranjene informacije pripadaju korisniku i čine dio njegovog privatnog života, oni mogu biti kompromitirani na način da, na primjer, treći bez znanja i privole pristupaju terminalnoj opremi kojom se on služi kako bi pohranili određene informacije, odnosno pristupaju podacima koji su u njoj pohranjeni. Navedene se informacije, naime, odnose na tu osobu i one mogu biti i osjetljive, privatne prirode. Štetne posljedice nedopuštenih aktivnosti trećih nad terminalnom opremom korisnika i njihovim podacima osobito su prisutne kod različitih malicioznih virusa i softvera koji omogućavaju tajni nadzor radnji korisnika terminalne opreme i kontrolu nad radom te opreme, poput *spywarea*. Opisane aktivnosti trećih predstavljale bi oblike zadiranja u privatan život korisnika kojima se osobito narušava tajnost elektroničkih komunikacija i pripadajućih prometnih podataka, a koja se jamči pretplatnicima i korisnicima javno dostupnih elektroničkih komunikacijskih usluga.[135] Osim u vezi s navedenim potrebama zaštite od djelovanja zlonamjernih i štetnih programa, ta se pitanja posljednjih godina osobito sagledavaju u kontekstu prakse instalacije kolačića te sličnih uređaja i tehnologija[136] u terminalnoj opremi, te nastavnog prikupljanja i daljnje obrade informacija koje se odnose na korisnika (i koje su sadržane u npr. već pohranjenim kolačićima). Često se ovdje radi o postupcima koji su nužni iz sigurnosnih i autentikacijskih razloga, odnosno kako bi se korisniku mogle pružiti pojedine *online* usluge (usluge informacijskog društva) koje je on izričito zatražio. No danas su u tom kontekstu osobito na razini prava EU-a posebno aktualna pitanja u vezi s poduzimanjem *online* ciljanog ili bihevioralnog oglašavanja, tj. praćenja ponašanja na mreži radi poduzimanja ciljanih oglašivačkih aktivnosti, u pogledu čega su poglavito prisutne zamjerke da se prema korisnicima ne provodi transparentno.

Kod posljednje je izmjene Direktive o e-privatnosti prepoznata potreba da se osigura jednako visoka razina zaštita osoba bez obzira dohvaćaju li se štetni programi nenamjerno putem elektroničkih komunikacijskih mreža, ili se oni dostavljaju i instaliraju putem softvera koji se nalaze na vanjskim medijima za pohranu podataka. Stoga se utvrdila obveza obavještavanja i traženja privola pretplatnika i korisnika usluga u slučaju svakog pristupa terminalnoj opremi radi pohrane podataka ili pristupa podacima, neovisno o tome ostvaruje li se taj pristup ili pohrana u okviru korištenja elektroničke komunikacijske mreže. Zakon o elektroničkim komunikacijama trenutno ne slijedi takav pristup.[137] Tako se prema pravilu u zakonu *korištenje elektroničkih komunikacijskih mreža za pohranu podataka ili za pristup već pohranjenim podacima u terminalnoj opremi* pretplatnika ili korisnika usluga dopušta samo u slučaju kada je taj pretplatnik ili korisnik usluga *dao svoju privolu, nakon što je dobio jasnu i potpunu obavijest u skladu s posebnim propisima o zaštiti osobnih podataka*, i to osobito o svrhama obrade podataka. Time se ne može spriječiti *tehnička pohrana podataka* ili pristup podacima *isključivo u svrhu obavljanja prijenosa komunikacija* putem elektroničke komunikacijske mreže, ili, *ako je to nužno, radi pružanja usluga informacijskog društva na izričit zahtjev pretplatnika ili korisnika usluga*.

5.6.7. Sigurnost i cjelovitost elektroničkih komunikacijskih mreža i usluga

U Zakonu o elektroničkim komunikacijama se propisuju važna pravila u svrhu *zaštite sigurnosti i cjelovitosti elektroničkih komunikacijskih mreža i usluga* (čl. 99.), koja u velikoj mjeri sadrže rješenja važećeg regulatornog okvira EU-a za područje elektroničkih komunikacija.

