PRAVNA REGULATIVA VEZANA UZ ZAŠTITU OSOBNIH PODATAKA

Martinelli, Marija

VELEUČILIŠTE U POŽEGI

STUDENT:Marija Martinelli, MBS:3698

PRAVNA REGULATIVA VEZANA UZ ZAŠTITU OSOBNIH PODATAKA

ZAVRŠNI RAD

Požega, 2016 godine.

VELEUČILIŠTE U POŽEGI

DRUŠTVENI ODJEL

PREDDIPLOMSKI STRUČNI STUDIJ

UPRAVNI STUDIJ

PRAVNA REGULATIVA VEZANA UZ ZAŠTITU OSOBNIH PODATAKA

ZAVRŠNI RAD

IZ KOLEGIJA INFORMATIKA II

MENTOR: mr.sc. Kristian Đokić

STUDENT: Marija Martinelli

Matični broj studenta: 3698

Požega 2016 godine.

SAŽETAK

Tema ovog rada je pravna regulativa vezana uz zaštitu osobnih podataka, njen nastanak i unapređivanje tijekom vremena donošenjem i uvrštavanjem pravila o vrstama i načinima postupanja s osobnim podatcima. Poseban naglasak daje se na suvremen način života i stalan tehnologijski napredak s kojim je društvo suočeno i mogućnostima određivanja i odjeljivanja osobnih podataka u svakodnevnom društvenom i poslovnom svijetu.

Digitalno doba koje donosi izuzetne mogućnosti i pogodnosti u pogledu brzine komunikacije, količina i brzina dostupnih informacija koje su važan i sastavni dio svakodnevnog života, uz sve blagodati koje donosi također zahtjeva osvrt i na opasnosti koje prijete iz tako velikih mogućnosti.

Je li uopće moguće zaštititi osobne podatke i privatnost koja je svakom čovjeku važna i zajamčena tko sve i na osnovu kojih prava ima mogućnosti uvida u osobne podatke, njima se koristiti i obrađivati ih. Kako se osigurava zaštita osobnih podataka, te koje su institucije nadležne za to i koliko je učinkovita njihova zaštita.

KLJUČNE RIJEČI: osobni podatak, prikupljanje podataka, zaštita podataka

ABSTRACT

The subject of this work is legal regulation related to personal data protection, its emergence and improvment over time, by enacting and introducing in applicable rules, based of types and ways of proceeding with personal data. Special emphasis is given to the modern way of life, permanent technological progress which society is faced with and the possibilities of determination and separation of personal data in everyday social and business world.

The digital age, which brings extraordinary possibilities and benefits in the field of communication speed, quantity and speed of available information which are eventful and integral part of everyday life, with all the benefits that it brings, still requires a retrospect to the risks threating from both great features.

Is it even possible to protect personal data and privacy, which are important and assured to every human being.Who can, and based on which law, access personal information, use them and process them. How is personal data secured, which institutions have the jurisdiction over it and how effective is their protection.

KEY WORDS:personal data, data collecting, data protection

SADRŽAJ

1. UVOD

Ovim radom će se promotriti nastajanje osobnih podataka te pravnih pravila kojima se nastoji takve podatke zaštititi kroz povijest i njihovo usklađivanje s tehnološkim i društvenim napretkom.

Cilj ovog rada je pokušati definirati što je osobni podatak, iz čega se može dobiti, tko sve i kojim pravom može prikupljati i obrađivati osobne podatke pojedinaca s naglaskom na suvremeni život i informacijsku tehnologiju. Jednako tako bit će dan pregled mjera zaštite kojima su osobni podatci zaštićeni od moguće zlouporabe.

Svaki pojedinac je nositelj osobnih podataka. Upoznavanjem sadržaja, vrste osobnih podataka i pravila kojima se štite omogućava se stjecanje svjesnosti pojedinaca o pravima, te potrebama i mogućnostima zaštite takvih podataka.

2. OSOBNI PODATAK

Na početku rada potrebno je definirati što sve mogu biti osobni podatci da bi se lakše moglo utvrditi na što se obrađene pravne norme odnose. Sve ono što se prije samo dvadesetak godina činilo kao znanstvena fantastika i o čemu su „sanjarili“ u serijama poput Zvjezdanih staza, danas čini normalan život čovjeka. Tadašnje strane riječi poput čipova, memorije, podatak, baza i nadzor, sastavni su dijelovi kako poslovnog, tako i privatnog života. Munjevit napredak znanosti i tehnologije osim što omogućava prikupljanje velikog broja podataka na svim poljima, omogućava i njihovu analizu i obradu, te čuvanje i naknadno korištenje prema potrebama. Kako je sve to povezano s osobnim podatcima, vidljivo je iz zakonske definicije osobnog podatka, gdje zakon kazuje da je osobni podatak „svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati (u daljnjem tekstu: ispitanik); osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet.“ Zakon o zaštiti osobnih podataka. (NN 103/03, 118/06, 41/08, 130/11, 106/12, čl.2., st- 1.)

Tu je sasvim jasno kako osobni podatak, da bi to stvarno i bio, mora imati svoju pripadnost nekome, a taj netko mora biti poznat, odnosno identificiran te nedvojbeno podatak mora pripadati njemu. Tako u Priručniku o europskom zakonodavstvu o zaštiti podataka (Vijeće Europe, 2014.) prepoznaju problematiku pravne definicije osobnih podataka promišljajući kada se osoba smatra identificiranom. Navodeći da identifikacija podrazumijeva elemente koji osobu opisuju na način koji je razlikuje od svih drugih osoba i prepoznaje kao pojedinca. Ime osobe prvi je primjer takvih elemenata opisa. Budući da mnoga imena nisu jedinstvena, za utvrđivanje identiteta osobe mogu biti potrebni dodatni identifikatori kako bi se osiguralo da se osoba ne zamijeni nekim drugim, pa se koriste datum i mjesto rođenja. U pojedinim su zemljama također uvedeni personalizirani brojevi poput OIB-a, kako bi se građani međusobno razlikovali. Osim toga, biometrijski podaci, kao što su otisci prstiju, digitalne fotografije ili skeniranja šarenice oka, sve su važniji za identificiranje osoba u tehnološko doba, jednako kao što se na osnovu posjedovanja nekih stvari, kao na primjer vozila snimljenog video nadzorom može utvrditi identitet, i prema javno dostupnim informacijama objavljenim u zemljišnim knjigama koje katastarske čestice vežu uz vlasnikovo ime, prezime i osobni broj.

Ukratko rečeno, sve ono što jesmo, što čitamo, radimo, kupujemo, koristimo, kuda idemo, s kim se družimo i komuniciramo bilo telefonski ili elektroničkim putem, sve može biti snimljeno i pohranjeno i u određenom trenutku identifikacijom može postati koristan, ili pak opasan osobni podatak, koji se na bilo koji način mora zaštititi od javnosti, ili od moguće zlouporabe.

2.1. Osjetljivi osobni podatci

Budući da se na osnovu prikupljenih osobnih podataka identificirane osobe dalje mogu raditi daljnja istraživanja i analize, neki su podatci, naravno iznimno u slučajevima predviđenim svim nacionalnim i međunarodnim normama, dodatno prošireno na iznimnu dozvolu ispitanika, te u slučaju kada je potrebno radi zaštite njegovog zdravlja ili života, zaštićeni od daljnjih obrada. Možda se svi i neće složiti s kategorijom osjetljivih podataka, jer netko bi radije zaštitio nekakve druge podatke, ali u tu kategoriju podataka prema Zakonu o zaštiti osobnih podataka pripadaju slijedeći podaci. “ Zabranjeno je prikupljanje i daljnja obrada osobnih podataka koji se odnose na rasno ili etničko podrijetlo, politička stajališta, vjerska ili druga uvjerenja, sindikalno članstvo, zdravlje ili spolni život i osobnih podataka o kaznenom i prekršajnom postupku.“Zakon o zaštiti osobnih podataka. (NN 103/03, 118/06, 41/08, 130/11, 106/12, čl.8.) izuzimajući situaciju kada je sam ispitanik objavio takve podatke, te postavljajući jasnu granicu povjerljivosti podataka i daljnjih korisnika ograničavajući se na nadležna tijela i svrhu u koju je podatak prikupljen.

