**PRAVNA INFORMATIKA**

\* napomena: ovo je skripta po knjizi iz 2015.g. i dosta je detaljna; neka vas ne obeshrabri broj stranica jer je neke dijelove dovoljno samo procitati ☺

**2.CJELINA: Informacijska sigurnost**

- **David Attenbourgh**: „ Life on Earth“( objavljeno 1979.godine)- zadnje poglavlje ima karakterističan naslov( „Strast komuniciranja“ )🡪 smatra da vodeće mjesto u nastanku i razvoju čovjeka ima nagon i interes za slanje poruka,a prema tome se čovjek razlikuje od ostalih živih bića(na to upućuju i slike od prije 30 000 godina u pecinama..)

- čovjekov urođeni talent,inteligencija i obrazovanje dolaze do izražaja kroz **komunikaciju** s drugim ljudima

-u početku su se koristili jednostavni oblici mimike,gestikuliranja,slikovitog izražavanja, govora, pisanja,dimnih signala,itd.,a od sred.15.st. se širi korištenje sve savršenijih tehničkih pomagala i tehnoloških rješenja 🡪 odvija se **informacijska revolucija,** tj.nastupa doba koje karakterizira permanentna **informatička revolucija** sa učestalijim promjenama

\* za razliku od informacijske revolucije, informatička revolucija obuhvaća ona tehnološka rješenja koja se ostvaruju korištenjem modernih informatičkih i komunikacijskih postrojenja,uređaja i mreža kojima se unose,obrađuju i pohranjuju podaci, prenose slike,glas,zvuk i signali u digitalnom obliku

- **INFORMACIJSKA REVOLUCIJA** – povijesni zaokret u komuniciranju među ljudima i njihovim organizacijama i zajednicama,izazvan određenim tehnološkim pronalaskom ili nizom tehničkih otkrića i odgovarajućih tehnoloških postupaka(često se poistovjećuje i koristi kao sinonim za informatičku revoluciju,ali je to širi fenomen koji se javlja sred.15.st. – informatička revolucija je samo etapa u tom razvoju,a odnosi se na promjene što ih je sred. 20.st. donijela mikroelektronička tehn. u prikupljanju,pohrani,obradi,distribuciji i upotrebi informacija)

- pogrešno je i poistovjećivanje informacijske revolucije i informacijske tehnologije jer prateće suvremene informacijske tehnologije sežu u 3.milenij pr.Kr. kada se javljaju 1.ručna računala- **abak ili abakus**)

- **Castells** - pojam informacijske tehnologije obuhvaća „konvergentni set tehnologija s područja mikroelektronike,računalstva,telekomunikacija/emitiranja te optoelektronike; ubraja i genetski inženjering i njegov sve širi skup razvoja i primjena jer je usmjeren na dekodiranje,manipulaciju te eventualno programiranje informacijskih šifri žive materije“

- u suvremenom smislu, **informacijska tehnologija je** „sprega mikroelektronike, računala, telekomunikacija i softvera koja omogućuje unos,obradu i prijenos informacija“

- sve su češći slučajevi da se mikroračunala ili njihovi dijelovi ugrađuju u različite proizvode čija prvenstvena namjena nije obrada podataka u klasičnom smislu- to su **parainformacijske tehnologije** (primjena u medicini,vojnoj industriji,prometu,industriji zabave, obrazovanju, izdavaštvu, grafičkoj industriji,kulturi i umjetnosti,procesnoj industriji)

-od parainformacijske tehnologije treba razlikovati **visoku tehnologiju** (engl.High Tech) koja obuhvaća samo najnovija otkrića na području informatičkih i komunikacijskih tehnologija

-možemo govoriti o 4 informacijske revolucije do sad

**2.1. Prva informacijska revolucija**

- ljudi se od davnina od drugih živih bića razlikuju težnjom za razvojem i međusobnim komuniciranjem

- **Bronowski: „Porijeklo znanja i imaginacije“ –** u proteklih milijun godina ljudska kultura je bila najvažniji selektivni utjecaj koji je od čovjeka stvorio ono što jest,a toga ne bi bilo bez razvoja komunikacije koja je u početku bila sadržajno i prostorno ograničenog dometa te je trebalo proći puno vremena da bi se stvorili uvijeti proširenja diljem svijeta – to je omogućila **prva informacijska revolucija** sred. 15.st.

- prva infor. revolucija počinje 1440.g., pronalaskom i upotrebom Gutenbergova tiskarskog stroja,a posebno nakon objave prve tiskane knjige 1455.g.

**2.2. Druga informacijska revolucija**

**-** obilježava ju nastanak i razvoj otkrića koja su dovela do nastanka i razvoja telekomunikacija i masovnih medija

- to razdoblje otvara Morseov telegraf 1840.g., zatim Bellov telefon 1875.g., kinematograf braće Lumiere 1895.g.,pojava Teslinog radija 1909.g. i Zworkynova ikonoskopa 1926.g. koji je otvorio put razvoju suvremene televizije

- javljaju se masovni mediji i uvodi se obvezno obrazovanje

\* Gugliermo Marconi – osnivač bežićne telegrafije (Nobelova nagrada 1909.g.), zasluge za prvi prijenos signala preko Atlantskog oceana i komercijalizacija radija

**2.3. Treća informacijska revolucija**

- počinje izumom i primjenom elektroničkih kompjutora sred. 20.st. te serije pronalazaka koji su posljednjih nekoliko desetljeća omogućili masovnu uporabu kompjutora i dr.uređaja

- usporedno s 1. i 2. informacijskom revolucijom stvaraju se preduvjeti koji ce dovesti do **mikroelektroničke revolucije**,a posebno nakon otkrića kompjutora(preduvijeti prije stvoreni)

- izumom i unapređenjem različitih strojeva ručnu obradu podataka zamjenjuje mehanička

- **Wilhelm Schichard** konstruira 1623.g. prvi računski stroj,a 20 godina kasnije **Blaise Pascal** izrađuje stroj za zbrajanje i oduzimanje,a 30ak god. nakon toga **Leibnitz** izrađuje stroj s 4 računske operacije, 50ak godina nakon javlja se **Braunov** mehanički računski stroj za komercijalnu upotrebu

- **Christopher Latham Sholes** konstruira 1867.g. pisaći stroj, nakon čega serijska proizvodnja takvih strojeva počinje u SAD-u 1874.g. I u Njemačkoj 1898.g.

- 1833.g. **Charles Babbage** razvija analitički stroj i postavlja teorijske osnove za rad suvremenih kompjutora

- **Howard Aicken** konstruira računalo **Mark 1** (1944.g.) golemih razmjera(brzo se pregrijavao)

- istovremeno, **Conrad Zuse** razvija svoj **Z3** (također relejno računalo)

- slavna trojka, **Echert,Mauchlay i von Neumann** – 1. Elektronički kompjutor: **ENIAC** (Electronic Numerical Integrator and Calculator) koji služi isključivo za znanstvene svrhe u razdoblju 1946.-1955.

- s **UNIVAC**-om (**Universal Automatic Computor**) počinje proizvodnja kompjutora za komercijalnu obradu podataka

- **prva generacija kompjutora** (1951.-1958.)-koristi se elektronskim cijevima i kablovskim vezama u obradi podataka

**- druga generacija kompjutora** (1959.-1963.)- upotreba tranzistora i tiskanih krugova s magnetskim jezgrama

**- treća generacija kompjutora** (1964.-1970.)- uvodi i razvija tehnologiju integriranih krugova, a koriste se i viši programski jezici

**- četvrta generacija kompjutora** (1971.-1987.)- integriranje poluvodičkih sklopova

**- peta generacija kompjutora** (1989.-1992.)-razvija kompjutore na osnovi paralelne arhitekture i arsenid čipova

**- šesta generacija kompjutora** (od 1993.)- usavršava neurokompjutore na osnovi neuronske mreže, primjene umjetne inteligencije i iskorištavanja ekspertnih sustava u ostvarivanju ciljeva

- taj napredak informatičke tehnologije omogućava povećanje dostupnosti informacija

- u svakoj se sredini nastoje stvoriti uvjeti za kontinuirani tehnički napredak i sve se više govori da čovječanstvo ulazi u razdoblje permanentne **znanstveno-tehnološke revolucije**

- središnje mjesto i vodeću ulogu u tom razvoju i revoluciranju ima **čip,** sićušni komadić kristala poluvodiča(ponajviše silicija) na koji se utiskuje sklop ili niz sklopova što čine elektronički integrirani krug; na njegovoj se površini od nekoliko mm utiskuju tisuće tranzistora, kondenzatora i dr. raznih elemenata

- porast moći integriranih kola dovodi do pojave i uporabe **mikroprocesora**,jednog ili nekoliko povezanih čipova koji djeluju kao samostalni kompjutor

- **Gordon Moore** - vodeći istraživač američke tvrtke Intel; uočio je da se broj tranzistora u mikroprocesoru udvostručuje svakih 18 mjeseci,a slična situacija je i s kapacitetom memorije 🡪 njegov zaključak je poznat pod nazivom **Mooreov zakon**

- sve je više aplikacija i podataka koji zahtijevaju goleme kapacitete za potrebe kompleksnih proračuna i stimulacija,pa se izlaz nalazi u povezivanju više manjih računala,koja pri tome mogu biti i fizički udaljena i povezana putem interneta 🡪 tako se javlja **GRID računarstvo:** pojam koji označava koordinirano korištenje većeg broja manjih računala i diskovnih sustava koji prema krajnjim korisnicima djeluju kao jedno veliko računalo ili mainframe

- na taj način povećava se iskoristivost postojećih resursa koji ionako nisu cijelo vrijeme u upotrebi,omogućava se njihova upotreba izvan radnog vremena,smanjuju se troškovi, koriste se standardne komponente i postiže veća fleksibilnost u radu

- 80-ih g. 20.st.-intezivan razvoj nanotehnologije koja obuhvaća istraživanje i razvoj tehnologije na atomskom,molekularnom ili makromolekularnom nivou

-istovremeno, informatičku revoluciju obilježavaju masovnost i rasprostranjenost korištenja te konvergencija,tj.povezivanje različitih informatičkih i komunikacijskih tehnologija

**2.4. Četvrta informacijska revolucija**

- početak poč. 20.st., razvojem tehnologija računalnog umrežavanja što je omogućilo povezivanja računala pomoću komunikacijskih uređaja i protokola,razmjenu podataka, dijeljenje računalnih resursa te razvoj interneta

- telefonska komunikacija se danas sve više ostvaruje posredstvom interneta – tzv. **IP telefonija**

- internet je postao platforma za svaki oblik komunikacije u današnjem društvu

- zbog velikog transformativnog utjecaja koji internet ima na društvo, 4.inf.revoluciju nazivamo **internetskom revolucijom**