[135] Uvodne izjave br. 24.-26. Direktive o e-privatnosti i uvodne izjave br. 65.-66. Direktive 2009/136/EZ o pravima građana, SL L 337, 18.12.2009., str. 11 – 36.

[136] Npr. tehnologija digitalnog otiska prsta uređaja. RS29, Opinion 9/2014 on application of Directive 2002/58/ EC to device fingerprinting, 14/EN WP 224, 25.11.2014.

[137] Gumzej, N., Grgić, S., ePrivacy rules and data processing in users' terminal equipment: a Croatian experience, MIPRO Proceedings, 20-24.5.2013. Opatija, 2013., str. 1501-1507.

Posebne obveze operatora javnih komunikacijskih usluga radi zaštite sigurnosti i cjelovitosti elektroničkih komunikacijskih mreža i usluga uključuju primjenu odgovarajućih tehničkih i ustrojstvenih mjera kako bi se zaštitila sigurnost njihovih usluga kao i obvezu poduzimanja potrebnih mjera radi zaštite sigurnosti elektroničke komunikacijske mreže i usluga (zajedno s operatorima javnih komunikacijskih mreža).

Navedenim se mjerama mora osigurati razina sigurnosti koja odgovara postojećoj razini opasnosti za sigurnost mreže, vodeći pritom računa o raspoloživim tehničkim i tehnološkim rješenjima i troškovima tih mjera. Mjere se osobito provode kako bi se *spriječio i umanjio utjecaj sigurnosnih incidenata na korisnike usluga i međupovezane elektroničke komunikacijske mreže*. Njima se osobito mora osigurati to da *osobnim podacima mogu pristupati samo ovlaštene osobe u zakonom dopuštene svrhe kao i to da se preneseni ili pohranjeni osobni podaci zaštite od slučajnog ili nezakonitog uništenja, slučajnog gubitka ili izmjene te neovlaštene ili nezakonite pohrane, obrade, pristupa ili razotkrivanja, a mora se osigurati i primjena sigurnosne politike u odnosu na obradu osobnih podataka*. Potonja mjera provedbe sigurnosne politike potrebna je radi utvrđivanja ranjivosti u sustavu, a redovito bi se trebale provoditi i nadzorne, preventivne te korektivne aktivnosti kao i radnje radi ublažavanja štetnih posljedica, odnosno rizika.[138]

Operatori javnih komunikacijskih mreža također su dužni poduzimati sve odgovarajuće mjere kako bi zajamčili cjelovitost svojih mreža u svrhu osiguravanja neprekinutog obavljanja usluga koje se pružaju putem tih mreža. Pored navedenog, operator javno dostupnih elektroničkih komunikacijskih usluga mora obavijestiti korisnike svojih usluga u slučaju osobite opasnosti za sigurnost mreže, a ako je opasnost izvan opsega mjera koje operator poduzima, mora obavijestiti korisnike i o raspoloživim mjerama za uklanjanje opasnosti i/ili njezinih posljedica, uključujući naznaku mogućih troškova takvih mjera. U slučaju povrede sigurnosti ili gubitka cjelovitosti od značajnog utjecaja na rad njihovih mreža ili obavljanje njihovih usluga operatori javnih komunikacijskih mreža i operatori javno dostupnih elektroničkih komunikacijskih usluga moraju o tome bez odgode izvijestiti HAKOM pisanim putem. HAKOM može obavijestiti javnost ili zahtijevati od operatora da obavijeste javnost o takvoj povredi sigurnosti ili gubitku cjelovitosti ako utvrdi da je takva obavijest u javnom interesu.

Operator javno dostupnih elektroničkih komunikacijskih usluga mora odrediti odgovornu osobu za provedbu ovdje izloženih mjera. Ovlaštena tijela za nadzor mjera koje operatori poduzimaju radi provedbe navedenih obveza kao i za davanje preporuke o najboljoj praksi u vezi s razinom sigurnosti koju te mjere moraju ostvariti su HAKOM i AZOP. Način i rokovi u kojima operatori javnih komunikacijskih mreža moraju poduzimati odgovarajuće mjere kako bi zajamčili cjelovitost svojih mreža te način izvješćivanja HAKOM-a o povredi sigurnosti ili gubitku cjelovitosti od značajnog utjecaja na rad njihovih mreža ili obavljanje njihovih usluga detaljno su uređeni *Pravilnikom o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga* (NN br. 109/12, 33/13, 126/131 i 67/16).