Ovdje je jasno kako u pogledu osjetljivih podataka nedovoljnom pažnjom ispitanik može iznijeti u javnost dio takvih podataka, pogotovo u današnje vrijeme kada je dovoljan samo jedan *„like“* (sviđa mi se) na nekoj od društvenih stranica da ga poveže s nekom pripadnom skupinom ili rasom, a da on toga nije niti svjestan. Međutim, to ipak ne znači da će odmah biti stigmatiziran ili će uslijediti nekakva zlouporaba takvih podataka, ali u svakom slučaju ostavlja otvorene mogućnosti.

3. PRAVNA REGULATIVA VEZANA UZ ZAŠTITU OSOBNIH PODATAKA

Osobni podatci obuhvaćaju vrlo širok spektar informacija o pojedincima, fizičkim osobama i njihovom djelovanju i životu uopće. Ne samo da se odnose na klasične podatke o osobama poput imena prezimena, datuma rođenja, adrese stanovanja i nekakvim identifikacijskim brojevima, već se proteže na pripadnost koju pojedinci izražavaju prema nekakvim strankama, vjerskim zajednicama, istomišljenicima raznih tradicionalnih i suvremenih pokreta. Kako svaki takav podatak može potencijalno dovesti ili do osuđivanja na osnovi pripadnosti, ili se tim podatcima na bilo koji način pojedinac može dovesti u poziciju da budu ugrožena njegova osnovna ljudska prava, bilo je nužno takve podatke i zaštititi.

3.1. Pravne osnove za zaštitu osobnih podataka

Kao osnovna polaznica u zaštitit osobnih podataka pretpostavlja se Konvencija za zaštitu ljudskih prava i sloboda, koja svojim odredbama, osim nastojanja zaštite ljudskih života i osnovnih uvjeta za život pokušava unijeti i regulirati privatno vlasništvo pod svoje okrilje, te zaštititi privatnost čovjeka na osnovnoj razini navodeći da „Svatko ima pravo na poštovanje svoga privatnog i obiteljskog života, doma i dopisivanja.“ (Konvencija za zaštitu temeljnih ljudskih prava i sloboda, 1950. čl.8.1 st.1.)

Iako je odredba koja je omogućila početak zaštite osobnih podataka štura i ne govori puno, uglavnom iz osnovnog razloga što u ono vrijeme nije niti postojalo puno definiranih mogućih činjenica koje su mogle biti zaštićene, ipak do danas čini sasvim čvrst temelj za daljnju nadogradnju s obzirom na specifičnosti suvremenog načina života i opseg situacija i privatnih stvari. Napretkom društva i društvenog uređenja pojavljuje se sve više podataka koji zahtijevaju i normativnu regulativu, samim time i postaju podatak koji je nužno sačuvati, pohraniti i prema potrebi ponovno pronaći za nekakve nove poslove, pojavljuje se potreba za dodatno proširenje i detaljnije određivanje što su privatni podatci, tko ih prikuplja, kako ih arhivira i koristi te kako se štite takvi podatci. Tako se preko jednostavnijih proširivanja Konvencije njenim protokolima, novim ugovorima proizašlim iz proširenja Europske Unije pristupanjem novih članica nastoji uvesti univerzalno uređenje na cijelom području država članica koja će osigurati kako sigurnost građana i njihovih privatnih podataka, tako i mogućnost država da iste podatke razmijene i koriste razmjerno svojim potrebama i ovlastima u svrhu zaštite javnog dobra trećih osoba i privatnosti svih građana. Pojavom informacijske

tehnologije i informatizacije70-ih godina prošlog stoljeća i geometrijske progresije protoka podataka uključenih u suvremeni način života pojavljuje se potreba za novom zasebnom granom u pogledu zaštite osobnih podataka pojedinaca, budući da se unatoč donošenju brojnih rezolucija nije uspjelo dovoljno dobro osigurati potrebnu zaštitu na području privatnosti. Tako se 1981. otvara Konvencija Vijeća Europe o zaštiti pojedinaca pri automatskoj obradi osobnih podataka (Konvencija br. 108)Kao takva postaje jedini pravno obvezujući međunarodni akt zemalja potpisnica u području zaštite podataka i primjenjuje se na obradu osobnih podataka u privatnom i u javnom sektoru. Konvencija štiti pojedinca od zloporaba prilikom prikupljanja i obrade osobnih podataka nastojeći istodobno regulirati prekogranični prijenos osobnih podataka. (Priručnik o europskom zakonodavstvu 2014.)

U pogledu prikupljanja i obrade osobnih podataka, načela iz Konvencije osobitu pažnju posvećuju postupku pravednog i zakonitog prikupljanja i automatske obrade podataka pohranjenih u određene legitimne svrhe, koji nisu namijenjeni uporabi u drugim neprimjerenim svrhama, i koji se ne smiju zadržavati dulje no što je to potrebno. Načela Konvencije se osvrću i na kvalitetu podataka, te određuje kako svi podatci prvenstveno moraju biti prikladni, točni, relevantni i ne pretjerani, odnosno razmjerni. Osim propisanih postupaka i kvalitete prikupljenih podataka, Konvencija izričito zabranjuje obrade takozvanih „osjetljivih podataka“ u što su uvršteni rasa, političko opredjeljenje, zdravlje, vjera, seksualni život ili kaznena evidencija pojedinca, te im ujedno i osigurava pravo informiranosti o količini i vrsti prikupljenih podataka o njima. Unatoč odredbi o slobodnom prijenosu takvih prikupljenih podataka među članicama potpisnicama, određuju se i ograničenja vezana uz državnu sigurnost, obranu, te vrstu pravnog uređenja pojedine države.

Iako je osnovna Konvencija 108 izmijenjena 1999. iz razloga da se omogući Europskoj Uniji svojstvo stranke, budući se Konvencija odnosila samo na članice potpisnice, a sve veći zahtjevi za sigurnost i očuvanje mira potiče potrebu za suradnjom i sa zemljama nečlanicama, te prekograničnom protoku i razmjeni podataka, protokolom uz Konvenciju 108, omogućeno je zemljama nečlanicama, kao i neeuropskim zemljama sudjelovanje u zaštiti podataka, uz uvjet osnivanja nacionalnih tijela nadležnih za područje zaštite podataka.

Osim tih promjena, na temelju Konvencije donesena je Direktiva 95/46/EZkao temeljni pravni akt, na prostoru gospodarskih partnera kao preduvjet za slobodnu razmjenu roba i dobara kako između članica, tako i uključujući neke država nečlanice, ali od gospodarske važnosti. Tom Direktivom su dodatno proširena sadržana prava određena u Konvenciji, uz naglasak na primjenjivost prilikom usklađivanja s nacionalnim pravima zemalja pristupnica vezano uz zaštitu podataka, te Uredbom Europske Zajednice br. 45/2001,

budući je Europska Unija stekla pravo stranke, a za provođenje određenih postupaka u njezinim tijelima osigurano je na taj način sigurno postupanje podatcima kojima ona u svom radu raspolaže. (Priručnik o europskom zakonodavstvu 2014.)