**2.4.1. Razvoj i arhitektura interneta**

**a) Razvoj interneta**

- u općoj kulturi razvoj interneta se povezuje s nastankom računalne mreže ARPANET (načelno je to točno,ali i pogrešno – projekt ARPANET temeljio se na idejama i rezultatima rada brojnih pojedinaca koji su dali značajan doprinos razvoju računalnih i mrežnih tehnologija)

Rani koncepti

- **Joseph Carl Robnett Licklider** – idejni začetnik interneta

- 1962.g. je u radovima objavljenim na Massachusets Institute of Technology (MIT) iznio ideju tzv. **Galaktičke mreže** (Galactic Network) – globalne mreže preko koje će svatko moći brzo pristupiti kompjutorskim podacima i programima

- u radu „ Man-Computer Symbiosis“ je iznio ideju o **„thinking centers“** koji bi kombinirali funkcionalnosti pohrane informacija i njihove obrade (njihovim korištenjem postigla bi se veća brzina obrade informacija,a troškovi bi se dijelili)

- **Paul Baran** – poč. 60-ih g. 20.st. je objavio nekoliko radova u kojima je iznio ideju o stvaranju tzv. **distribuiranih računalnih mreža** (tada je bio zaposlenik korporacije RAND – vodeći politički i tehnološki think tank zamišljen kao potpora istraživačkim i analitičkim naporima vojske SAD-a)

- tražio se odgovor na pitanje kako osigurati mogućnost komuniciranja vojnih sustava u slučaju nuklearnog udara, a Baranov odgovor je bio u specifičnom dizajnu komunikacijske mreže

-prema njemu **računalne mreže se mogu podijeliti na**:

**a)** centralizirane

**b)** decentralizirane

**c)** distribuirane

- Baran je smatrao da centraliz. i decentraliz. računalne mreže ne mogu pružiti adekvatnu pouzdanost, iz razloga što se u slučaju prestanka funkcioniranja jednog ili više centara komunikacija može u potpunosti onemogućiti

-prema njemu,najbolje rješenje za osiguranja visoke razine pouzdanosti je izgradnja komunikacijske mreže prema distribuiranom modelu,a za ovakve mreže je moguće i matematički dokazati veću razinu pouzdanosti u slučaju kada određeni broj čvorišta prestane funkcionirati

- Baranov rad na distribuiranim mrežama je vjerovatno uzrok zablude prema kojoj je cilj ARPANET-a bio stvoriti računalnu mrežu otpornu na takve udare ( ARPANET je imao druge ciljeve,a početni napori unutar RAND-a su definirani opasnošću mogućeg ratovanja)

- internet je u visokom stupnju distribuirana mreža(utjecaj Barana)

- druga bitna ideja Baranove rasprave je ona o podijeli poruka koje se prenose mrežom na manje standardizirane dijelove,a svaki od tih dijelova može samostalno putovati mrežom te se tek na odredištu ponovno sklapaju u cjelinu

- Baranov opis tih standardiziranih paketa odgovara tehnologiji koja se danas koristi u protokolima na kojima se zasniva funkcioniranje interneta,a za tu ideju zaslužan je i **Donald Davies** koji je prvu tehnologiju opisao izrazom **„packet switching“**

**ARPA i ARPANET**

**-** 1958.g. je,u okviru ministarstva obrane SAD-a,osnovana **ARPA (Advanced Research Project Agency)**

\* ARPA 1971.g. mijenja naziv u DARPA ( Defense ARPA), vraća stari naziv 1993. i onda ponovno u DARPA 1996.g.

- **cilj ARPA-e :** provođenje dugoročnih istraživanja u području novih tehnologija (potencijalna vojna primjena)

- unutar ARPA-e je osnovan **IPTO ( Information Protection Techniques Office)** koji se bavio istraživanjem u području računalne tehnologije (na čelu Licklider)

- pod Lickliderovim vodstvom,IPTO je uspostavio suradnju s institutima za računarstvo na najuspješnijim sveučilištima SAD-a ( zbog njegova angažmana mnogi autori Lickliderov rad u ARPA-i ističu kao početak uspostavljanja inteneta)

- sveučilišta koja su surađivala s ARPA-om su imali potrebu koristiti sve više računalnih kapaciteta,ali uočavalo se i stvaranje nepotrebnih troškova (rješenje za taj problem: trebalo je međusobno povezati računala da bi istraživači na različitim institucijama mogli dijeliti resurse i raditi učinkovitije)

- plan umrežavanja relevantnih institucija u djelo počeli su pretvarati **Bob Taylor** (treći voditelj IPTO-a) i **Lawrence Roberts**

- pod njihovim vodstvom,1967. je stvoren plan s osnovnim odrednicama buduće mreže (vodilo se računa i o Baranovim idejama o decentral. mrežama i prijenosu podataka u standardiziranim paketima)

- druga ideja: računala koja se planiralo umrežiti- hostovi- ne povežu na mrežu direktno, nego putem manjeg računala(koje se nazivalo **IMP**,tj. **Interface Message Processor**) koje bi služilo kao posrednik prema mreži

- **Roberts**- temeljna prednost tog plana je da se mreža može graditi,a da ne vodi računa o specifičnostima krajnjih računala poveznih u mrežu

- spajanje pojedinih računala na IMP-ove ne bi trebao biti posao dizajnera mreže,nego vlasnika tih računala

- Roberts- u slučaju većih promjena u arhitekturi mreže, „jednostavnije je izmijeniti program u IMP-u, nego u 20 različitih računala“

- prva 4 IMP-a bila su smještena na sveučilištima UCLA,Stanford, University of California i University of Utah – međusobno se povezali u rujnu 1969.g.

- ARPANET je službeno predstavljen u listopadu 1972.g. (15 institucija u mreži tada)

- kako bi računala,povezana u mrežu,mogla komunicirati međusobno,bilo je potrebno uspostaviti zajednički komunikacijski protokol

- **protokoli su** pravila po kojima kompjutori međusobno komuniciraju unutar kompjutorske mreže,njima se određuje oblik i način prenošenja podataka putem mreže,kontrola integriteta prenesenih podataka te način obavještavanja o eventualnim greškama u tijeku prijenosa

- 1970.g. uspostavljen je **NCP (Network Control Protocol)**-1.službeni protokol za komunikaciju unutar mreže ARPANET

- ARPANET nije bila jedina računalna mreža u to vrijeme

- stvorene su drugačije tehnologije za povezivanje računala,a jedna takva,koja se zasnivala na bežičnom prijenosu podataka,koristila se unutar mreže **ALOHANET** koja je razvijena na University of Hawaii ( te mreže nisu bile povezane međusobno)

- **fizička mreža**- računalna mreža pri kojoj se svi povezani uređaji koriste istom tehnologijom i protokolom (npr.ALOHANET i ARPANET)

- ALOHANET i ARPANET su se povezale,a javljale su se ideje i povezivanja s drugim mrežama

- protokoli koji su na razini različitih fizičkih mreža riješili problem komunikacije povezanih računala su sada sami postali problem,budući da su bili međusobno nekompatibilni 🡪 problem je riješen u novom setu protokola čija je implementacija rezultirala stvaranjem interneta kao „mreže svih mreža“

Razvoj novih protokola i nastanak interneta

- s radom na novom protokolu(koji mijenja NCP) započeli su **Bob Kahn i Vinton Cerf** 1973.g. (protokol je teorijski opisan u zajedničkom radu objavljenom 1974.g.-dorađivan je)

- novi protokol se zvao **TCP (Transmission Control Protocol)**

- nekoliko godina kasnije, **Jon Postel** predlaže da se iz TCP-a izdvoji 1 set funkcionalnosti u zaseban protokol – **Internet Protocol (IP)**

- ova 2 protokola su značajan napredak prema već korištenom NCP protokolu,a oni su omogućili komunikaciju između različitih računala i fizičkih mreža

- implementacijom TCP-a i IP-a postalo je moguće bilo koju fizičku mrežu povezati s drugima

- ukupnost tih mreža danas zovemo internetom

- 1.1.1983.- ARPANET napušta stari protokol i počinje s korištenjem TCP-a i IP-a

**b) Arhitektura interneta**

- implementacijom TCP-a i IP-a definirana je arhitektura interneta(do danas nepromijenjena)

- **internet danas**- sustav računalnog umrežavanja koji se temelji na 4 sloja :

**1)** aplikacijski sloj

**2)** transportni sloj

**3)** mrežni sloj

**4)** fizički sloj

\* *vidi sliku br.2. (15.str.)*

- na svakoj od ovih razina se koriste specifični komunikacijski protokoli (svaki uređaj na rubu mreže – računalo,tablet ,pametni telefon.. – mora imati implementiran bar 1 protokol na svakoj razini,ali ovo ne vrijedi za uređaje u središtu mreže koji samo prenose podatke jer oni moraju implementirati samo odgovarajuće protokole na razini mrežnog i fizičkog sloja)

Aplikacijski sloj

- najviša razina u strukturi interneta

-na ovoj razini se implementiraju protokoli pomoću kojih međusobno komuniciraju razne aplikacije koje razmjenjuju informacije putem interneta

- internetski preglednici na računalima(npr. Chrome,Firefox,..) komuniciraju sa serverima koji sadržavaju stranice unutar **Word Wide Weba (WWW)** na temelju **Hypertext Transfer Protocola (HTTP)**

**- FTP (File Transfer Protocol)-** aplikacija zapreuzimanje datoteke s interneta

- **SMTP ( Simple Mail Transfer Protocol)** – protokol nužan za funkcioniranje e-maila

- **BitTorrent** – protokol za razmjenu datoteka preko interneta

- nekad popularan **IRC (Internet Relay Chat)** – za dopisivanje u obliku tekstualnih poruka

- svaki računalni program koji razmjenjuje podatke putem interneta koristi se aplikacijskim protokolom

- **aplikacijske protokole dijelimo na** **:**

**1)** otvorene - dostupni svima jer su njihove specifikacije javno poznate i svatko može stvarati aplikacije koje će se njima služiti

**2)** zatvorene - njihova uporaba može biti podvrgnuta ograničenjima koja postavlja onaj tko je izradio dotični protokol; koriste se samo za jednu aplikaciju te se štite pravima intelektualnog vlasništva (npr. Skype)

- primarna uloga aplikacijskih protokola je da formiraju podatke koji se razmjenjuju tako da ih druga istovrsna aplikacija može prepoznati(npr. Ako osobe A i B komuniciraju putem elektroničke pošte,tada je uloga aplikacije za komunikaciju e-poštom osobe A da poslana pošta struktuira prema pravilima protokola SMTP,koji može razumijeti aplikacija e-pošte osobe B)

Transportni sloj

- na ovoj razini djeluje manji broj protokola

- 2 najčešće korištena su **TCP** te **UDP ( User Datagram Protocol)** – TCP ima širu primjenu

- zadaća im je da preuzmu podatke od aplikacije-pošiljatelja,podijele te podatke u manje dijelove koji će se slati putem interneta,označe ih na odgovarajući način te ih proslijede na nižu razinu,gdje se obavlja sam prijenos putem mreže