Kako je ranije pojašnjeno, Opća uredba o zaštiti podataka uređuje po prvi puta na razini općeg pravnog okvira zaštite podataka EU-a postupke u slučaju *povreda osobnih podataka*. Postupci povodom tih povreda do tada su bili uređeni samo Direktivom o e-privatnosti i Uredbom Komisije br. 611/2013 o mjerama koje se primjenjuju na obavješćivanje o povredama osobnih podataka u skladu s

[138] Uvodna izjava br. 57. Direktive 2009/136/EZ o pravima građana.

Direktivom 2002/58/EZ[139], a u Hrvatskoj su propisani Zakonom o elektroničkim komunikacijama (čl. 99a – Povreda osobnih podataka u elektroničkim komunikacijama).

5.6.8. Odnos Direktive o e-privatnosti i Opće uredbe: aktualnosti

Uredbom se ne propisuju dodatne obveze fizičkim ili pravnim osobama u pogledu obrade u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga u javnim komunikacijskim mrežama u EU-u povezane s pitanjima u pogledu kojih vrijede posebne obveze s istim ciljem iz Direktive o e-privatnosti. Prema tome, Uredba bi se trebala primjenjivati na sva pitanja u vezi sa zaštitom temeljnih prava i sloboda u odnosu na obradu osobnih podataka koja ne podliježu posebnim obvezama s istim ciljem koji je utvrđen Direktivom o e-privatnosti, uključujući obveze voditelja obrade i prava pojedinaca. Kako bi se pojasnio odnos između Uredbe i Direktive i osigurala usklađenost s Uredbom, tu je Direktivu trebalo izmijeniti na odgovarajući način nakon donošenja Uredbe (čl. 95. i uvodna izjava br. 173. Uredbe). Akt kojim će se zamijeniti Direktiva o e-privatnosti (*prijedlog Uredbe o privatnosti i elektroničkim komunikacijama*) trenutno je u zakonodavnom postupku.[140]

5.7. Privatnost i kriptografija

Kriptografske metode danas su nezamjenjivo sredstvo zaštite podataka bez obzira na to nalaze li se oni pohranjeni unutar memorije računala, na nekom drugom mediju ili se prenose putem komunikacijskih kanala. Cilj je takvih metoda osigurati tajnost podataka kako njihov sadržaj ne bi bio dostupan neovlaštenim osobama. U uvjetima kad se komunikacija sve više odvija daljinski, ovakve su metode iznimno važne kako bi se zaštitila informacijska i komunikacijska privatnost građana i osigurala tajnost drugih povjerljivih podataka.

Riječ kriptografija potječe od grčkih riječi kripto (skriveno) i graphein (pisanje), a znači sustavno razmještanje ili zamjenjivanje znakova nekog zapisa ili poruke kako bi se očuvala njihova tajnost od onih kojima unaprijed generiran ključ za dešifriranje (dekriptiranje) nije namijenjen. Iako se često poistovjećuju kriptografija s kriptologijom i kriptoanalizom, one nisu sinonimi. Kriptologija (grčki kryptos »skrivena« i logos »riječ«) znanost je o sigurnoj (najčešće tajnoj) komunikaciji,[141]a obuhvaća već spomenutu kriptografiju i kriptoanalizu (grčki kryptos i analyein »otvoriti«) koja je znanost o ponovnom dobivanju informacija iz njihovog kriptiranog oblika. Drugim riječima to je znanost o dešifriranju (dekripciji) prethodno šifriranih (enkriptiranih) poruka. Kriptografijom se koristi od najstarijih vremena, pa se tako prve kriptografske metode razvijaju još u antičkom dobu. Kasnije se ona često koristila za očuvanje tajnosti vojne i diplomatske komunikacije. No, sve do kraja 19. stoljeća kriptografske metode nemaju širu primjenu. Tada dolazi do niza otkrića koja su omogućila njezin daljnji razvoj i širenje, a obilježila su početak jednog razdoblja poznatog pod nazivom druga informacijska

[139] SL L 173, 26. 6. 2013., str. 2–8.; izdanje na hrvatskom jeziku: 13/Sv. 66, str. 159-165.