Vidljivo je da vremenski periodi donošenja novih pravila postaju sve kraći uzrokovani brzinom napretka društva zbog informatizacije. Osim što donosi niz novih mogućnosti i prednosti u brzini i količini protoka informacija, donosi i niz novih zahtjeva za normiranje istih i usklađivanje uvrštavanjem u nacionalno pravo i u temeljne akte na globalnoj razini. Unatoč naporima da se donesenim direktivama urede gotovo svi poznati odnosi procvatom interneta današnji načini prikupljanja, obrade i arhiviranja osobnih podataka neprestano zahtijevaju prilagodbe te se svakim napretkom donose nove regulative poput Direktiva 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija kojom je detaljno razrađena regulativa osobnih podataka u sustavu telekomunikacijskih usluga putem javnih distribucijskih mreža, koje svoje usluge pružaju fizičkim i pravnim osobama. Tako (Direktiva 2002/58/EZ) u osnovama određuje da svaki pružatelj usluga mora omogućiti korisniku zaštititi svoje podatke i to bez naknade, te ga upozoriti o korištenju i vrsti korištenih njegovih osobnih podataka. Posebna pažnja je usmjerena na vidljivost broja pozivatelja, te mogućnosti da se taj broj ne prikazuje na zahtjev korisnika, ili s druge strane da korisnik ima mogućnost odbiti pozive koji za njega nisu poznati. Nadalje, uz klasični oblik zaštite sadržaja komunikacije, te lokacije poziva koje mogu biti prikupljene, i niza specifičnih situacija koje se događaju prilikom uspostavljanja komunikacije takvim načinom, naravno uz određena ograničenja predviđena u slučajevima razmjerne zaštite javnog reda i sigurnosti drugih osoba. Direktiva 2006/24/EZ o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža, svoje postojanje opravdava upravo činjenicama da su dosadašnjim postupcima štiteći prava pojedinaca otvorili prostor anonimnoj zlouporabi sveukupnog tehnologijskog napretka koji su u pitanje dovodili i nacionalne sigurnosti i druge osobe. Upravo iz tog razloga je odlučeno Direktivom 2006/24/EZ omogućiti zadržavanje odnosno pristupe pohranjenim podatcima nadležnim tijelima u svrhu kasnije obrade i otkrivanja povezanosti s kaznenim djelima.

Države članice donose mjere kako bi osigurale da se podaci zadržani u skladu s ovom Direktivom daju samo nadležnim nacionalnim tijelima u posebnim slučajevima te u skladu s nacionalnim pravom. Uzimajući u obzir odgovarajuće odredbe prava Europske unije ili međunarodnog javnog prava, a posebno ECHR-a kako ga tumači Europski sud za ljudska prava, svaka država članica u svom nacionalnom pravu propisuje postupak i uvjete koji se

moraju ispuniti kako bi se ostvarilo pravo na pristup zadržanim podacima u skladu sa zahtjevima nužnosti i proporcionalnosti.“ (Direktiva 2006/24/EZ 2006.) jednako tako taksativno navodeći kategorije podataka obradivih u te svrhe, kao što su identifikacija korisnika u odlaznoj i dolaznoj telefonskoj komunikaciji i u pokretnim i nepokretnim mrežama, internetska telefonska komunikacija, internetske elektroničke pošte te pohranjivanje podataka o brojevima, adresama internetske pošte i lokacija.(Direktiva 2006/24/EZ 2006.)

Ovo bi bio ukratko prikaz samo nekih, osnovnih normi i evolucije prava vezanih uz zaštitu osobnih podataka, na kojima dalje svaka država izgrađuje svoje zakone i donosi akte za daljnju razradu prema vlastitim potrebama.

3.2. Pravne osnove zaštite osobnih podataka u Republici Hrvatskoj

Kao i u svakoj državi, temelj za donošenje zakona o pojedinim pitanjima i njihovom uređivanju nalazi se u Ustavu. Tako je ustavnom odredbom Ustava Republike Hrvatske člankom 37. „Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se uređuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihovoga prikupljanja.“ (Ustav RH, NN, 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14, čl. 37.) postavljen okvir za donošenje Zakona o zaštiti osobnih podataka objavljenih u Narodnim Novinama , br. 103/03-, 18/06., 41/08., 130/11.i 106/12 kojima je uređena zaštita osobnih podataka, i nadzor nad prikupljanjem, obradom i uporabom na teritoriju Republike Hrvatske. Osim toga i obveza proizašla iz članstva u Europskoj Uniji, i iz potpisivanja sporazuma i konvencija,država je bila dužna donijeti norme u sladu s europskim zakonodavstvom vezano uz tu materiju, i osnovati nacionalno tijelo koje će imati isključivu nadležnost u postupanju s osobnim podatcima.

3.2.1 Agencija za zaštitu osobnih podataka

Agencija za zaštitu osobnih podataka je pravna osoba s javnim ovlastima, koja samostalno i neovisno obavlja poslove u okviru djelokruga i nadležnosti utvrđenih Zakonom o zaštiti osobnih podataka ("Narodne novine", broj 103/03, 118/06, 41/08, 130/11, 106/12). Agencija je uspostavljena i djeluje samostalno i neovisno o izvršnoj i zakonodavnoj vlasti, ne primajući upute i naloge od bilo kojeg državnog tijela, kako je propisano Direktivom 95/46 Europskog parlamenta i Vijeća od 24. listopada 1995. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka. Navedena Direktiva je temeljni

europski propis o zaštiti osobnih podataka i implementirana je u svim državama članicama. Direktiva 95/46 izričito propisuje neovisnost svih tijela za zaštitu osobnih podataka na području Europske unije, tako da je čl. 28. propisano da svaka država članica osigurava da je jedno ili više javnih tijela na njenom području odgovorno za nadzor primjene odredbi koje su donijele države članice u skladu s navedenom Direktivom i da ta tijela u provedbi funkcija koje su im povjerene djeluju potpuno neovisno. Neovisnosti tijela za zaštitu osobnih podataka propisuje osim toga i Konvencija za zaštitu osoba glede automatizirane obrade osobnih podataka (Konvencija 108 Vijeća Europe) i Dodatni protokol uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka. Hrvatski sabor je zakonom potvrdio Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatni protokol uz Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka.

Glavni zadaci Agencije za zaštitu osobnih podataka su učinkovito djelovanje na ispunjavanje svih prava i obaveza iz područja zaštite osobnih podataka koje se Republici Hrvatskoj nameću kao punopravnoj članici Europske unije i Vijeća Europe, povećanje odgovornosti svih sudionika u procesu obrade osobnih podataka vezano za primjenu propisa koji su obuhvaćeni zakonskim okvirom zaštite osobnih podataka u Republici Hrvatskoj uz odgovarajuću primjenu mjera informacijske sigurnosti.

Trajna zadaća Agencije je podizanje razine svijesti javnosti, o važnosti zaštite osobnih podataka i o njihovim pravima i obvezama, predlaganje mjera za stručno osposobljavanje i usavršavanje službenika za zaštitu osobnih podataka kao i ukupna provedba svih upravnih i stručnih poslova koji proizlaze iz Zakona o zaštiti osobnih podataka. (Agencija za zaštitu osobnih podataka2016.)

4. RADNJE I POSTUPCI VEZANI UZ PRIKUPLJANJE OSOBNI PODATAKA

4.1. Prikupljanje i obrada osobnih podataka

Iako se osobni podatci mogu naći na svakom koraku, njihovo prikupljanje i daljnja obrada jednako kao i sadržaj su normirani. Tako se prikupljanje podataka povjerava osobama koje se nazivaju voditeljima zbirki osobnih podataka. U tu kategoriju, prema zakonu, uvršteni su: državna tijela, tijela lokalne i područne (regionalne) samouprave te pravne i fizičke osobe, predstavništva i podružnice stranih pravnih osoba i predstavnici stranih pravnih i fizičkih osoba koje obrađuju osobne podatke. Zakon o zaštiti osobnih podataka. (NN 103/03, 118/06, 41/08, 130/11, 106/12

> Voditelj zbirke osobnih podataka je fizička ili pravna osoba, državno ili drugo tijelo koje utvrđuje svrhu i način obrade osobnih podataka. Kada je svrha i način obrade propisan zakonom, istim se zakonom određuje i voditelj zbirke osobnih podataka. Osnovu za prikupljanje podataka, zakon u svom sadržaju propisuje kao dobrovoljnu, onu na koju ispitanik daje suglasnost, i na onu koju je ispitanik dužan po zakonu odgovoriti, odnosno podatke koje je dužan dati. Dužnost davanja podataka odnosi se isključivo na situacije kada su podatci nužni za zaštitu javnog interesa, zaštitu života, ili na potrebe za izvršavanje drugih zakonskih radnji. Zakon o zaštiti osobnih podataka. (NN 103/03, 118/06, 41/08, 130/11, 106/12, čl.2. st.4.)