- nakon prijenosa podataka do odredišnog uređaja,odgovarajući transportni protokol preuzima segmentirane podatke od protokola na nižoj razini,sastavlja ih natrag u prvobitni oblik te ih prosljeđuje odgovarajućoj aplikaciji (npr. Nakon što je primio e-poruku od odgovarajuće aplikacije za upravljanje e-poštom,transportni protokol TCP na računalu pošiljatelju tu poruku rastavlja na segmente i priprema ih za slanje putem interneta. Nakon obavljenog prijenosa,transportni protokol TCP kod primatelja e-poruke sve pojedine dijelove sastavlja u prvobitni oblik te se e-pošta dostavlja aplikaciji koja ga je u stanju prikazati korisniku)

- TCP se brine i o pouzdanosti prijenosa poruke (npr.ako neki dio poruke ne stigne na odredište,TCP će tražiti njegovo ponovno slanje)

Mrežni sloj

- aplikacijski i transportni protokoli su uvijek implementirani na krajnjim računalima koji komuniciraju putem interneta

- činjenica da se ti poslovi obavljaju na rubnim dijelovima mreže je odraz načela **end-to-end**

- daljnji posao preuzimaju protokoli na razini mrežnog sloja

-ključni protokol na ovoj razini je IP koji omogućava prijenos podataka putem mreža u obliku tzv.**internetskog datagrama**

- internetski datagram se sastoji od **podatkovnog dijela(payload) i zaglavlja**

-u podatkovnom dijelu datagrama se nalazi TCP ili UDP segment preuzet iz transportnog protokola,dok se u zaglavlju nalaze informacije potrebne IP protokolu na raznim uređajima da bi mogli uspješno prenijeti datagrame od njihova izvora do odredišta

- **primarna funcija** IP-a je adresiranje,a njome se određuje na koji način će se identificirati uređaji koji su spojeni na internet te kako će podaci putovati između krajnjih odredišta

- ključnu ulogu u ovom procesu imaju **IP adrese** – jedinstvene oznake pomoću kojih se identificiraju uređaji povezani na internet; ima je svaki uređaj koji je povezan na mrežu

- uređaji u središtu mreže,čija primarna funkcija je obavljanje prijenosa podataka između uređaja na rubovima mreže,koriste se IP adresama kako bi na najučinkovitiji način prenijeli IP datagrame od izvora do odredišta

- dva uređaja spojena na internetu ne mogu imati istu IP adresu

- prva uspješno korištena implementacija IP (**IPv4**) je IP adresu definirala kao numerički niz od 32 bita,koji se sastoji od oznake mreže i lokalne adrese uređaja unutar mreže,a takve IP adrese se sastoje od 4 dijela unutar kojih se može nalaziti bilo koja vrijednost od 0 do 255, odvojenih točkom(npr.161.53.157.13.)🡪problem: broj potencijalnih kombinacija je limitiran što IP adrese čini ograničeno dostupnim resursima

- vjerovalo se da je mogući spektar adresa u IP-u četvrte verzije dovoljan za sve buduće potrebe,ali se u praksi to pokazalo pogrešnim 🡪 u tu svrhu storen je **IPv6** u kojoj je IP adresa definirana kao 128 bitna vrijednost(npr. 2001:0db8:85a3:0042:1000:8a2e:0370:7334)

Fizički sloj

- najniža razina

- riječ je o tehnologijama kojima se podaci fizički prenose od jednog uređaja do drugoga

- u praksi se za taj prijenos koristi nekoliko različitih tehnologija prijenosa(žičanim putem, bežićno, satelitskim vezama,..)- svaka se od ovih tehnologija koristi vlasitim protokolom

- uređaji koji su povezani istim protokolom na ovoj razini tvore **fizičku mrežu**

- ograničenje fizičkih mreža – ne mogu jednostavno komunicirati s drugim fizičkim mrežama koje se ne baziraju na istoj tehnologiji (osim ako se ne uspostavi novi zajednički protokol, a to je IP)

-internet se nekad naziva „mreža svih mreža“ (internet kao mreža se zasniva na uporabi IP-a koji omogućava povezivanje različitih fizičkih mreža,pa bilo koja buduća tehnologija za prijenos podataka može postati dio interneta ako implementira protokol IP)

**Obilježja arhitekture interneta**

- to su modularnost, slojevitost i end-to-end prijenos podataka

**1) Modularnost** – takav način dizajna nekog sustava u kojem su njegovi sastavni dijelovi nezavisni u što većoj mjeri

-cilj modularnog dizajna je da smanji ovisnost između dijelova sustava

-u internetskoj arhitekturi,modularnost dolazi do izražaja kroz neovisnost protokola koji funkcioniraju na različitim razinama (protokoli funkciniraju samostalno)

**2) Slojevitost**- specifičan oblik modularnog dizajna

-načelo slojevitosti zahtijeva da moduli budu postavljeni u hijerarhijski odnos dok modularni ne postavlja nikakvo ograničenje u načinu povezivanja modula(aplikacijski sloj je na vrhu,a fizički na dnu hijerarhije)

**3) End-to-end** – zahtijeva da složenije funkcije u komunikacijskoj mreži budu koncentrirane u njenim rubovima,a da uređaji u centru mreže obavljaju samo temeljne i najnužnije komunikacijske funkcije

- unutar internetske arhitekture,to znači da je sva kompleksnost sustava koncentrirana u aplikacijskom sloju

Druge mreže temeljene na TCP i IP protokolima

- krajem 70-ih i poč. 80-ih 20.st. je nacionalna zaklada za znanost (NSF) u SAD-u podržala razvoj alternativne sveučilišne mreže,poznata kao **NSFNET**

- istovremeno,druge mreže bazirane na tehnologiji TCP/IP počele su se javljati u europskim državama

- s vremenom, NSFNET je preuzeo primat nad ARPANET-om zbog toga što je ponudio veće brzine prijenosa podataka

- ARPANET je ugašen 1989.g.(stvorene i druge mreže u to vrijeme)

- zajednička karakteristika svih tih mreža je korištenje TCP-a i IP-a(internet je ukupnost mreža koje se koriste protokolom TCP i IP-om za međusobno komuniciranje)

**c) Sustav naziva internetskih domena**

- problem prijenosa podataka je prije svega tehnološki

- prosječan korisnik interneta ne zna nakoji način se podaci prenose,ali postoji i dio arhitekture interneta koji je vidljiv korisnicima interneta,a to je **DNS (Domain Name System)**- ima razna imena: DNS,sustav domena, sustav naziva domena ili sustav domenskih naziva

- sustav naziva internetskih domena implementiran je putem protokola na aplikacijskoj razini inernetske mreže,a prema tome domenski sustav nije nužan dio arhitekture interneta

- korištenje interneta bez oslanjanja na domenski sustav bi bilo tegobno za korisnike interneta,pa je zbog toga DNS esencijalan dio internetske arhitekture

- IP adrese su učinkovito sredstvo pomoću kojeg se uređaji identificiraju 🡪 nedostatak: one za korisnika interneta nemaju nikakvo inherentno značenje (samo kad korisnik memorira adresu,on može saznati o kojoj se radi adresi)

*Primjer! : Usporedba s telefonskom mrežom i sustavom telefonskih brojeva*

*- telefonska mreža(kao i internetska) zahtijeva da svaki individualan zaključak ima jedinstvenu oznaku 🡪 ta oznaka je telefonski broj( ti brojevi nemaju inherentni smisao koji bi upućivao na koga se odnose te ih stoga nije lako ni pamtiti, ni povezati s konkretnim osobama koje se iza njega nalaze🡪 rješenje tog problema je telefonski imenik: sustav koji omogućuje povezivanje pojedinog broja s korisnikom)*

- računala povezana na ARPANET su se,također, označavala numeričkim adresama (bile su jednostavnije,ali nisu imali inherentni smisao)

- dok je broj računala povezanih u ARPANET bio mali, korisnici cu počeli stvarati popise u kojima su navodili nazive pojedinih računala u mreži i njihove numeričke adrese(nepraktično- kada su se u mrežu spojila nova računala,trebalo je ažurirati popise što je postajalo sve napornije i isti posao je obavljao velik broj pojedinaca i institucija – nije postojao srediđnji autoritet koji bi mogao ponuditi pouzdanu informaciju o identitetu svih umreženih računala)

- 1973.g. je dogovoreno da računalni centar sa Sveučilišta Stanford preuzme ulogu sastavljanja i održavanja „službenog“ popisa svih povezanih računala ( ideja je bila da se taj popis učini dostupnim putem mreže, u obliku dokumenta koji bi uvijek bio na istoj lokaciji i kojem svi mogu pristupiti putem protokola FTP)

- format tog popisa je definiran u siječnju 1974.g. – imenik je nazvan **hosts.**txt

- uvođenjem hosts.txt osigurala se pouzdanost podataka o spojenim računalima

- hosts.txt pokazuje nedostatke poč. 80-ih 20.st. (problem: rast broja računala i korisnika- kad im je broj prešao 2000)

- za dodavanje svakog novog računala trebalo je čekati da središnje tijelo ažurira popis hosts.txt

- postojeći sustav imenovanja računala je pokazao nedostatke vezane za korištenje e-pošte (adrese e-pošte su u početku imale oblik korinsik@računalo, a zbog toga je pošiljatelj morao znati korisničko ime osobe kojoj šalje poruku i oznaku računala na kojem se nalazi e-mail račun primatelja)

- od 1981.g. se intezivno rasparavlja o novom sustavu

- priznanje za razvoj sustava koji je zamijenio hosts.txt pridaje se **Paulu Mockapetrisu, Jonu Postelu, Craigu Patridgeu te Davidu Millsu** (Mills je smatrao da je hosts.txt neodrživ)

- prema Millsu,rješenje je bilo da se uvede novi tip oznake- tzv. **imenovane domene (name domain)** 🡪 njegova osnovna ideja: da se naziv računala zamijeni oznakom koja bi bolje održavala stvarne društvene odnose , u kojima su korisnici primarno povezni s institucijom, a ne s računalima,a ta oznaka je naziv domene)

- koncept naziva domena dalje su razradili **Zaw-Sing Su i Jon Postel** sred. 1982.g.