[140]Prijedlog Uredbe Europskog parlamenta i Vijeća o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama), COM(2017) 10 final, 2017/0003 (COD).

[141] Encyclopedia Britanica, CD izdanje, 2009.

revolucija. Daljnji poticaj razvoju kriptografije uslijedio je sredinom prošlog stoljeća, točnije za vrijeme II. svjetskog rata, kada uslijed naglog razvoja informatičke tehnologije dolazi do pojave prvih namjenskih elektroničkih računala kojim su se koristili za dekodiranje (kriptoanalizu) telegrafskog prometa.[142] Nesumnjivo je da su oni odigrali vrlo važnu ulogu u II. svjetskom ratu, i u znatnoj mjeri pridonijeli njegovu bržem završetku. Međutim, tek razvojem računalnih mreža, daljinskog rada i posebno interneta, kriptografija postaje opće prihvaćena i široko rasprostranjena. Naime, sve do tada njezina je primjena bila ograničena i u pogledu onih koji su je razvijali, onih koji su je koristili i u pogledu razloga zbog kojih je korištena. Širenjem interneta, a s njim i broja zloupotreba, pitanje sigurnosti komuniciranja poprimilo je potpuno novi sadržaj, što je dovelo do razvoja novih kriptografskih metoda i alata. Takvi programi više nisu isključivo namijenjeni poslovnom korištenju, već se sve više razvijaju jednostavni i učinkoviti programi namijenjeni zaštiti osobnog komuniciranja i razmjeni podataka među građanima.

Danas, kad se prijenos sve više obavlja putem javne mreže, kriptografijom se koristi za kodiranje (enkripciju, šifriranje) podataka uz pomoć algoritama za enkripciju s namjerom da se tajno i sigurno prenesu komunikacijskim kanalom do primatelja. Algoritmi za enkripciju koriste se »ključevima« u obliku binarnih brojeva, najčešće dužine od 40, 128 ili više bitova. Uz pomoć toga ključa podaci u binarnom obliku kombiniraju se s njegovim bitovima prema određenom matematičkom ključu, što rezultira dobivanjem šifrirane poruke koju je moguće slati putem javne mreže. Djelotvornost kriptografije ovisi o algoritmu (pravila koja specificiraju metodu kriptiranja) kojim se koristi i dužini ključa. Sam postupak kodiranja (enkripcije) može se provesti softverski (primjenom nekih od kompjutorskih programa na kompjutoru opće namjene) ili hardverski (primjenom namjenskih uređaja). Prednost prvog je cijena, jer se do takvih programa može doći i besplatno, te fleksibilnost, dok je prednost hardverske enkripcije ide brzina koja može biti veća od 10 do čak 100 puta.

Kriptografske sustave moguće je klasificirati: 1) prema matematičkim operacijama putem kojih se izvorna poruka (tzv. plaintext) skriva primjenom enkripcijskog ključa. S obzirom na to, razlikuju se: sustav transpozicije (premještanja), sustav supstitucije (zamjene) ili njihova kombinacija; i 2) ovisno o tome koriste li se pošiljatelj i primatelj poruke istim ključem (simetrični kripto-sustav) ili različitim ključevima (asimetrični kripto-sustav).

U prvom slučaju, pri sustavu transpozicije, znakovi se razmještaju unutar poruke po određenom ključu, ali pritom ne mijenjaju svoj oblik, odnosno značenje, dok se kod sustava supstitucije, znakovi zamjenjuju drugim znakovima ili simbolima, također prema određenom ključu. Moguća je i kombinacija ovih dvaju sustava odnosno metoda. Druga podjela polazi od toga koriste li se primatelj i pošiljatelj za enkripciju i dekripciju istim kriptografskim ključem ili ne. Objasnit ćemo to na primjeru dva kriptografska algoritma koji se danas najčešće primjenjuju. Stariji, tzv. simetrični algoritam, koristi se tajnim ključem koji posjeduju i primatelj i pošiljatelj. Takav je DES algoritam koji se najčešće koristi 56-bitnim ključem.[143] Ova je