Osobni podaci mogu se prikupljati u svrhu s kojom je ispitanik upoznat, koja je izričito navedena i u skladu sa zakonom, a dalje mogu biti obrađivani samo u svrhu u koju su prikupljeni, odnosno u svrhu koja je koja se podrazumijeva sa svrhom prikupljanja.

Takvi osobni podatci moraju biti bitni u postizanju zaključaka koju bi obradom istih mogli donijeti izvršitelji obrade podataka, ali samo u opsegu koji ne zadire, odnosno koji ne može dovesti do zaključaka na osnovu kojih bi bilo moguće ugroziti zakonom zaštićenu kategoriju osjetljivih osobnih podataka, na koje ispitanik nije dao izričit pristanak. Količina i vrsta podataka ne smije biti veća od nužne da se zadovolji navedena svrha. Prikupljeni podatci moraju biti točni, potpuni, istiniti i ažurirani. Zakon o zaštiti osobnih podataka. (NN 103/03, 118/06, 41/08, 130/11, 106/12)

U obradu osobnih podataka prema zakonu podrazumijeva se svaka radnja ili skup radnji izvršenih na osobnim podacima, bilo automatskim sredstvima ili ne, kao što je

prikupljanje, snimanje, organiziranje, spremanje, prilagodba ili izmjena, povlačenje, uvid, korištenje, otkrivanje putem prijenosa, objavljivanje ili na drugi način učinjenih dostupnim, svrstavanje ili kombiniranje, blokiranje, brisanje ili uništavanje, te provedba logičkih, matematičkih i drugih operacija s tim podacima. Zakon o zaštiti osobnih podataka. (NN 103/03, 118/06, 41/08, 130/11, 106/12) Nadalje u pogledu korištenja osobnih podataka, osim zaključaka dobivenih obradom podrazumijeva se i davanje na korištenje, objavljivanje, dijeljenje, ili bilo koji način kojim se omogućava dostupnost takvih informacija.

Davanje podataka na korištenje zabranjeno je osim u taksativno navedenim slučajevima u Zakonu o zaštiti osobnih podataka i odnosi se kao i u slučajevima prikupljanja i obrade na zaštitu javnog interesa i sigurnosti, te na zaštitu života ispitanika, i druge zakonom definirane situacije.

Prije početka svake radnje u smislu prikupljanja i obrade podataka zakon navodi obvezu da se o namjerama obavijesti ispitanika, te mu na takav način omogući saznanje tko i u koju svrhu prikuplja podatke upućujući na zakon o pristupu informacijama, te obznaniti koje kategorije korisnika imaju prava uvida u te informacije, i o eventualnim potrebama za ispravcima prikupljenih informacija.

Svaki ispitanik ima pravo znati koje je podatke voditelj zbirke o njemu prikupio i u koju svrhu, te mu mora bit omogućen uvid u zbirku njegovih osobnih podataka. Jednako tako, ako su podatci prikupljeni na osnovu pristanka osobe, moguće je i pristanak povući, ili zatražiti brisanje nekakvih podataka za koje ispitanik smatra da nisu bitni, ili primjereni razlozima i cilju za koji su prikupljeni. Zakon o zaštiti osobnih podataka. (NN 103/03, 118/06, 41/08, 130/11, 106/12)

4.2. Načini prikupljanja podataka

Teoretski gledano svaki, na bilo koji način zabilježen trenutak može biti prikupljanje podataka. Međutim iako su zabilježeni, tek njihovom analizom mogu postati osobni, samo ako se na temelju bilo kojeg načina, kao što je prethodno bilo navedeno, može identificirati osoba na izravan, ili neizravan način. U nastavku su dani neki od načina prikupljanja podataka, a vezani su uz nove tehnologije.

4.2.1. Video nadzor i prikupljanje podataka

Jedan od suvremenih načina prikupljanja podataka je video nadzor, koji je uveden kao sustav mjere zaštite imovine zasnovan na zakonskoj odredbi koja omogućava vlasniku da zakonito prikupi i podatke koji su osobni. Samo prikupljanje podataka i ne predstavlja problem, budući se zakonske odredbe prema Zakonu o zaštiti osobnih podataka, (NN 103/03,

118/06, 41/08, 130/11, 106/12, čl.3.) izuzimaju primjenu zakona na obradu osobnih podataka koje provode fizičke osobe isključivo za osobnu primjenu, ili za potrebe kućanstva. Pravi problem nastaje kada se dođe do šireg pristupa informacijama drugih neovlaštenih korisnika na temelju čega izravno dolazi do kršenja prava pojedinca na zaštitu osobnih podataka. Iako je sustav video nadzora uvelike koristan jer stvarno doprinosi jačanju sigurnosti i potencijalnom smanjenju kriminala, kao i lakše određivanje i dokazivanje tijeka događaja i sudionika u događajima, zahtjeva poseban oprez prilikom njegovog korištenja.

Video nadzor je jedan od uobičajenih načina na koji i poslodavci štite svoju imovinu, ali i osiguravaju nadzor primjene zakona i pravilnika. Za takve vrste nadzora postoje uvjeti pod kojima mogu biti postavljeni nadzorni uređaji i obveze poslodavca kao voditelja zbirke o poštivanju zakonskih normi predviđenih za prikupljanje i obradu osobnih podataka. U svom priručniku Plazonić i Šoić (2015: 6.1,str.2.) kao osnovne pretpostavke za uvođenje video nadzora navode ;

- donošenje dokumenta pravilnika o radu, ili nekog drugog pravilnika
- savjetovanje s radničkim vijećem o uvođenju video nadzora
- određivanje i imenovanje osobe ovlaštene za pristup osobnim podatcima
- uočljivo i nedvojbeno označavanje (slikom i tekstom) da je objekt pod video nadzorom
- te da se radi o prostoru koji je prihvatljiv za video nadzor

Prvom točkom poslodavac uređuje najvažniju stvar, a to je informiranje svih koji se u tom prostoru nalaze o provođenju nadzora putem video kamera, te time u neku ruku dobiva i svojevrstan oblik neizravne suglasnosti potencijalnih ispitanika. Nadalje pravilnikom definira razloge opravdanosti takve vrste nadzora te opseg, ovlaštenje u pogledu obrade podataka,te mogućnost uvida u vlastite osobne podatke radnika o kojima su takvi podatci sačinjeni. U slučajevima kada poslodavac propusti donijeti pravilnik kojim je uredio takvu vrstu nadzora, svaki sačinjen podatak postaje nezakonit, a samim time predstavlja i povredu prava na zaštitu podataka.

Iako je drugom točkom predviđeno savjetovanje s radničkim vijećem, ono ne donosi nikakve pravne odlučnosti u pogledu namjera poslodavca, već eventualno otvara mogućnost suradnje u zaštiti radničkih prava. Dakle bez obzira na mišljenje, pristanak, ili odbijanje pristanka poslodavcu pripada pravo zaštiti svoju imovinu, te će se unatoč protivljenju nadzor vršiti zakonito. Izuzev u slučajevima kada je video nadzor usmjeren tako da čitavo radno

vrijeme kontinuirano prati svaki pokret radnika na radnim mjestu, onda je nužna suglasnost radničkog vijeća ili sindikata ukoliko radničko vijeće ne postoji.

Kada je riječ o ovlaštenju osobe koja će nadzirati i imati pristup takvim informacijama poslodavac kao voditelj zbirke ima obvezu imenovati u pisanom obliku osobu zaduženu za zaštitu osobnih podataka, ako zapošljava do 20 radnika, a ako zapošljava više od 20 radnika, tada je obvezan o imenovanju i o zbirci izvijestiti Agenciju, kao središnje tijelo nadležno za područje osobnih podataka. Osoba koja je u ime voditelja zbirke ovlaštena za zaštitu osobnih podataka mora biti istaknuta i objavljeni kontaktni podatci na mrežnim stranicama, ili drugim načinom učinjeno dostupnom svima čiji podatci se mogu nalaziti u zbirci.