- **taj dokument je bitan iz nekoliko razloga:**

**1)** Postel i Su su definirali pojam domene kao područja nadležnosti za dodjelu naziva mreži

**2)** Su i Postel su predložili uspostavu hijerarhije domena koje bi se prostirale na više razina, ali te domene ne bi bile nedjeljive cjeline jer bi se unutar njih mogle osnivati poddomene od kojih bi svaka imala svoj naziv (individualni korisnici bi se povezali s najnižom domenom koja postoji u njihovom sustavu)

- to rješenje je omogućilo povećanje broja mogućih kombinacija kojima se identificiraju resursi na mreži (pojedini naziv mora biti jedinstven samo unutar određene domene,ali ne i unutar drugih domena)

- hijerarhija u međusobnom odnosu domena je omogućila decentralizaciju tereta dodijeljivanja naziva

- sustav naziva domena osigurava stabilnost pri označavanju resursa na internetu

- nazivi domena se povezuju s IP adresama računala(moguće je promijeniti IP adresu određenog računala i novu povezati s istom domenom,a da korisnici ne primijete ništa)

- u studenom 1983.g. **Paul Mockapetris** je definirao ključne elemente budućeg sustava za adresiranje kojeg je nazvao **DNS**

Struktura i funkcioniranje sustava domenskih naziva

- sustav domenskih naziva je uspostavljen hijerarhijski

-1. razinu DNS-a zauzimaju **vršne domene ( TLD-Top-Level Domain)** ,tj.domene 1.stupnja 🡪 to su temeljne organizacijske cjeline unutar domenskog prostora,a unutar svake od njih postoji velik broj domena 2.stupnja,tj. **Sekundarnih domena ( SLD, Second-Level Domain)** koje su poddomene vršnih(i unutar sekundarnih se mogu stvarati poddomene)

- iako DNS omogućava stvaranje do 127 razina poddomena,najčešće u praksi su 3 do 4

- pojam **„naziv domene“** može imati 2 značenja:

**1)** može se raditi o nazivu 1 konkretne domene na 1.stupnju domenskog sustava ili na nekom od nižih stupnjeva

**2)** može se raditi o jedinstvenoj oznaci određene domene,tako da se navede ta domena i nazivi svih njoj nadređenih domena (tu govorimo o **potpunom nazivu domene- Fully Qualified Domain Name,FQDN**)

-nazivi domena pišu se s lijeva na desno,od nižih prema vršnoj

*Primjer! :* [*http://knjiznica.pravo.unizg.hr*](http://knjiznica.pravo.unizg.hr)*.*

*- vršna domena je „ .hr“ – nacionalna vršna domena RH*

*- unutar nje je sekundarna domena(koja pripada Sveučilištu u Zagrebu),a glasi „ unizg“*

*- Pravni fakultet je sastavnica Sveučilišta u ZG te se njegov domenski prostor nalazi unutar sveučilišnog,na tercijarnoj domeni „pravo“*

*- knjižnica PF-a kao organizacijska cjelina ima vlastiti domenski prostor,koji se nalazi unutar fakultetskog, na domeni „knjiznica“*

- pojedinu domenu ne možemo identificirati ako ne navedemo i naziv svih njoj nadređenih domena

Vršne domene

- predstavljaju najvišu razinu u hijerarhiji internetskog domenskog prostora

- **dijele se u 2 kategorije:**

**1) nacionalne vršne domene** (Country Code Top-Level Domain,ccTLD)- one koje se dodijeljuju pojedinim državama ili njihovim entitetima(npr. .hr ( Hrvatsku), .eu (Europska Unija), .de (Njemačka)..) 🡪 1 država može dobiti 1 vršnu domenu

**2) generičke vršne domene** ( Generic Top-Level Domain,gTLD)- sve koje nisu nacionalne, njihov broj se dugo vremena nastojao držati ograničenim

- prvih 7 generičkih domena je uspostavljeno u procesu pokretanja DNS-a sred.80-ih 20.st. : .com, .org, .net, .edu, .gov, .mil, .int (jedine generičke domene do 2000.g. kad je uvedeno 7 novih: .aero, .biz, .coop, .info, .museum, .name, .pro)

- 2003.g. : .asia, .cat, .jobs, .mobi, .tel, .travel

- 2009. i 2011.g. : .post i .xxx ( do kraja 2011. Ukupno 22 generičke domene uvedene)

- do lipnja 2015.g. odobreno je njih 639

- **generičke domene se dijele na:**

**a) otvorene generičke vršne domene**

- to su regulirani internetski prostori

- to su one domene unutar kojih poddomenu može steći bilo koja pravna ili fizička osoba, bez bilo kakvih ograničenja s obzirom na državnost,djelatnost kojom se bavi i sl.

- jedini zahtjevi koji se postavljaju pri stjecanju ovih domena su da korisnik pristane na uvijete korištenja te da plaća propisani iznos na ime registracije domene( .com, .org, .net, .info, .biz)

- .com, .org, .net su najpoznatije,ali i prve implementirane domene(iz sred.80-ih 20.st.)

- registracija poddomena unuta ovih domena je u potpunosti slobodna za svaku osobu

- domena .com je izvorno bila namijenjena za komercijalne svrhe, .net je trebao služiti pružateljima raznih mrežnih usluga,a .org je zamišljena kao domena opće kategorije,za organizacije koje nisu spadale u neku drugu od predviđenih kategorija

- .com je najpopularnija domena na internetu koja je u 2014.g. obuhvaćala više od 115.600,000 sekundarnih domena

- domena .biz je jedna od 7 novih generičkih vršnih domena koje je ICANN odabrao 2000.g. (registarcija je u .biz moguća za svaku osobu, pri čemu ne postavlja nikakva teritorijalna ili personalna ograničenja; jedino ograničenje je ono prema kojem se poddomene unutar nje moraju koristiti ili biti namijenjene za korištenje u „bona fide poslovne ili trgovačke svrhe“

- .info se od ostalih razlikuje po tome što je o početaka definirana kao otvoreni gTLD,dok su .com,.org i .net to postale faktičkim putem

**b) sponzorirane generičke vršne domene**

- njima upavlja određena sponzorska organizacija koja propisuje uvjete registracije sekundarnih domena

- najstarije su .gov, .mil, .int

- **domena .gov** je pokrenuta 1984.g.,a mogućnost registracije sekund. domena unutar nje imaju samo tijela savezne vlasti te ona iz pojedinih saveznih država i lokalnih jedinica u SAD-u

- i **domena .mil** je prisutna od samih početaka DNS-a,a njegovo korištenje moguće je samo za različite subjekte povezane s ministarstvom obrane SAD-a

- **domena .int** je pokrenuta 1988.g.,a dostupna je samo međunarodnim organizacijama koje su zasnovane na međunar. ugovoru i smatraju se valjanim subjektima međunarodnog prava

- sve 3 domene imaju strog režim registracije,tako da nisu pretjerano relevantne kada je riječ o korištenju domenskog prostora od privatnopravnih subjekata

- s vremenom je pokrenut veći broj sponzoriranih domena koje su u slobodnijem režimu korištenja,ali i dalje imaju više ograničenja nego otvorene generičke vršne domene 🡪 to uvođenje je rezultat tendencije liberalizacije internetskog domenskog prostora

- s vremenom se pokazalo da bi bilo korisno otvoriti mogućnost registracije i unutar drugih naziva kojim bi se koristili kao vršnim domenama,a tome je doprinijela i činjenica da se broj registriranih poddomena unutar .com vršne domene znatno povećao,pa je logično bilo otvoriti nove domenske prostore

- domena .areo je namijenjena za poslovne subjekte iz zrakoplovne industrije, .asia služi potrebama korisnika iz Azije,Australije i Pacifika, .cat služi za subjekte koji se povezuju s katalonskim jezikom i kulturom

- nakon što je ICANN 2012.g. omogućio stvaranje vršnih domena za privatnopravne subjekte,u **root zonu** domenskog prostora dodano je preko 650 novih vršnih domena (tako su npr. .golf, .date, .news, .tech, .casino, .style,.. postale vršne domene)🡪 ovakve domene imaju nazive općeg značenja,njima upravljaju od ICANN-a ovlaštene sponzorske organizacije koje nude poddomene unutar ovih vršnih domena pojedinim gospodarskim subjektima uz naknadu

- neke kompanije su odlučile registrirati i vršne domene kojim će se koristiti samo za vlastite potrebe s ciljem izgradnje kvalitetnih servisa za odnose sa svojim potrošačima (.cisco, .microsoft, .windows, .bbc)

Načela registracije poddomena unutar generičkih vršnih domena

- nazivi domena su se počeli registrirati tako da se domena dodjeljivala onom subjektu koji bi je prvi zatražio – to je pravilo **first come,first served** ( tko prvi,domena njegova)

- načelo first come,first served je jednostavno i lako primjenjivo,ali ako se ono primjeni kao jedini kriterij,može doći do nekih drugih problema

- u slučajevima kada se ne provjerava imaju li osobe,koje registriraju nazive domena, odgovarajuće pravo na korištenje naziva koji se unosi u domenu, moguće su zloupotrebe do kojih dolazi kada domenu registrira osoba koja nema nikakvo pravo za korištenjem,prilikom čega dolazi do sporova o nazivima domena

- u nekim domenama se provode registracije poddomena po fazama,a najčešće se razliku **3 faze:**

**1) sunrise** – pravo na registraciju poddomena imaju samo nositelji određenih zaštićenih naziva,primjerice žigova ili tvrtki

**2) landrush** – omogućava se registracija bilo kojeg naziva domene koji prije nije registriran i tu se ne koristi načelo first come,first served,nego se svi zahtjevi za registraciju spremaju te se o njima odlučuje po nekom drugom kriteriju na kraju landrush faze (npr. jedna od metoda kojom se ponekad koristi je **aukcija**-u slučaju da više osoba želi registrirati isti naziv domene, on se dodjeljuje onome tko ponudi najveći iznos kao cijenu registracije)

**3) otvaranje domene po načelu first come,first served** – svi preostali nazivi domena se registriraju po tom načelu

Posebno o nacionalnoj vršnoj domeni RH

- 27.2.1993. – RH dobiva svoju vršnu domenu ( **.hr** ) koju IANA uvrštava u DNS root zonu, a upravljanje njome je prepustila **Hrvatskoj akademiji i istraživačkoj mreži (Croatian Academic and Research Network, CARNet)**

- 1998.g. je (prema CARNet-ovim podacima) bilo registrirano 1378 poddomena unutar .hr

- u lipnju 2015.g. registrirano je 89094 poddomena

- pravila registracije i korištenja poddomena unutar .hr vršne domene sadržana su u **Pravilniku o ustrojstvu i upravljanju vršnom nacionalnom internetskom domenom** donesenom 2010.g.