[142] Colosus je namjenski elektronički digitalni kompjutor razvijen u tajnosti 1943. godine u Post Office Research Laboratories u Londonu pod vodstvom dr. Tommy Flowersa. Koristio se u britanskim vladinim uredima u Bletchley Parku za dekodiranje njemačkog telegrafskog prometa. Nakon što su Nijemci razvili stroj za šifriranje pod nazivom Enigma Britanci su uz pomoć Colossusa uspješno dešifrirali njihove tajne poruke. Nakon prvog modela koji se sastojao od 1500 vakuumskih cijevi razvijen je i drugi pod nazivom Mark II 1944. godine sa 2500 vakumskih cijevi. Ovaj kompjutor nije bilo moguće reprogramirati.

[143] »DES (engl. skra Data Encryption Standard) je standard šifriranje podataka razvijen u IBM-u i odobren od Nacionalnog ureda za standardizaciju SAD 1977. godine. Koristi se 56-bitnim ključem za enkripciju i koristi

metoda najbrža, ali je prijenos tajnog ključa nesiguran. Iako se u početku tvrdilo da se ovaj algoritam ne može probiti, radi čega je bio vrlo rasprostranjen posebno u bankarstvu, već devedesetih pokazalo se da to nije točno. Prvi put učinjeno je to 1993. uz pomoć tehnike zvane »linearna kriptoanaliza« za što je bilo potrebno oko 50 dana na samo jednoj radnoj stanici, a drugi put 1997. za nešto manje od mjesec dana, pri čemu je korišteno više od 14.000 kompjutora.[144] Zbog nesigurnosti, danas je DES velikim dijelom zamijenjen algoritmom Advanced Encryption Standard (AES).

Drugi, tzv. asimetrični algoritam ili metoda javnog ključa upotrebljava dva različita ključa: tajni (privatni) i javni ključ. Takav je RSA algoritam, koji su 1976. razvili Rivest, Shamir i Adelman. Dok je privatni ključ tajan i ima ga samo primatelj, javni ključ je dostupan svima pa se tako njime mogu koristiti svi jer je putem interneta (ili na drugi način) do njega jednostavno doći. Pošiljatelj se u tom slučaju koristi javnim ključem kako bi šifrirao (zaštitio) podatke koje je moguće dešifrirati samo uz pomoć tajnog ključa, koji posjeduje samo primatelj. Iako sporija, ova je metoda daleko sigurnija jer vlasnik privatnog ključa ne mora nikome slati svoj tajni ključ, budući da se njime koristi samo on (za dešifriranje). Prednost je ove metode u odnosu na prethodnu što se koristi različitim ključevima za enkripciju i dekripciju, koji mogu biti različite dužine. Posebno visok stupanj sigurnosti predstavlja 512-bitni ključ, za čije bi probijanje na najsuvremenijim i najsnažnijim kompjutorima po nekim procjenama trebalo tisuće godina. No, ova je metoda daleko sporija od prethodne. Ove dvije metode moguće je i kombinirati i to na način da se metodom javnog ključa koristi samo za prijenos tajnog ključa, dok se za prijenos podataka koristi metodom tajnog ključa.

Razvoj kriptografije doveo je do pojave brojnih kriptografskih programa, koji više ili manje, osiguravaju nesmetanu i tajnu komunikaciju među korisnicima. Jedan od poznatijih, uz to i besplatan (fteeware), bio je PGP (engl. Pretty Good Privacy), američke tvrtke Pretty Good Privacy Inc. Razvio ga je amerikanac Phil Zimmerman, čiji su problemi s vlastima, zbog zakonskih ograničenja u pogledu izvoza kriptografskih programa, javnosti dobro poznati. Naime, protiv njega je u SAD-u podignuta optužnica, zato što kriptografski proizvodi u SAD-u imaju status jednak nuklearnom oružju, a njihovo stavljanje na raspolaganje potencijalnim korisnicima izvan zemlje tretira se kao izvoz vojne tehnologije. Za enkripciju se koristi RSA kriptografskom metodom. Premda je tako zaštićene podatke moguće dešifrirati (dekodirati), ovaj program ipak pruža odgovarajući stupanj zaštite korisniku.