Osim objavljenog pravilnika, prethodno objašnjeno, jasna i nedvojbena informacija da je objekt pod video nadzorom obavještava radnike o prikupljanju podataka, te im osim sigurnosti omogućava i korištenje nadzora nad prikupljenim podatcima i korištenjem istih u granicama predviđenim pravilnikom, te osigurava mogućnost zaštite osobnih podataka od zlouporabe i prekomjernih korištenja.

Kao prihvatljivi prostori u kojima se može vršiti video nadzor navedeni su prilazi, izlazi, parkirališta, vitalni pogonski dijelovi i procesi, ali i zabrana snimanja prostora u kojima se radnici presvlače, te sanitarne prostorije budući da one predstavljaju područje od privatnosti radnika.

4.2.2. Podatci prikupljeni biometrijskim sustavom

Biometrijski sustav, ili biometrijski podatci kako je objašnjeno u priručniku Plazonić i Šoić (2015: 7.1, str 1.) su podatci ili postupci kojim se osoba identificira temeljem jednog ili više bioloških obilježja te obilježja ponašanja. Načini na koji se provodi biometrijska identifikacija jesu oni kojima se mjere fizičke i fiziološke karakteristike osobe, a one moraju biti jedinstvene za svaku osobu, univerzalne i trajne, te prikupljene na jednostavan način.

U biometrijske podatke svrstani su otisak prsta, skeniranje oka, prepoznavanje lica (prema tome i video nadzor predstavlja oblik prikupljanja biometrijskih podataka) prepoznavanje glasa, otisak dlana, DNK analiza, neke fizičke karakteristike svojstvene samo za tu osobu poput hoda, mimike, fizičkih nedostataka, ponašanja u određenim situacijama.

Prikupljanjem i obradom podataka na ovakav način moguće je izvesti i osjetljive osobne podatke kojima je direktno dovedeno u pitanje dostojanstvo osobe i njegovo pravo na zaštitu takvih podataka. Plazonić i Šoić (2015:7.1, str 2-6) smatraju da za jednostavnu evidenciju prisutnosti na poslu putem otiska prsta nije primjerena svrsi koju se želi postići, navodeći primjere u kojima se osoba i sama mogla na takav način osigurati, ili osigurati svoju

imovinu, te pohranom takvog podatka njegova jedinstvenost u primjeni nije više jednaka, a samim time i dovodi u pitanje sigurnost takvog podatka od zlouporabe. Isto se odnosi i na ostale biometrijske podatke poput skeniranja oka, glas, te izradom profila ispitanika na temelju prikupljenih podataka s namjerom procjene karaktera, analize i predviđanja zdravlja,ekonomske situacije, sklonosti pojedinaca ili njihovog kretanja, pozivajući se na preporuku Vijeća europe (2010) zaključuju kako je nužno o takvoj vrsti prikupljanja i obrade podataka obavijestiti i dobiti izričit pristanak ispitanika, osim u slučajevima određenim zakonom.

4.2.3. Podatci prikupljeni GPS sustavom i tahografom

Ovakav način prikupljanja podataka uglavnom služi za dobivanje rezultata rada, odnosno za preglednost ostvarivanja ciljeva predviđenih u nekom vremenskom periodu ili procesu. Iako se takvim sustavima koriste poslodavci kao oblikom kontrole položaja službenih vozila primjerice GPS sustav, odnosno bilježenje podataka tahografom u prijevozništvu,a u njima neposredno mogu biti i prikupljeni podatci o radniku, čini se kako je njihova svrha sasvim razmjerna i osim eventualnih podataka o savjesnosti radnika, ne predstavlja znatnije zadiranje u osobne podatke. Primjena takvih uređaja i analiza podataka dobivenih na takav način pokazala se višestruko korisna kako u nadzoru nad poštivanjem radnog vremena odnosno vrijeme koje vozači provedu vozeći bez stajanja, određene rute propisane nalogom poslodavca, tako i kao isprave svjedočanstva i dokaza pred sudom i drugim tijelima o okolnostima nekog događaja i sudionicima.

Do sada ovakav oblik prikupljanja i obrade podataka pokazuje potpunu razmjernost i svrhovitost svog korištenja i ne nalazi se kršenja osobnih prava kao u ostalim metodama. Iako je dužnost poslodavca izvijestiti radnika o korištenju takvih uređaja, te isto urediti pravilnikom, gotovo da je takav način sasvim logičan i radnici očekuju takve sustave na vozilima, pa se oko toga niti ne vode daljnje rasprave.

4.2.4. Prikupljanje podataka poligrafskim testiranjem

Iako poligrafsko testiranja ili detektor laži kao popularna metoda prikupljanja podataka može dati vrlo korisne podatke, stručnjaci, kao i autori priručnika Plazonić i Šoić (2015: 7.3 , str1,2.) smatraju kako nije razmjerna svrhama u koje se koristi, te da se za sve podatke može upotrijebiti manje invazivna metoda. Jednako tako rezultati koje će prilikom testiranja dati ispitanik, nisu samo podatci koji su potrebni već i niz osjetljivih podataka koji su prekomjerni za korištenje. Rezultati osim toga mogu ovisiti o stanju ispitanika, njegovom zdravlju, te nizu drugih čimbenika, te se vjeruje kako točnost i istinitost nisu neupitni s

obzirom na ispitanika, ispitivača, a i osobe koja obrađuje i analizira iste. Samim time svoju primjenu ne nalazi često, i podatci dobiveni takvim metodama ne koriste kao isprave i dokazi, samo mogu poslužiti kao smjernice i pomoć u drugim postupcima. Za provođenje takvih metoda naglašeno je da je izričan pristanak osobe nužan, i da se ni na koji drugi način ne provodi,već isključivo na temelju njega, s obvezom detaljnog objašnjenja postupka i metoda prije samog testiranja.

4.3. Iznošenje osobnih podataka u druge zemlje

Iznošenjem osobnih podataka u druge zemlje smatra se svako ustupanje, dijeljenje i davanje na uvid. Prema Agenciji kao nadležnom tijelu za postupanje s podatcima, nije dozvoljeno osobne podatke fizičkih osoba iznositi iz Republike Hrvatske u druge države ili međunarodne organizacije ukoliko one ne osiguravaju odgovarajuću zaštitu osobnih podataka. Na svojoj stranici taksativno navode zemlje čiji sustavi osiguranja odgovaraju zakonodavnim okvirima Republike Hrvatske, te naglašavaju uvijete koje je potrebno ostvariti da bi nečiji osobni podatci mogli biti izneseni u druge država.

> Ukoliko protivno uvjetima određenima u ZoZOP-u iznosi osobne podatke iz Republike Hrvatske u svrhu daljnje obrade ili ih objavi ili na drugi način učini dostupnim drugome ili tko prikupljanjem, obradom ili korištenjem osobnih podataka sebi ili drugome pribavi znatnu imovinsku korist ili prouzroči znatnu štetu, kaznit će se kaznom zatvora do tri godine.(Potrka 2013)
>
> Tako navode uvijete redom kao što su:

- postoji privola ispitanika ili - iznošenje je nužno u svrhu zaštite vitalnih interesa ispitanika ili - iznošenje se temelji na ugovoru koji pruža dovoljna jamstva za zaštitu podataka (primjerice ugovor koji je sukladan standardnim ugovornim klauzulama Europske komisije) ili
- iznošenje je potrebno radi izvršenja ugovora između voditelja zbirke osobnih podataka i ispitanika ili provedbe predugovornih mjera na zahtjev ispitanika ili
- iznošenje je potrebno za zaključivanje ili izvršenje ugovora između voditelja zbirke osobnih podataka i treće osobe a koji je u interesu ispitanika ili
- iznošenje je potrebno ili određeno zakonom radi zaštite javnog interesa ili radi zakonskih potraživanja ili
- iznošenje se obavlja iz evidencije koja je sukladno zakonu ili drugom propisu namijenjena pružanju informacija javnosti.