- Pravilnik 2010 definira .hr domenu kao element nacionalne prepoznatljivosti i nacionalnog bogatstva te kao polazište strukturiranja,organizacije i prezentacije informacija vezanih uz RH na internetu (upravljanje vršnom domenom je djelatnost općeg interesa)

- Pravilnik 2010 se temelji na ideji da svaka pravna i fizička osoba ima pravo na „prisutnost i opstanak u virtualnom prostoru“ zbog čega im se daje pravo da bez naknade registriraju 1 domenu,a fizičke i pravne osobe imaju uz naknadu pravo registrirati dodatne domene

- ali, fizičke i pravne osobe nisu u potpunosti izjednačene kada je riječ o pravu na registraciju domena ( sukladno **čl.18. Pravilnika 2010**, pravna osoba može biti nositelj registracije najviše 10 domena; fizičke osobe imaju pravo na registraciju najviše 2 domene)

Registracija domena

- **čl. 10. Pravilnika 2010** postulira pravo prema kojem se prednost daje onom zahtjevu koji je prije zaprimljen(ako zahtjeve postavi više osoba),a isto određuje i **čl. 14/3. Pravilnika 2010** koji određuje da se o zahtjevima za registraciju odlučuje redoslijedom zaprimanja

- proces registarcije provodi se elektroničkim putem,pri čemu se određene domene registriraju izravno kod CARNet-a,a neke se registriraju putem drugih ovlaštenih registra

- CARNet registrira osnovne (besplatne) domene za ostvarivanje virtualnog identiteta pravnih osoba,registriranih samostalnih djelatnosti,domene državnih tijela i jedinica lokalne i područne samouprave te domene fizičkih osoba

- naplatne domene registriraju se putem ovlaštenih registra(gospodarskih subjekata koje je CARNet ugovorom ovlastio na obavljanje poslova registracije .hr domena)

Zabrana zlouporabe prava i zaštita stečenih prava

- **čl. 9. Pravilnika 2010** sadrži temeljno pravo,prema kojem su korisnici domena dužni postupati sukladno načelu savjesnosti i poštenja te se suzdržavati od zlouporabe domena

- u slučaju kršenja ove obveze, CARNet je ovlašten uskratiti registraciju domene,brisati domenu ili je privremeno deaktivirati

- **čl. 12. Pravilnika 2010** obvezuje CARNet da štiti prava korisnika domena te da registrirane domene ne briše prije isteka registracije

Raspolaganje domenom i prestanak prava na korištenje domenom

- osoba koja registrira domenu unutar .hr nije njen vlasnik nego samo ima određena korisnička prava

- korisnik može rabiti svoju domenu neograničeno dugo,pod uvjetom da redovito obnavlja registraciju te ispunjava uvjete propisane pravilnikom

- **čl. 28/1. Pravilnika 2010** – jedno od ključnih ograničenja prava korisnika domene je ono prema kojem korisnik nema pravo prenijeti registriranu domenu na drugu osobu

- **čl. 28/2. Pravilnika 2010** – ako se utvrdi da se domenom koristi osoba koja nije njen registrirani korisnik,CARNet je ovlašen odrediti njeno brisanje

- **čl. 28/3. Pravilnika 2010** – jedina mogućnost za prijenos prava korištenja domene na drugu osobu je u slučaju smrti,prestanka postojanja,statusnih ili drugih pravnih promjena na strani korisnika domene; u takvim slučajevima,domena se briše te se istovremeno provodi nova registracija na pravnog slijednika korisnika ili osobu koju je on odredio; slijednik ili osoba koju je odredio prijašnji korisnik ima pravo prednosti na registraciju iste domene koje traje 6 mjeseci

- pravo na korištenje domenom prestaje prestankom postojanja njezinog korisnika ili brisanjem domene na temelju neke druge odredbe Pravilnika 2010

-najčešće,pravo na korištenje domenom prestaje uslijed neplaćanja naknade za njezino korištenje

- kako određuje **čl. 30/3. Pravilnika 2010**, ako korisnik domene ne plati naknadu za sljedeće razdoblje korištenja u roku od 60 dana od isteka prethodne registracije,domena će se brisati

- pravo na korištenje domenom može prestati i na temelju arbitražne odluke u slučaju spora o nazivu domene

Proces razlučivanja domena

- DNS omogućava korisnicima interneta da se oslanjaju na nazive domena kao oznake za identificiranje resursa na interneta

- IP zahtijeva da se ti isti resursi identificiraju putem IP adresa,a iz toga slijedi da je svaki naziv domene potrebno pretvoriti u IP adresu prije nego što se može ostvariti komunikacija

- proces pretvaranja naziva domena u IP adrese se naziva **razlučivanje(domain name resolution ili resolving)** 🡪odvija se automatski između uređaja koji su spojeni u mrežu te je u potpunosti nevidljiv za korisnike interneta

- proces razlučivanja se temelji na interakciji između tzv**. DNS klijenata** (domain name resolver,razlučitelj) i DNS servera

-svaka internetska domena mora imati jedno centralno računalo- **DNS server ili Name Server** (nužno raspolaže IP adresama svih računala koje se nalaze unutar njegove domene)

- u slučaju da domena ima poddomene,ključno je za funkcioniranje sustava domenskih naziva da DNS server pojedine domene rapolaže IP adresama svih DNS servera njenih poddomena

- DNS server se smatra autoritativnim,a može imati i podatke o IP adresama drugih računala, ali se u pogledu njih se ne smatra autoritativnim

- ako pretpostavimo da korisnik interneta želi pristupiti sadržaju na adresi pravo.unizg.hr, javlja se pitanje **kako se obavlja pretvaranje ovog naziva domene u IP adresu**

- **prvi korak** u procesu pretvaranja naziva domene je da DNS klijent na strani uređaja koji rabi korisnik interneta šalje odgovarajući zahtjev svom DNS-serveru(da bi to funkcioniralo, pretpostavka je da DNS klijent ima pristup bar jednom DNS serveru)

- u slučaju da je kontaktirani DNS server autoritativan za tu domenu,on će jednostavno vratiti DNS klijentu traženu IP adresu(npr. ako korisnik koji želi pristupiti web-stranici pravo.unizg.hr to čini s računala na Pravnom fakultetu,čitav proces pretvaranja naziva domene u IP adresu će se odviti samo posredstvom DNS servera na toj instituciji)

- puno je češća situacija u kojoj DNS server nije autoritativan za traženu domenu (pretpostavimo da se radi o korisniku iz SAD-a,koji koristi usluge lokalnog pružatelja pristupa internetu; u tom slučaju DNS server tog pružatelja usluga neće sam raspolagati podatkom koja IP adresa odgovara traženoj domeni)

- daljnji razvoj ovisi o tome koristi li se sustavom **rekurzivnog ili iterativnog pretvaranja**

- u sustavu **rekurzivnog pretvaranja** naziva domene,DNS server koji je kontaktirao DNS klijent mora sam pribaviti traženu IP adresu i vratiti je klijentu

- lokalni DNS server će proći cijeli postupak pretvaranja naziva domena,od vršnih prema nižim

- da bi pretvorio domenu pravo.unizg.hr u odgovarajuću IP adresu,taj server će najprije morati saznati IP adresu DNS servera koji je nadležan za „.hr“ vršnu domenu

- podatke o DNS serverima vršnih domena imaju **tzv. root serveri**,koji predstavljaju najvišu točku u hijerarhiji interneta

- lokalni DNS server kontaktira neki od root servera i od njega dobije informaciju koja je IP adresa DNS servera nadležnog za „.hr“ vršnu domenu

- lokalni DNS server kontaktira DNS server za „.hr“ domenu,od kojeg dobije IP adresu DNS servera nadležnog za domenu „.unizg“

- jednak korak se onda ponavlja u pogledu domene „.pravo“ koja je poddomena od „.unizg“

- jednom kada dobije adresu računala na domeni „pravo.unizg.hr“ lokalni DNS server korisnika interneta će je proslijediti DNS klijentu,koji će je iskoristiti za ostvarivanje komunikacije

- sustav **iterativnog razlučivanja** se razlikuje od rekurzivnog po tome što u njemu zadatak kontaktiranja DNS servera za domene na različitim razinama pada na DNS klijenta korisnika interneta,a ne na njegov lokalni DNS server

- u ovom slučaju, lokalni DNS server će DNS klijentu dati najbolji podatak kojim raspolaže, nakon čega će DNS klijent morati obaviti daljnju komunikaciju sa serverima na nižim razinama i na taj način sam doći do tražene IP adrese

-u praksi se ova 2 razlučivanja kombiniraju,pa tako DNS klijent od svog DNS servera zahtijeva IP adresu na rekurzivan način,a taj server od servera nadležnih za druge domene taj podatak dobiva iterativnim putem

- da se poboljšava učinkovitost mreže,DNS serveri često podatke o nazivima domena i odgovarajućim IP adresama koje dobiju u odgovoru na određeni upit pohranjuju određeno vrijeme u privremenu memoriju,pa ih u tom slučaju mogu jednostavnije proslijediti klijentima,a da u svakom pojedinom slučaju iznova ne provede čitav postupak razlučivanja

**d) WWW i drugi internetski servisi**

- internet je modularan i hijerarhijski organiziran informacijsko-komunikacijski sustav u kojem se razne funkcionalnosti ostvaruju na različitim razinama

- slojevitost interneta ima za posljedicu to da se sve aktivnosti koje se ne moraju obaviti na nižim razinama prebacuju na one više (aplikacijski sloj-tu se obavlja najviše funkcionalnosti,a i najvidljiviji je)

- **internetski servisi su** funkcionalnosti interneta koje se razvijaju na aplikacijskoj razini (u tom kontekstu se govori o WWW-u, e-pošti, Skypeu,Google Hangoutsu,..)

- WWW je najpoznatiji i najkorišteniji internetski servis

- WWW je razvijen na europskom istraživačkom institutu **CERN** poč. 90-ih 20.st. –ključna osoba za njegov razvoj je **Tim Berners-Lee** koji je 1990.g. zajedno s **Robertom Cailliauom** na CERN-u iznio prijedlog za pokretanje tzv. **„HyperText projekta“**

- motivacija za stvaranje hipertekstualnog sustava je bila u činjenici što je CERN rasposlagao mnoštvom informacija,sadržanim u računalnim dokumentima u različitim formatima

- tim informacijama nije moguće uvijek jednostavno pristupiti zbog nekompatibilnosti računalnih sustava i programa koji su se koristili za obradu🡪rješenje (osmislili su ga Berners-Lee i Cailliau) je u uporabi hiperteksta,pod čime su smatrali specifičan način povezivanja dokumenata

- u hipertekstualnom okruženju, dokumenti mogu sadržavati poveznice-linkove-na druge takve dokumente, što omogućuje jednostavnu navigaciju između njih

- hipertekstualni dokumenti se strukturiraju prema pravilima poznatima kao **HTML (Hyper Text Markup Language)**

-HTML je standardni format hipertekstualnih dokumenata (prve verzije ovog formata sežu u rane 90-te 20.st.,autor je Tim Berners-Lee, prva standardizirana verzija je HTML 2.0 objavljena 1995.g.,danas je u uporabi HTML standard pete generacije)

- dokumenti na WWW-u se označavaju uporabom jedinstvenih oznaka koje se zovu **Uniform Resource Locators (URL)**-sastoji se od oznake http,naziva domene na kojoj se nalazi dokument i oznake tog sadržaja unutar računalnog sustava,koji je smješten na toj domeni

*Primjer! URL* [*http://www.pravo.unizg.hr/PI*](http://www.pravo.unizg.hr/PI)

*- „http“ je oznaka aplikacijskog protokola, „www“ upućuje da se radi o sadržaju World Wibe Weba, „pravo.unizg.hr“ je naziv domene,a „PI“ upućuje na konkretni dokument u formatu HTML na kojem su sadržane određene informacije(u ovom slučaju Katedre za pravnu informatiku)*

- naziv domene je od oznake konkretnog dokumenta na serveru odvojen kosom crtom (/)

- korisnici interneta sadržajima na WWW-u pristupaju:

1) izravno putem naziva internetskih domena ili URL-ova

2) putem linkova s drugih web-odredišta

3) posredstvom internetskih pretraživača

- koju će opciju korisnik upotrijebiti,ovisi o nekoliko okolnosti,uključujući tu njegove preferencije,pitanje je li mu poznato gdje se nalazi sadržaj koji traži i sl.