Razvoj alata koji omogućavaju tajnu komunikaciju nastavljen je i na području mobilne telefonije ponudom i sve širom primjenom pametnih telefona, mobilnih aplikacija i internetskih servisa koji omogućavaju kriptiranu komunikaciju (npr. servis Skype, ili mobilne aplikacije RedPhone ili Telegram).

U uvjetima kada se komunikacija sve više odvija elektroničkim putem, a usluge poput internetskog bankarstva i trgovine postaju našom svakodnevicom, kriptografija postaje nezamjenjiva i zasigurno ako ne najvažnija, onda jedna od najvažnijih metoda zaštite, posebno

---

tzv. blok čiper metodu kojom razbija tekst u 64 bloka prije enkripcije. Budući da ovaj algoritam nikada nije postao općim standardom za šifriranje, jer ga je 1986. godine Nacionalna agencija za sigurnost SAD proglasila nesigurnim, pravilniji bi naziv bio Data Encryption Algorithm (DEA). Unatoč tome, još se uvijek nalazi u upotrebi širom svijeta. Sigurniju kriptografsku metodu predstavlja RSA.« – A. i D. Dragičević, Leksikon ekonomije i informatike, Informator,
Zagreb, 1999.

[144] Probijen DES algoritam, Večernji list, 30. lipnja 1997., str. 39.

kada su u pitanju financijske transakcije te osobna i poslovna komunikacija. U nastavku ćemo se osvrnuti na neke metode koje se temelje ili koji se koriste u kombinaciji s kriptografijom. Zbog svoje važnosti i uloge koju imaju danas, a imat će zasigurno i u budućnosti, zaslužuju da ih se posebno izdvoji. Odnosi se to na: steganografiju, digitalni certifikat, digitalni potpis i digitalni vremenski biljeg.

5.7.1. Steganografija

Steganografija (Steganography)[145] je umijeće i tehnologija skrivenog pisanja. Kao i pri kriptografiji cilj je očuvati tajnost komunikacije. U raznim oblicima koristi se već stoljećima.[146] Danas se ovom tehnologijom najčešće umeću podaci u neiskorištene dijelove informacijskog paketa koji se prenosi nekim komunikacijskim kanalom. Na taj se način podaci, bez obzira na to u kojem se obliku nalazili, kriju unutar naizgled bezazlenih poruka. Naime, podaci se putem računalne mreže prenose u paketima koji se sastoje od sadržaja (tekst, slika, zvuk), kontrolnog dijela i adresa primatelja i pošiljatelja. Određene su dužine i oblika te ako ne dođe do greške u prijenosu njihovim spajanjem na računalu primatelja, postaju mu dostupni za korištenje. Sam prijenos, sigurnost i kontrolu integriteta (cjelovitosti) podataka osiguravaju komunikacijski programi i protokoli.

Budući da u takvim paketima ima neiskorištenih bitova, unutar njih se mogu umetnuti podaci na osnovi kojih će primatelj dobiti neku tekstualnu, video ili audio poruku, ili pak provjeriti vjerodostojnost primljenih podataka ili identitet pošiljatelja. Postupak je sličan onom koji se primjenjuje pri zaštiti novca gdje se upotrebljava vodeni žig, umeću zlatne niti i sl., koji na prvi pogled nisu vidljivi korisniku. Takvo je npr. skrivanje teksta unutar slike. Iako nije u pitanju kriptografska metoda, vrlo je učinkovita kad se koristi u kombinaciji s nekom takvom metodom. Sama poruka, slika ili zvučna datoteka ne mora biti uopće zaštićena jer je pretpostavka da treće osobe ne sumnjaju da se u njima krije neki drugi sadržaj. Zato ona ne mora biti niti kriptirana. Postupak se, također, može primijeniti i na neiskorištenim dijelovima (sektorima) magnetskog diska ili diskete. Primjenom ove metode moguće je učinkovito sakriti i digitalni potpis.