Ujedno ostavljajući mogućnost voditeljima zbirki, ukoliko postoji sumnja u opravdanost i sigurnost iznošenja podataka u druge zemlje, razmotriti i savjetovati ih u tom slučaju.

5. OBLICI PRIKUPLJANJA OSOBNIH PODATAKA PUTEM INTERNETA

Živimo u društvu koje karakterizira upotreba usluge *World Wide Web*, pametnih mobilnih uređaja i društvenih mreža, gdje pojedinac namjerno ili nenamjerno može podatke učiniti dostupnima pa samim time može biti nadziran i može biti određena njegova trenutna lokacija. Svaku od ovih novo razvijenih tehnologija prate različiti problemi vezani uz privatnost. Prije svega ove tehnologije omogućavaju prikupljanje puno informacija o korisnicima određene tehnologije, a tako prikupljene informacije mogu biti pohranjene, kombinirane te analizirane u bilo koje vrijeme. Nadalje ove tehnologije omogućavaju daljnje širenje i publikaciju informacija u raznim oblicima, te samim time predstavljaju opasnost za povredu prava vezanih uz zaštitu osobnih podataka i njihovu zlouporabu.

Kroz ovo poglavlje bit će predstavljen dio oblika prikupljanja i obrade osobnih podataka koji su najčešće korišteni u svakodnevnom životu ljudi, poput elektroničke pošte i internetskih poziva, društvenih mreža i kupovine putem weba te samog pregledavanja sadržaja na internetskim stranicama.

5.1. Elektronička pošta i pozivi putem interneta

Kod internetske komunikacije bilo elektroničko poštom, ili video i audio pozivima jednako može doći do otkrivanja osobnih podataka, ili neovlaštenog prikupljanja.

Iako sam identitet poput imena, korisničkog imena i lozinke, budući ga sam korisnik obznanjuje nije sporan, informacije unutar same komunikacije mogu biti izvor raznih informacija koje su direktno ili indirektno osobni podatci. Upravo iz tog razloga potrebno je razumjeti što je u stvari Internet i što na njemu predstavlja računalo korisnika, a evo kako je to objašnjeno u CARNET-ovoj brošuri.

> Važno je razumjeti da je naše računalo, kada ga spojimo na Internet, dostupno svim drugim računalima spojenima na Internet, komunicirali mi s njima ili ne. Internet je mreža u kojoj su svi međusobno povezani. Naše računalo samo po sebi i nije posebno zanimljivo, no tisuće takvih kao što je naše predstavljaju velike resurse s kojima se štošta može napraviti. (CARNET 2001)

Budući je internetska veza osnova ovakve komunikacije logično je da je izloženost takvim mogućnostima sigurna. Bilo tko u bilo kojem trenutku može prikupiti podatke, a da ustvari nisu niti nužni ni potrebni, gotovo bez ikakvog nadzora. Jedino, kada je komunikacija

takvim načinima dio rada odnosno odvija se na radnom mjestu na službenim uređajima poslodavca, tada se u pogledu nadzora otvaraju drugačija pitanja. Svaki oblik komunikacije se i dalje prema Konvenciji smatra privatnim životom i dopisivanjem, pa čak i ako se odvija sa službenih uređaja. Kako bi poslodavcu ipak bilo omogućeno da u vlastite svrhe vrši nadzor, nužno je da o takvim radnjama izvijesti radnike, te uputi na svrhu i opravdanost takvih radnji. Prilikom obrade i čuvanja podataka nužno je voditi računa i o osobama prema kojima se vodila komunikacija, jer u ovakvim slučajevima i osobni podatci trećih osoba ostaju u bazi podataka.

Elektroničkom komunikacijom, osim što podatke koji mogu biti osobni, a izneseni su u sadržajima, jednako tako neočekivana i neželjena komunikacija poput poznatih spamova mogu omogućiti prenošenje podataka, a da toga nismo niti svjesni. Kao što je već bilo rečeno, spajanjem uređaja na Internet omogućen je pristup svim informacijama. Često se tako za mogućnost pristupa određenim stranicama traži registracija, a obično uključuje unošenje adrese elektroničke pošte. I ne mora značiti da će upravo s te stranice biti izvršen nekakav pokušaj zlouporabe, ali načini funkcioniranja su uglavnom marketinški i komercijalni i sigurno je kako će o svom radu i uslugama koje je moguće dobiti i kupiti slati obavijesti na adrese putem kojih su se korisnici prijavili. Od takvih oblika pošte, ako je stranica ozbiljna nije problem ostvariti zaštitu, budući uvijek ostavlja mogućnost odabira „želim primati obavijesti ili ne želim“, problem je sa stranicama koje upravo iz razloga prikupljanja takvih podataka ne ostavljajući mogućnosti izbora na takav način dobivaju pristup adresi elektoničke pošte i mogu predstavljati ozbiljnu opasnost za podatke koji se mogu nalaziti na uređaju.

5.2. Društvene mreže kao izvori podataka

Sastavni dio života od nedavno su postale i razne društvene mreže kreirane na internetu, koje svojim članovima nude pregršt raznih mogućnosti. Osim što su iznimno popularne, pa samim time i zabavne za većinu ljudi, sadržavaju i ogromnu količinu podataka o svom korisniku, odnosno vlasniku. Na društvenim mrežama je moguće osim imena, prezimena, adrese, datuma rođenja postavljati slike, iznositi stajališta, uključivati se u razne druge grupe istomišljenika, sklapati prijateljstva i komunicirati širom svijeta u stvarnom vremenu.Osim toga toliko su popularizirane da su u njih uključene i javne institucije, kao jedan od mogućih načina približavanja građanima i lakšeg i bržeg komuniciranja. Ukratko, globalno selo u kojemu se sve može saznati i najbogatija riznica osobnih podataka, i onih osjetljivih kojima se mogu svi poslužiti uz nedovoljnu pažnju vlasnika. Istina je kako je

moguće zaštiti sve podatke, ali to nerijetko iziskuje dosta vremena, puno znanja i vršenje odabira klikanjem na razne mogućnosti, što baš rijetko tko je spreman izdvojiti.

Vrlo je vjerojatno da će upoznavanjem nove osobe biti provjeren njen profil na nekoj od društvenih mreža, ili čak i poslodavci posežu za takvim taktikama nebili priskrbili čim više podataka o potencijalnom zaposleniku. Samim time lišava se odgovornosti i mogućnosti da se ogriješi o pravila postavljajući nedopuštena pitanja, budući odgovore može pronaći na ovakav način. Osim konkretnih informacija i podataka može se stvoriti i karakterističan profil o osobi kao radniku, čovjeku, imati uvid u razmišljanja i odnos prema poslu i poslodavcu. To je svakako puno više podataka nego što bi bilo potrebno i razmjerno situaciji, međutim osobno su učinjeni dostupnima. Da ne bi izgledalo samo u lošem svjetlu, velika količina informacija nikako ne mora nužno značiti loše. Ponekad upravo to daje više sigurnosti i povjerenja.

5.3. Osobni podatci prilikom kupovine putem interneta

Za razliku od komunikacije, druženja i objavljivanja na društvenim mrežama, kupovina putem interneta je jedan od osjetljivijih, a i kriminalu najzanimljiviji izvor podataka. Ne tako začuđujuće, ali tu se ipak provede najviše vremena nastojeći zaštititi podatke od vitalne važnosti. Prema tome ispada da je pojedinac ipak najranjiviji kada je novčanik u pitanju. Tako se prilikom kupovine osim onih osnovnih podataka poput imena, prezimena i adrese radi dostavljanja kupljenih proizvoda unose i pojedincu osjetljivi podatci o bankovnim računima i karticama kojima će proizvodi biti plaćeni.