*Primjer! Korisnik interneta koji često pristupa društvenoj mreži Facebook ili servisu za razmjenu videosadržaja YouTube vjerovatno će znati da se oni nalaze na domenama facebook.com i youtube.com,te će im pristupiti unošenjem odgovarajućeg naziva domene u internetski preglednik računala. U nekim slučajevima,korisnik interneta neće znati na kojoj domeni se nalazi sadržaj koji mu je potreban,pa će pokušati pogoditi naziv domene. (npr. osoba koja želi pristupiti web-odredištu tvrtke XYZ može pretpostavljati da se traženi web-sadržaj nalazi na domeni xyz.com ili nekoj trećoj, unijeti dotičnu adresu u internetski preglednik i nadati se da će je ona odvesti na pravo odredište)*

- drugi način kojim se pristupa sadržajima na WWW-u su linkovi na web-stranicama,koji upućuju na druge stranice

- ključno svojstvo hiperteksta je da može sadržavati poveznice na druge dokumente u hipertekstualnom formatu(korisnici WWW-a se oslanjaju na te poveznice,tj.linkove)

-najčešće korisnik interneta neće znati niti će htjeti pogađati na kojoj internetskoj domeni se nalazi sadržaj koji mu je potreban(slična situacija je kada korisnik zna naziv domene,a ne zna URL dokumenta koji traži)🡪pretpostavlja se da će korisnik koristiti internetski pretraživač

**e) Internetski pretraživači**

- WWW odlikuje informacijama iz svih aspekata društvenog života(količina inf. se povećava)

- iako na tržištu internetskog pretraživanja djeluje velik broj poduzetnika,najveći dio tržišta kontrolira samo nekoliko kompanija (npr. Google drži 2/3 ukupnog tržišta)

- prosječan korisnik nije upoznat ni s procesom odabira web-odredišta kao rezultata pretraživanja,niti s ekonomskim aspektima svake pojedine transakcije

**1)** prvi i nužni korak da bi internetsko pretraživanje bilo moguće je **indeksiranje sadržaja**

- taj proces se odvija prije nego što korisnik interneta inicira postupak pretraživanja, tj. indeksiranje sadržaja je proces u kojem se internetski pretraživači koriste specifičnim računalnim programom (engl. crawler),koji pregledava sadržaj svih web-odredišta do kojih može doprijeti,kopira taj sadržaj i pohranjuje ga u svoju bazu podataka(indeks)

**2)** u drugom koraku,korisnik usluge internetskog pretraživača započinje proces pretraživanja tako da na web-odredištu pretraživača definira svoj **upit** (engl. query)

- pojmovi koje korisnik unosi su rezultat njegovog subjektivnog osjećaja o tome koje riječi će rezultirati najtočnijim rezultatima(korisnik može i griješiti)

**3)** u trećem koraku,pretraživač uspoređuje upit korisnika sa sadržajem svih web-odredišta koje je prethodno indeksirao te **odabire rezultate** koje će prikazati korisniku

- to je ključna faza u procesu pretraživanja jer o njoj ovisi u kolikoj će mjeri biti ostvareni interesi svake od strana koje su uključene u proces pretraživanja

- **odabir rezultata pretraživanja se svodi na 2 procesa :**

**a)** pretraživač provjerava koja web-odredišta zadovoljavaju parametre definirane u upitu (ona kod kojih to bude,pojavit će se u rezultatima pretraživanja)

**b)** pretraživač rezultate koje je prethodno odabrao rangira prema njihovoj procijenjenoj relevantnosti u odnosu na upit,tj. pretraživač nastoji utvrditi koju informaciju korisnik pokušava pronaći)

- proces odabira i rangiranja rezultata je u potpunosti automatiziran ( u praksi to znači da internetski pretraživači razvijaju algoritme koji imaju za cilj odrediti najrelevantnije rezultate)

- algoritmi,prema kojima se vrši rangiranje , su tajni,ali ipak su neki od osnovnih kriterija na koje se pretraživači oslanjaju poznati javnosti (npr. Google uzima u obzir mjesto gdje se nalazi traženi pojam ili broj linkova koji vode na pojedino web-odredište s drugih odredišta)

**4)** u četvrtom koraku, jednom utvrđena i sortirana lista rezultata pretraživanja se prezentira korisniku – ti rezultati se nazivaju **prirodni rezultati pretraživanja** (engl. natural results)

- ovi rezultati se prikazuju kao niz linkova koje u pravilu prati i manja količina teksta s web-odredišta na koje ti linkovi vode

- ključna osobina prirodnih rezult. pretraž. je njihova objektivnost, odnosno nepristranost

- **pod „objektivnošću“** prirodnih rezult. pretraž. se podrazumijeva samo to da bolji rang pojedinog web-odredišta nije moguće „kupiti“, budući da on ovisi isključivo o izračunu na temelju algoritma sadržanih u pretraživaču,a s ciljem da se korisnicima daju rezultati koji su procijenjeni kao najrelevantniji

- u kojoj će mjeri ti rezult. biti najrelevantiniji, ovisi o sposobnosti korisnika da kvalitetno definira svoj upit te kvaliteti algoritma na temelju kojih se odabiru i sortiraju rezultati

- u pogledu rezultata pretraživanja interneta različiti subjekti imaju različite interese,a moguće je govoriti o interesima pružatelja sadržaja na WWW-u, interesima korisnika usluge pretraživanja te o interesima samih pretraživača

- subjekti koji upravljaju web-odredištima(pružatelji sadržaja) imaju interes da na svoja odredišta privuku što više korisnika interneta,a to čine tako da povećaju vidljivost web-odredišta na internetskim pretraživačima

- metode kojima se postiže da neko web-odredište bude bolje plasirano u rezultatima pretraživanja se zovu **Search Engine Optimization (SEO)**

- **SEO se temelji na 2 elementa:**

**1)** pokušava se razumjeti na koji način intern. pretraživači funkcioniraju i koje faktore uzimaju u obzir pri odabiru rezultata pretraživanja i njihovom rangiranju

**2)** web-odredište se ciljano prilagođava tako da se ističu oni faktori koje pretraživači uzimaju u obzir,kako bi ono bilo bolje rangirano u rezultatima pretraživanja

- internetski pretraživači se prema SEO-u odnose dvojako

- oni oblici optimiziranja web-odredišta koji pridonose mogućnosti pretraživača da pravilnije procijeni njegovu relevantnost(tu se ubraja jasno strukturiranje sadržaja,korištenje pojmova koji najbolje opisuju sadržaj u naslovima) u pravilu se potiču

- pokušaji umjetnog podizanja ranga nekog web-odredišta u nekim slučajevima sankcionirali se se njegovim smanjivanjem ili čak izbacivanjem iz indeksa pretraživača

- **cilj korisnika usluge pretraživanja** je da dobiju rezultate koji upućuju na web-odredišta koja objektivno i u najvećoj mjeri odgovaraju njihovim potrebama

- za korisnike usluge pretraživanja su idealni rezultati oni koji su nepristrani,u smislu da se internetski pretraživač pri njihovom formiranju vodi isključivo najboljim interesom svojih korisnika

- **pristrani rezultati** su oni pri kojima bi internetski pretraživač favorizirao određenog pružatelja sadržaja iz razloga koji ne odražavaju najbolji interes korisnika

- **internetski pretraživači** u načelu dijele interes svojih korisnika za nepristranim rezul.pretr. 🡪 razlog za to je u činjenici što njihov poslovni uspjeh ovisi o broju korisnika njihovih usluga

- pretraživači moraju komercijalizirati svoja ulaganja te nastoje stvoriti profit iz usluge koju pružaju (nastoje zaraditi putem oglasa)

**2.4.2 Pojam i uloga interneta danas**

- internet definiramo kao globalnu informacijsko-komunikacijsku mrežu, koja u biti jest skup međusobno povezanih računalnih mreža,a ključna karakteristika svih tih mreža je da se koriste zajedničkim protokolima(TCP i IP) za prijenos podataka

- arhitektira interneta omogućava da se na aplikacijskoj razini mreže razvijaju razni internetski serveri čija je ukupnost,kao i činjenica da je velik broj njih slobodan te besplatan za korištenje, učinila internet najznačajnijim inf.-komunik. sustavom u povijesti čovječanstva

- trenutno se internetom koristi više od 3 milijarde ljudi(40% populacije) i taj broj raste

- očekuje se da će br. korisnika u 2015.g. rasti za oko 8% u odnosu na 2014.g.,a to će biti prvi put od njegova nastanka da je br. korisnika rastao po stopi manjoj od 10% godišnje (od 1995. do 2000.g. broj korisnika se udeseterostručio, od 2000. do 2010.g. se povećao za oko 5 puta, dok se od 2010.g. do danas povećao za oko 50%)

- relativni br. koris. interneta u ukupnoj populaciji je veći u razvijenim državama,tj.regijama

- razlike među pojedinim regijama uočavamo ako kombiniramo podatke o broju kućanstava koji imaju vezu na internet(prednjači Europa,pa slijede SJ i J Amerika), broju individualnih korisnika(Europa najviše,Afrika najmanje), korištenju mobilnim i fiksnim širokopojasnim (broadband) pristupom mreži(Europa najviše,Afrika i Arapske države najmanje)

- razlike se očituju i ako se podaci grupiraju po stupnju razvoja pojedine države

- postoji digitalni jaz između pojedinih država i regija,pa se kao prioritet postavlja razvoj internetske infrastrukture u manje razvijenim državama

- **podaci o RH** (prema Eurostat iz 2014.g.) : 68% kućanstava ima pristup internetu( RH među manje razvijenim državama EU,ali značajno iznad svjetskog prosjeka-46%)

- dostupnost informacija putem interneta utječe na povećanje znanja kao osnova kvalitetnijeg upravljanja i odlučivanja

- WWW je najkomercijalniji dio interneta

- tijekom razvoja interneta profilirale su se razne aktivnosti i funkcije koje se odvijaju putem njega,**a najčešće su:**