5.7.2. Digitalni certifikat

Digitalni certifikat (digital certificate) je isprava u digitalnom obliku kojom se potvrđuje identitet neke pravne ili fizičke osobe. Izdaju ih za to ovlaštene organizacije (Certification

---

[145] Steganografija je umjetnost i znanost komuniciranja na način da se sakrije prisustvo takve komunikacije.« – Markus Kuhn, 1995. Tekst je dostupan na internetskoj adresi: www.thur.de/ulf/stegano/announce.html.

[146] »Jedan od prvih načina korištenja steganografije bilo je pisanje tintom koja bi bila nevidljiva sve dok se papir ne zagrije. Mikrotočka, dio filma koji sadrži vrlo visoko smanjenu sliku tajne poruke i umetnutu u znakove interpunkcije normalnog dokumenta, izumljena je tijekom drugog svjetskog rata. Šezdesetih je fotografija članova USS Pueblo izdana od strane njihovih otimača kako bi pokazali njihovu suradnju izgledala sasvim obično dok pažljivo ne pogledate položaj njihovih ruku. Znakovima su ispisali riječ 'SNOWJOB'. A svi se sjećamo histerije zbog otkrića sotonističkih poruka obrnutim puštanjem nekih snimki.« – Bruce T. Fraser, On cryptography and Privacy, School of Library and Information Studies, 1996.

Authority – CA) kao što su VeriSign i Mountain View. Sigurnost i povjerljivost podataka iz takve isprave osigurava se upotrebom asimetrične kriptografije pri čemu izdane isprave sadržavaju tajni ključ za dešifriranje, dok se ovjeravanje obavlja javnim ključem agencije koja ih je izdala. Na taj način nositelj takvih elektroničkih isprava potvrđuje svoj identitet i osigurava nesmetanu i sigurnu komunikaciju. Posebno je to važno u elektroničkom poslovanju gdje se na taj način osigurava plaćanje kreditnim karticama putem interneta. Pri prijenosu korisničkih imena, adresa i brojeva kreditnih kartica radi zaštite podataka koristi se sigurnosnim protokolom (npr. SSL – Secure Socket Layer ili SET – Secure Electronic Transaction) koji omogućava enkripciju i provjeru takvih digitalnih isprava.

5.7.3. Digitalni potpis

Digitalni potpis (Digital signature) je tehnologija provjere vjerodostojnosti poruka primljenih u komunikaciji koja se odvija između udaljenih kompjutora. Takav »potpis« nalazi se u digitalnom obliku i sastavni je dio šifrirane poruke koja se šalje, a sadrži izračunati zbroj same poruke. Budući da je gotovo nemoguće izmijeniti sadržaj teksta a da zbroj ostane isti, predstavlja vrlo siguran način provjere vjerodostojnosti samog teksta i sigurne komunikacije. Nakon što primatelj dešifrira primljenu poruku i digitalni potpis, sam provjerava zbroj takve poruke i uspoređuje s primljenim. Budući da digitalni potpis potvrđuje vjerodostojnost teksta koji se šalje odnosno prima, ali ne i identitet osobe koja ga šalje, često se koristi u kombinaciji s digitalnim certifikatom koji izdaje za to ovlaštena agencija. Svrha ove metode nije osigurati tajnost komunikacije pa se njome najčešće koristi u kombinaciji s kriptografskim metodama, uz pomoć kojih se može učinkovito zaštititi sam sadržaj podataka koji se razmjenjuju. Tehnologija digitalnog potpisa svoju primjenu nalazi na brojnim područjima koja se susreću s potrebom za takvom provjerom, a posebice u pravu. To je i razumljivo s obzirom na sve veći broj isprava u digitalnom obliku kojim se koriste u pravnom prometu.

5.7.4. Digitalni vremenski biljeg

Digitalnim vremenskim biljegom (Digital time stamping), koristi se za provjeru kada je digitalni dokument kreiran, odnosno posljednji put promijenjen, što je važno za utvrđivanje vjerodostojnosti dokumenta primljenih, odnosno poslanih putem mreže. Slično kao pri digitalnom potpisu koristi se kriptografijom za stvaranje jedinstvenog koda koji se zatim šalje primatelju. Primatelj tada uspoređuje primljeni kod s kodom do kojeg je došao sam korištenjem istim algoritmom.