> Najnovija velika anketa hrvatskih kompanija Perpetuum Mobilea, PBZCarda, Symanteca i Bugaotkriva da 65% hrvatskih državljana kupuje na internetu. Zanimljivo je da je korištenje PayPala gotovo već dosegnulo korištenje kreditnih kartica**.** Naime, za kupnju na internetu Hrvati najviše koriste kreditne kartice (75,6 %), ali blizu je i postotak Paypala (72,7 %), što svjedoči trendu da građani žele što jednostavnije transakcije na internetu. Stoga ne čudi da oni koji upotrebljavaju e-bankarstvo najviše se njime koriste zbog lakše dostupnosti, a čak ih petina ne želi ili nema vremena odlaziti na šalter.(Lijović 2016)

Iz prethodnog odlomka je očigledno da velik broj podataka kola internetom. Neki servisi za plaćanje nakon jednog korištenja pamte podatke o kartici i iduća kupovina moguća je uz korištenje samo korisničkog imena i lozinke. U tom slučaju, korisničko ime i lozinku jednako su osjetljivi podatak kao i sve informacije o kartici. Ako je moguće, preporuča se uklanjanje podataka o kreditnoj kartici iz web profila nakon korištenja. U slučajevima zlouporabe podataka na ovim internetskim uslugama, ne samo da se na osnovu kupljenih proizvoda može

procijeniti stavove i ukuse, te navike osoba, već se direktno može nanijeti financijska šteta krađom podataka o računima i karticama.

6. METODE ZAŠTITE OSOBNIH PODATAKA

Prilikom razmatranja i definiranja mogućih metoda zaštite osobnih podataka potrebno ih je razdijeliti na one koji sastavni dijelovi zbirki za koje su voditelji poznati i ovlašteni, te na one koje se slučajno, ili namjerno mogu naći u javnosti.

6.1. Vrste i metode zaštite podataka u bazama voditelja zbirki

Kod osobnih podataka sadržanih i obrađivanih u bazama voditelja zbirki generalno postojanje opasnosti svedeno je na samo na savjesnost voditelja, i izvršitelja obrade podataka po nalogu voditelja, te na adekvatan sustav zaštite njihovih baza podataka. To znači da je prema Zakonu o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11, 106/12) voditelj zbirke definiran kao svaka pravna i fizička osoba državno ili drugo tijelo koje utvrđuje svrhu i način obrade osobnih podataka. Kada je svrha i način obrade propisan zakonom, istim se zakonom određuje i voditelj zbirke osobnih podataka.
Voditelj zbirke osobnih podataka za svaku zbirku osobnih podataka koju vodi, uspostavlja i vodi evidenciju koja sadrži temeljne informacije o zbirci, a osobito sljedeće:

1. naziv zbirke,

2. naziv, odnosno osobno ime voditelja zbirke i njegovo sjedište, odnosno adresu,

3. svrhu obrade,

4. pravni temelj uspostave zbirke podataka,

5. kategorije osoba na koje se podaci odnose,

6. vrste podataka sadržanih u zbirci podataka,

7. način prikupljanja i čuvanja podataka,

8. vremensko razdoblje čuvanja i uporabe podataka,

9. osobno ime, odnosno naziv primatelja zbirke, njegovu adresu, odnosno sjedište,

10. naznaku unošenja, odnosno iznošenja podataka iz Republike Hrvatske s naznakom države, odnosno međunarodne organizacije i inozemnog primatelja osobnih podataka te svrhe za to unošenje, odnosno iznošenje propisano međunarodnim ugovorom, zakonom ili drugim propisom, odnosno pisanim pristankom osobe na koju se podaci odnose,

11. naznaku poduzetih mjera zaštite osobnih podataka.

Što bi značilo da je svaki takav voditelj zakonit, i da je svaki izvršitelj imenovan od strane voditelja osoba od povjerenja i moralnih načela te su svi postupci vezani uz osobne podatke definirani zakonom i obvezuju voditelje i izvršitelje isključivo zakonito postupanje, te mogućnost provedbe nadzora nadležnog središnjeg tijela nad poštivanjem odredbi zakona, i po eventualnim pritužbama i zahtjevima osoba ispitanika kojima su prema zakonu omogućene metode kojima se štite osobni podatci.

> Valja napomenuti, što je posebno važno za djelatnike Ministarstva unutarnjih poslova,da ako kazneno djelo počini službena osoba u obavljanju svojih ovlasti, kaznit će se kaznom zatvora od šest mjeseci do pet godina. (Potrka 2013)

Tako je kao polazište u zaštiti osobnih podataka određeno zakonskom odredbom prava ispitanika da:

> Prije prikupljanja bilo kojih osobnih podataka, voditelj zbirke osobnih podataka ili izvršitelj obrade dužan je informirati ispitanika čiji se podaci prikupljaju o identitetu voditelja zbirke osobnih podataka, o svrsi obrade u koju su podaci namijenjeni, o postojanju prava na pristup podacima i prava na ispravak podataka koji se na njega odnose, o primateljima ili kategorijama primatelja osobnih podataka te da li se radi o dobrovoljnom ili obveznom davanju podataka i o mogućim posljedicama uskrate davanja podataka. U slučaju obveznog davanja osobnih podataka navodi se i zakonska osnova za obradu osobnih podataka. Zakon o zaštiti osobnih podataka. (NN 103/03, 118/06, 41/08, 130/11, 106/12)

Time je omogućeno ispitanicima kontrolirati prikupljanja i obradu podataka, postavljati zahtjeve voditeljima u pogledu istinitosti, točnosti i potpunosti podataka sadržanih u zbirkama te zahtjevom za brisanje određenih podataka, na koje su voditelji zbiraka dužni odgovoriti.

U slučajevima kada se radi o podatcima za koje je ispitanik dao suglasnost za njihovu obradu, ostavlja se zakonska mogućnost odustajanja od takve suglasnosti, a o svemu je dužnost voditelja informirati osobu ispitanika i to u roku od 30 dana.

Osim toga u slučajevima kada osoba smatra da neki od voditelja zbirke posjeduje ili obrađuje podatke a da o istome nije obaviještena, može podnijeti zahtjev voditelju zbirke, na koji je on dužan dostaviti pisanu potvrdu o tome :

- obrađuju li se osobni podatci koji se odnose na njega ili ne;
- dati obavijest o razumljivom obliku o podatcima koji se odnose na njega čija je obrada u tijeku te o izvoru tih podataka;

- omogućiti uvid u evidenciju zbirke osobnih podataka te uvid u osobne podatke sadržane u zbirci osobnih podataka koji se odnose na njega te njihovo prepisivanje;
- dostaviti izvatke, potvrde ili ispise osobnih podataka koji se na njega odnose, a koji moraju sadržavati i naznaku svrhe i pravnog temelja prikupljanja, obrade i korištenja tih podataka;
- dostaviti ispis podataka o tome tko je i za koje svrhe i po kojem pravnom temelju dobio na korištenje osobne podatke koji se odnose na njega;
- dati obavijest o logici bilo koje automatske obrade podataka koji se na njega odnosi. Plazonić, Šoić(2015: 8.1,str. 1,2)

Iz svega navedenog vidljivo je da kod zakonitih voditelja zbirki osobnih podataka postoji uređen sustav poštivanja pravila postupanja prilikom prikupljanja i obrade osobnih podataka, osiguranih kaznenim odredbama zakona kojima u suprotnom podliježu .

6.2. Zaštita osobnih podataka na internetu

Internet je danas jedan od najvećih izvora informacija kako za korisnike, tako i o korisnicima. Budući je prethodno definirano i objašnjeno kako vezano uz osobne podatke i voditelje zbirki ustvari postoji donekle učinkovito definiran i provediv sustav zaštite,iako u svom radu Boban (2012) smatra da je zakonodavna regulativa samo okvir koji uređuje pravo na pristup informacijama, u svakoj demokratskoj državi sudovi (ili ustavni sudovi) imaju posebnu ulogu i značaj, jer o sudskoj praksi uvelike ovisi hoće li jedno od najvažnijih osobnih prava biti afirmirano u praksi, i dovesti do toga da se državna tijela počnu sve više otvarati javnosti i osigurati transparentno upravljanje.