**a)** **prikupljanje,pohrana i dohvat inf**. te jednostavnija i brža razmjena podataka(FTP,WWW..)

**b)** **posredna i neposredna komunikacija**(e-pošta,UseNet,forumi,blogovi,socijalne mreže,..)

**c) elektroničko poslovanje** (e-trgovanje,e-bankarstvo,e-marketing,e-pravosuđe,e-uprava..)

**d) elektroničko učenje i obrazovanje** (suvremeni oblik edukacije i komunikacije,neovisan o prostoru i vremenu,koji se ostavruje korištenjem inf.-komunikacijskim tehnologijama)

- velika očekivanja se polažu u daljnju konvergenciju interneta i drugih informacijskih i parainformacijskih tehnologija,pa se zbog toga često koristi naziv **Internet stvari ( IoT, Internet of Things)**, tj.povezivanje raznih neovisnih uređaja putem internetskih tehnologija, omogućavajući njihovu kontrolu,praćenje i pružanje usluga daljinski

- internet stvari pokriva 3 vrste komunikacije koja se može uspostaviti u ograničenom okružju **(„Intranet stvari“)** ili učiniti javno dostupnima („Internet stvari“) : stvari s ljudima, između stvari ili između uređaja ( **M2M, machine to machine** )

**2.4.3. Upravljanje internetom i regulacija interneta**

- **Manuel Castells-** „sva ključna tehnološka dostignuća koja su dovela do interneta nastala su oko vladinih institucija,velikih sveučilišta i razvojnih centara. Korijeni interneta nisu u poslovnom svijetu. Bila je to prenapredna tehnologija,preskup projekt i prerizičan potez da bi ga započele organizacije okrenute zaradi“

- u razvoju interneta,presudnu ulogu je odigrala akademska zajednica(do sred. 90-ih 20.st. internet je bio skup poveznih računalnih mreža kojim se koriste primarno akademske instit.)

- internet se razvija procesima koji se temelje na neformalnoj koordinaciji velikog broja raznih dionika,a u takvom okruženju stvari funkcioniraju po ad hoc principu,nego što su rezultat osmišljenog plana razvoja(rjetko se postavljalo pitanje tko je nadležan za uređivanje nekog područja,a važno je bilo funkcionira li predloženo rješenje)

- taj način izgradnje sustava,koji se temelji primarno na konsenzusu, je suprotnost formalnom procesu odlučivanja kakav je prisutan u državnim strukturama (rana internetska zajednica je svoj model funkcioniranja smatrala superiornim drugim,formaliziranim procesima donošenja odluka)

- mnogi pojedinci su bili sumnjčavi prema državnim strukturama te su internet vidjeli kao područje koje bi trebalo funkcionirati po vlastitom setu vrijednosti i pravila,slobodno od normi koje bi nametala bilo koja nacionalna vlast

- te ideje su formulirane u **„Deklaraciji o neovisnosti kiberprostora“** koju je 1996.g. napisao **John Perry Barlow** (ta deklaracija je idejni manifest,nema nikakvu pravnu relevantnost,ali ipak jasno odražava stav koji je u internetskoj zajednici neko vrijeme vladao o pitanju regulacije interneta)

- ona odbacuje suverenitet države nad kiberprostorom,a ta ideja se dijelom temeljila na shvaćanju o internetu kao zasebnom prostoru

- ideja o tretmanu interneta kao područja koje se nalazi izvan pojedinih država je neko vrijeme bio izražen u pravnoj znanosti,pa su tako neki autori zastupali tezu da je kiberprostor sličan onome fizičkome,samo nije omeđen geografskim granicama nego „ekranima i lozinkama“( potrebno je stvoriti institucije i pravne norme koje bi uređivale taj prostor)

- te sve ideje nisu zaživjele,nego se dogodilo suprotno - gotovo sve države svijeta su počele pravno normirati razne aktivnosti povezane s upotrebom interneta,tj. nisu se ostvarili planovi da postoji zasebno i ujednačeno internetsko pravo u pogledu računalnog kriminaliteta, e-trgovine,privatnosti,slobode izražavanja,itd.

- države svoje postojeće režime protežu i na internet pri čemu se nerijetko donose posebna pravila u pojedinim područjima koja se tiču interneta,ali i tada su ta pravila dio pravnog poretka pojedine države,a ne autonomno „internetsko“ pravo (jedina iznimka od ovog rješenja su pravila koja reguliraju stjecanje i korištenje nazivom domena unutar područja generičkih vršnih domena)

Pojam upravljanja internetom(Internet Governance)

- u engl. se često koristi naziv Internet Governance za upravljanje i regulaciju interneta

- 2005.g. na drugom **Svjetskom summitu o informacijskom društvu(WSIS),** pojam **Internet Governance** označava proces u kojem „Vlade,privatni sektor i civilno društvo.. razvijaju i primijenjuju zajednička načela,norme,pravila,postupke odlučivanja i programe koji utječu na razvoj i korištenje internetom“

- izrijekom se utvrđuje da upravljanje internetom nije samo pitanje koje se tiče država, tj.vlada, nego uključuje i subjekte privatnog sektora te one iz domene civilnog društva

- pod načelima,normama,pravilima i programima se mogu smatrati brojne aktivnosti

- postoje **2 temeljna pristupa o definiranju aktivnosti** koje ulaze u upravljanje internetom:

**a)** **uži pristup** – upravljanje int. se odnosi na aktivnosti koje se tiču internetske infrastrukture (raspravlja se primarno o regulaciji domenskog prostora te dodjeljivanju IP adresa)

**b) širi pristup** – upravljanje int. se odnosi na veći broj aktivnost koje se tiču stabilnosti interneta,internet.infrastrukture,kibersigurnost,zaštita prava intelektualnog vlasništva, slobode izražavanja,privatnosti i osobnih podataka,sprječavanje kiberkriminala i spama..

- pitanja obuhvaćena širim konceptom upravljanja internetom se grupiraju u **5 skupina:**

**1)** upravljanje infrastrukturom i standardizacija

**2)** pravna pitanja

**3)** ekonomska pitanja

**4)** razvojna pitanja

**5)** društvena i kulturna pitanja

Upravljanje domenskim prostorom i spektrom IP adresa

- prelaskom na domenski sustav,IP i TCP,ključnu ulogu je preuzela akademska zajednica

- ovaj put,upravljanje sustavom IP adresa prepušteno je **Institutu za informacijske znanosti (Information Sciences Institute,ISI)** s **University of Southern California(USC)**

- unutar tog instituta,posao alociranja domenskih naziva i IP adresa je dugo vremena obavljao manji broj znanstvenika,na čelu s Jonom Postelom

-s vremnom,funkcije dodjeljivanja IP adresa i domenskih naziva su se počele neformalno zvati **Internet Assigned Numbers Authority(IANA)-** Postelov institut ih izvršava do 90-ih 20.st.

- IANA nije imala poseban pravni oblik(nije se radilo u pravnoj osobi),nego je predstavljala određene funkcije koje su se obavljale unutar internetske zajednice

- 1998.g. vlada SAD-a je odlučila privatizirati određene poslove upravljanja internetom

- htjeli su stvoriti novo tijelo koje bi imalo pravnu osobnost i koje bi preuzelo funkcije IANA-e (upravljanje spektrom vršnih domena i IP adresa) 🡪 u tu svrhu u SAD-u je osnovan **Internet Corporation for Assigned Names and Numbers(ICANN)**

- ICANN je specifičan pravni subjekt,riječ je o društvu sa sjedištem u Kaliforiniji

- **ICANN je tijekom svog razvoja bio vezan uz SAD iz 3 raloga**:

**1)** riječ je o pravnoj osobi osnovanoj po pravu SAD-a što ga definira kao pravni subjekt koji je podložan pravu te države

2) Vlada SAD-a je jedno određeno vrijeme imala ugovorom osiguranu mogućnost nadzora nad funcioniranjem ICANN-a

3) ICANN svoje ovlasti na upravljanje internetskom infrastrukturom crpi iz ugovora s Vladom SAD-a

- razvoj ide u smjeru napuštanja specifičnog položaja i ovlasti SAD-a,povećanja nezavisnosti ICANN-a te jačanja uloge međunarodne internetske zajednice u upravljanju internetom

- sukladno sporazumu(**Joint Project Agreement,JPA**)između Vlade SAD-a i ICANN-a iz 1998.g., ICANN je postao ovlašten obavljati određene poslove upravljanja internetskom infrastrukturom

- **među zadaćama koje JPA specificira,najvažnije su:**

**1)** razvoj politike upravljanja spektrom IP adresa i njihova dodjela regionalnim centrima

**2)** nadzor nad funkcioniranjem root zone domenskog prostora

**3)** razvoj pravila za dodavanje novih vršnih domena u internetski domenski prostor

- prema prvom JPA-u,predviđeno je da ICANN ove poslove obavlja pod nadzorom i u koordinaciji s ministarstvom trgovine SAD-a

- autonomija ICANN-a se postupno povećavala

- 2009.g. sporazum JPA je zamijenjen dokumentom **Affirmation of Commitments** kojim se ICANN-u daje de facto potpuna samostalnost od Vlade SAD-a

- nakon svog osnivanja, ICANN je preuzeo IANA funkcije koje je prethodno obavljao ISI

- ugovor između ICANN-a i Vlade SAD-a je obnavljan nekoliko puta-zadnji put 2012.g. (postojeći ugovor istječe u rujnu 2015.g. ,ali je predviđena mogućnost produženja do rujna 2019.g.)