Problem predstavljaju novine u tehnološkim mogućnostima koje same navode korisnike da otkrivaju javno svoje osobne podatke bilo putem komunikacije, prisutnosti na društvenim mrežama, kupovinom na internetu ili samim pregledavanjem sadržaja. Kako se smatra nisu svi podatci osobni, ili čak iako jesu ne moraju nužno biti povrijeđena prava, međutim prilika uvijek nađe i nepriliku. Tako se nerijetko događaju razne vrste prijevara, i zlouporabe podataka koje osobe ostavljaju samostalno na uvid svima.

Jedini učinkoviti način zaštite od takvih neovlaštenih prikupljanja i obrade osobnih podataka je da se prije nego li se odluči koristiti suvremenim načinima nauči kako se zaštititi od opasnosti koje vrebaju u tako velikim količinama informacija.

Tehnološka dostignuća i napredci nikako nisu usmjereni u pravcu koji bi trebao predstavljati opasnost za pojedince i njegove osobne informacije, ali uvijek se nalazi netko

tko želi takav način iskoristiti, dovodeći u pitanje osnovna ljudska prava. Današnji suvremeni sustavi Boban (2012) smatra trebali su riješiti neke stare probleme, ali ih zamjenjuju novijima, te stari postaju irelevantni, a novi sudbonosni.

Zaštita podataka u informacijskim sustavima svakako predstavlja velik izazov i stručnjacima i znanstvenicima. Za sada od nedopuštenih prikupljanja i obrađivanja, te objavljivanja podataka, jedina učinkovita metoda je osobna edukacija i ispravni odabiri pouzdanih izvora, dodatan oprez kod izbora podataka koji će se objavljivati, pažljiv izbor osoba koje će vidjeti određene podatke, te suradnja s davateljima usluga koji omogućavaju provođenje zaštite svojim korisnicima. Budući da je svaka tehnologija prvenstveno nastala iz želje za napretkom i boljitkom, a potencijalno postoji i mogućnost za njenu zlouporabu, na svaki napad zlonamjernika proizvođač nastoji odgovoriti adekvatnim zaštitama. Stoga je važno u skladu s uputama proizvođača ažurirati preglednike, programe i aplikacije kojima se koristi kako sami ne bi postali posrednici u neovlaštenim radnjama. Važno je pomno odabrati vrstu i količinu podataka koja će se obznaniti i provjeriti pouzdanost stranica koje se posjećuju.

7. ZAKLJUČAK

Govoreći o zaštiti osobnih podataka i proučavajući njeno porijeklo i značenje, nameće se zaključak kako su sva suvremena prava osobnih podataka potekla od samo jedne rečenice sadržane u Deklaraciji o pravima čovjeka, koja je jamčila u početku pravo na privatnost. Stalnim napretkom društva iz tog osnovnog prava izvode se nova prava, a samim time zahtijevaju i normativnu uređenost i zaštitu. Nije sve osobni podatak, ali obradom svaki podatak ili informacija može dati osobni podatak.

Pravna regulativa vidljiva je u tome što se na međunarodnom i domaćem području donosi niz pravila kojima se definiraju zakoniti voditelji zbirki podataka, određuju okviri opsega, načina prikupljanja, obrade te prenošenja i dijeljenja osobnih podataka pojedinaca. Kaznenim odredbama obvezuju se voditelji na pridržavanje normi i osiguravaju na takav način učinkovitu zaštitu osobnih podataka.

Suvremeni način života donosi niz novih mogućnosti u komunikaciji i dostupnosti informacija neovlaštenim osobama koje u pogrešnim rukama ili pogrešnom primjenom postaju prijetnja pojedincu i cjelokupnom društvu. Danas se osobni podatci nalaze gotovo svuda i mogu biti izvedeni iz samo nekoliko šturih informacija. Prenose se i dijele neslućenim brzinama ugrožavajući osnovna ljudska prava. Velikim brojem normi zakonodavstvo pokušava osigurati zaštitu, međutim stalni napredak onemogućava učinkovit način, barem ne na duži vremenski period.

Najučinkovitija metoda zaštite osobnih podataka jest stalna suradnja znanosti, tehnologije, državnih vlasti i pojedinaca, koji zajednički mogu vršenjem nadzora kojim se prepoznaju potencijalne opasnosti, izgradnjom i uvrštavanjem novih mehanizama u sustave, izvođenjem novih prava i pravila kao posljedice zahtjeva i pritužbi pojedinaca stvoriti i održavati učinkovite sustave zaštite.

8. POPIS KORIŠTENE LITERATURE

Knjige i priručnici:

1. Plazonić, K.; Šoić, N. (2015) Zaštita osobnih podataka: Priručnik o zakonitoj uporabi tehnologije u svrhu obrade osobnih podataka tijekom radnog odnosa s primjenama na CD-u. Zagreb: Forum Poslovni Medij d.o.o.

2. Agencija Europske unije za temeljna prava, (2014) ; Vijeće Europe,(2014.) Priručnik o europskom zakonodavstvu o zaštiti podataka. Luksemburg: Ured za publikacije Europske unije http://eurlex.europa.eu/legalcontent/HR/TXT/?uri=celex%3A32006L0024#ntr3-L_2006105HR.01005401-E000316.07.2016.

Znanstveni i stručni rad u zborniku i zbirci radova

1. Boban, M.(2012) Pravo na privatnosti i pravo na pristup informacijama u suvremenom informacijskom društvu. Split: Zbornik radova Pravnog fakulteta u Splitu, god. 49, 3/2012., str. 575.- 598.
2. Dragičević, D.; Gumzej, N.(2014) Obvezno zadržavanje podataka i privatnost, Zagreb: Zbornik Pravnog fakulteta u Zagrebu god. 64, (1) 39-80
3. Protrka, N.(2013) Normativna uređenost zaštite osobnih podataka u Republici Hrvatskoj, Policijska sigurnost. Zagreb: Univerzalna decimalna klasifikacija god. 22. (2013), broj 4., str. 509_521

Članak u časopisu

1. lijović, D. (2016) Koliko zaostajemo za europom: Hrvati na internetu najčešće kupuju knjige,softver-i plaćaju račune. Večernjilist 16.3.2016 http://www.vecernji.hr/techno/hrvati-na-internetu-najcesce-kupuju-knjige-softver-i-placaju-racune-1068804 29.7.2016

Norme i zakoni

1. Ustav Republike Hrvatske (2010) Zaštita ljudskih prava i temeljnih sloboda pročišćeni tekst, Narodne novine broj 85/10
1. Vijeće Europe (1981) Konvencija 108, Konvencija 108 za zaštitu osoba glede automatizirane obrade osobnih podataka
2. Vijeće europske unije (2002) Direktiva 2002/58/EZ Europskog vijeća i Parlamenta od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti na području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama)32002L0058
3. Vijeće europske unije (1995) Direktiva 95/46/EZ Europskog vijeća i Parlamenta od 24. listopada 1995 o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka31995L0046
4. Vijeće europske unije (2006) Direktiva 2006/24/EZ Europskog vijeća i Parlamenta od 15. ožujka 2006. o zadržavanju podataka dobivenih ili obrađenih u vezi s pružanjem javno dostupnih elektroničkih komunikacijskih usluga ili javnih komunikacijskih mreža te kojom se izmjenjuje i dopunjuje Direktiva 2002/58/EZ
5. Zakon o zaštiti osobnih podataka. (NN 103/03, 118/06, 41/08, 130/11, 106/)
6. Zakon o pravu na pristup informacijama . (NN 25/13, 85/15)

Internet izvori

1. Agencija za zaštitu osobnih podataka URL:http://azop.hr(20.7.2016)
2. CARNET URL:http://www.cert.hr (27.7.2016)

IZJAVA O AUTORSTVU RADA

Ja, **Marija Martinelli**, pod punom moralnom, materijalnom i kaznenom odgovornošću, izjavljujem da sam isključivi autor završnog/diplomskog rada pod naslovom **Pravna regulativa vezana uz zaštitu osobnih podataka,** te da u navedenom radu nisu na nedozvoljen način korišteni dijelovi tuđih radova.

U Požegi, 07. kolovoza 2016

Ime i prezime studenta

_____