- prema planu Vlade SAD-a iz ožujka 2014.g.,nakon isteka ugovora bi IANA funkcije trebale trajno prijeći na međunarodnu internetsku zajednicu

- nakon dobivanja samostalnosti,jedina bitna veza s između interneta i SAD-a je ugovor između Vlade SAD-a i ICANN-a na temelju kojeg je ICANN obavljao funkcije IANA-e

**Upravljanje spektrom IP adresa**

**-** IP adrese su ograničeni resursi(naročito u IPv4 sustavu),pa iz toga proizlazi potreba da ih se alocira na efikasan način

- raspodjela IP adresa je jedna od IANA funkcija

- danas se distribucija IP spektra odvija tako da ICANN slobodne adrese dijeli između 5 regionalnih centara **( Regional Internet Registries,RIR)** koji pokrivaju područje SJ Amerike, Središne i J Amerike,Europe(uključujući Rusiju,bliski i srednji Istok), Azije i Oceanije te Afrike

-ti centri dalje distribuiraju lokalnim i nacionalnim centrima,a oni dalje pojedinim korisnicima

**Upravljanje domenskim prostorom**

- u procesu razlučivanja naziva domena,vršne domene se koriste uslugama root servera,koji sadržavaju popis svih postojećih vršnih domena i IP adrese njihovih DNS servera

- trenutno postoji 13 root servera koji se označavaju slovima A-M i svi oni sadrže istovjetne informacije(podaci sa servera A su autoritativni,a svi ostali dupliciraju sadržaj A servera)

- s tehničke strane, root serveri predstavljaju nevidljivi vrh piramide domenskog sustava, te u procesu pretvaranja naziva domena u IP adrese omogućavaju usmjeravanje na vršne domene

- vršne internetske domene su samo one koje se nalaze u popisu root servera(nova vršna domena nastaje tako da se u root popis unese njen naziv i na njezin DNS server naziv organizacije koja će njome upravljati(isto tako može prestati brisanjem iz root popisa)

- onaj tko kontrolira root zonu domenskog prostora,a primarno root server A,ima de facto vlast nad tim prostorom

- svaka vršna domena ima tijelo koje je ovlašteno(od ICANN-a) da upravlja tom domenom –> to tijelo se zove **voditelj registra**(vršne domene)

-voditelji registra definiraju uvjete registracije i korištenja domenom niže razine unutar pojedine vršne domene

- najčešće voditelji registra omogućavaju pojedinim gospodarskim subjektima da budu posrednici pri registraciji poddomena unutar vršne 🡪 takve posrednike zovemo **voditelji registracije**

- fizičke i pravne osobe registriraju poddomene unutar vršnih bilo posredstvom voditelja registracije,bilo izravno kod voditelja registra ako on sam neposredno pruža registracijske usluge

Upravljanje ključnim internetskim standardima

- **Internet Engineering Task Force (IETF)** –neformalno organizirana grupa stručnjaka iz područja računalnih tehnologija,koja postoji od 1986.g.

- određene organizacijske i financijske aspekte funkcioniranja IETF-a podupire **Internet Society (ISOS)**

- članstvo u toj grupi je u potpunosti slobodno,a članovi grupe su uključeni u njen rad tako da sudjeluju u razmjeni mišljenja putem internetskih foruma(svake godine nekoliko sastanaka)

- među najvažnije uspjehe IETF-a ubraja se razvoj i održavanje IP-a

- **World Wide Web Consortium (W3C)** postavlja standarde u području WWW-a,osnovan je 1994.g. i djeluje primarno tako da izdaje preporuke u kojima se definiraju standardi za pojedine tehnologije

- među najvažnije standarde, koje je W3C uredio,spadaju HTML format koji je standardizirani jezik prikaza web-stranica, PNG format za prikaz grafike i CSS sintaksa koja olakšava upravljanje izgledom web-stranica te se nadopunjava s HTML formatom

Pitanje neutralnosti interneta

- podaci internetom putuju u obliku standardiziranih blokova (tzv. IP paketi)

- uređaji koji se nalaze u sredini mreže bi trebali teretiti sve IP pakete na jednak način,tj. jednakim prioritetom(takvo rješenje nije dugoročno tehnički održivo jer npr. nije isto ako se poruka e-pošte prenese s nekoliko sekundi kašnjenja ili ako do takvog kašnjenja dođe tokom videokomunikacije,npr.putem Skypea jer će to rezultirati smanjenom kvalitetom veze ili nemogućnošću komuniciranja videokomunikacijom)

- pružatelji usluga(da bi izbjegli takve probleme) koriste se raznim tehnikama optimiziranja prijenosa paketa sadržaja putem interneta,tj. tu se optimizira korištenje internetskom vezom iz **tehničkih razloga**

- do problema neutralnosti interneta dolazi jer mnogi pružatelji smatraju da treba davati prioritet određenim servisima pri prijenosu podataka iz tehničkih i ekonomskih razloga

- ideja je da pružatelj usluge prijenosa može u nekim specif. slučajevima naplatiti dodatne iznose onim pružateljima sadržaja na internetu koji zahtijevaju veću kvalitetu usluge ili konzumiraju značajne količine internetskog prometa (npr. argument je da bi servisi kao što je Netflix,čiji poslovni model ovisi o prijenosu ogromne količine podataka(video sadržaja) do krajnjih korinsika puteminterneta, trebali i sami plaćati za prijenos svojih podataka)

- implementacija tih rješenja bi značila da pružatelji usluga prijenosa podataka razvijaju **2 razine usluga:**

**1) komercijalnu** – pružatelji usluge prijenosa bi jamčili da će ta usluga biti odgovarajuće kvalitete,ali bi za tu kvalitetu pružatelji sadržaja posebno plaćali(SAD)

**2) nekomercijalnu**- pružateljima sadržaja se ne bi pružila nikakva jamstva za prijenos podataka,ali se od njih ne bi tražilo ni posebno plaćanje(EU)

**2.5. Nova informacijska revolucija**

- u njenim temeljima je daljnji razvoj biotehnologije,robotike i umjetne inteligencije

- prema **Konvenciji o biološkoj raznolikosti UN-a**, **biotehnologija** je svaka tehnologija koja koristi biološke sustave,žive organizme ili njihove derivate za proizvodnju ili izmjenu proizvoda ili procesa za posebnu namjenu (primjena u medicini,poljoprivredi i informatičkoj industriji)

- teži se stvaranju ljudskom oku nevidljivog čipa koji će dizajnirati kompjutori i proizvoditi roboti utiskivanjem submikronskih elemenata i linija rendgenskim zracima

- velike se nade polažu i u pronalazak i razvoj **biočipa** (cilj je da se u biološkim laboratorijima od živih bakterija uzgoje mreže kompjutorskih logičkih kola,samoobnovljivih, posve nevidljivih,s milijun puta povećanim kapacitetom memorije i djelovanjem poput ljudskog mozga)🡪to će stvoriti podlogu za razvoj umjetne inteligencije,robotizacije,digitalne univerzalne komunikacije i samodjelatne globalne znanstvene civilizacije

- velika su očekivanja i u razvoju **robotike** kao grane strojarstva,elektronike i računalnih znanosti koja se bavi dizajnom,izgradnjom,upravljanjem i primjenom informacija ( danas se roboti koriste na područjima poput proizvodnje,kućnih aparata,obrazovnih pomagala, medicine,vojne industrije,industrije zabave i dr.)

- **Digitalnim agendom za Europu** se potiču ulaganja u gigitalno istraživanje,razvoj i inovacije na području robotike

- vrijednost svjetskog tržišta robotike iznosi 15,5 milijarda eura godišnje(3 milijarde u EU), udjel EU na svj.tržištu industrijske robotike je 25% i 50% u sektoru robotike profesionalnih usluga, do 2060.g. br.osoba starijih od 65 godina u EU porast će iznad 30% (razvit će se roboti za pomoć starim osobama-**Eldercare social robots**), novo javno-privatno partnerstvo u robotici primit će 700 milijuna eura financiranja iz EU,uz 2 milijarde eura kroz privatna ulaganja)

- računalni sustav i robotika se povezuju s **umjetnom inteligencijom(Artificial Intelligence, AI)** koju **Marvin Minsky** s MIT-a definira kao znanost o tome kako postići da strojevi izvode zadatke koji bi iziskivali inteligenciju kada bi ih radio čovjek (primjenu umj.intelig. možemo naći u raznim programima i ekspertnim sustavima koji zamjenjuju stručnjake,a stvoreni su za rješavanje zadataka na područjima medicine,financija,kontrole proizvodnih i dr.procesa te prava sve češće)

**3.CJELINA: Informacijsko društvo**

**3.1. O pojmu i nastanku**

- tijekom 70-ih i 80-ih 20.st. prevladavala su uvjerenja da se ljudsko društvo nalazi na raskrižju koje vodi radikalnoj promjeni načina proizvodnje i zajedničkog života

- osim naziva postindustrijsko društvo,susreću se i izrazi superindustrijsko, postkapitalističko, tehnotroničko, postekonomsko,programirano,mikroelektroničko i dr. društvo

- termin „**postindustrijsko društvo**“ prvi je upotrijebio **Daniell Bell** na jednom predavanju u Salzburgu 1950.g.

- 1973.g.- Bell objavljuje knjigu **The Coming of Post-Industrial Society: A Venture in Social Forecasting** (potakla zanimanja i istraživanja nadolazećeg društva)

- u osnovi prvih shvaćanja postindustrijskog društva leži čuvena **teorija konvergencije**, probližavanja i stapanja kapitalizma i socijalizma u jedan novi društveni poredak,kojoj se priklonio veći krug istraživača

- početne ideje i teorije o konvergenciji datiraju iz vremena nastajanja teorije blagostanja koja proizlazi iz subjektivne teorije vrijednosti zapadnih ekonomista između 2 svjetska rata

- u takve izglede svjetskog razvoja vjeruje već osnivač **teorije blagostanja** - **A.C. Pigou** koji formulira svoje shvaćanje o blagostanju 1912.g. u djelu **Wealth and Welfare**,a potpunije ih je objavio u cjelovitom izlaganju u knjizi **The Economics of Welfare** iz 1920.g.

- nobelovac **Jan Tinbergen** – poznat po doprinosima ekonometriji,programiranju razvoja i nacionalnog gospodarskog planiranja

- među istaknute zagovornike teorije konvergencije ubraja se i **J.K.Galbraith** koji na tome temelji svoju poznatu trilogiju: **The Affluent Society**, **The New Industrial Society** i **Economics and the Public Purpose**

- **R.Aron** – **Dix-huit lecons sur la societe industrielle** i **Les Tendences da la pensee sociologigue** (u njima dokazuje ekonomski automatizam i na temelju toga tvrdi da ekonomska racionalnost potire razna ideološka obilježja)

- u svojoj teoriji postindustrijskog društva,Bell se priklanja tim gledištima i objašnjenjima suvremenog društvenog razvitka

- sveukupni napredak čovječanstva svodi se na 3 velike etape razvoja: **predindustrijsko** (u igri protiv prirode)**, industrijsko** (u igri protiv ukroćene prirode) **i postindustrijsko društvo** (u igri između ličnosti)

- toj periodizaciji suprotna je poznata dioba razrađena u djelu **W.Rostova: The Stages of Economic Growth** (on tvrdi da postoji 5 stadija razvoja društva: stadij tradicionalnog društva, stadij stvaranja pretpostavki za uspon,doba uspona,vrijeme kretanja k visokorazvijenom društvu te doba zrelosti čovječanstva)

- Bellovo **„predindustrijsko društvo“** je siromašno zajedništvo bespomoćnih ljudi koji u malom broju žive na ograničenom prostoru i zavise od mogućnosti da svojom nekvalificiranom radnom snagom prisvoje,prerade i umjetno isporuče ono što priroda daje

- naprednije je **„industrijsko društvo“** koje širi teritorij i bilježi stalan rast stanovništva,a ponajviše zavisi od energetskih izvora koji su temelj masovne proizvodnje i potrošnje

- **„postindustrijsko društvo“** temelji se na informacijama i razvoj mu je funkcija kodifikacije teorijskog znanja

- u knjizi **The End of Ideology** (1960.g.),Bell izlaže uvjerenje da se bliži kraj ideologija jer liberalizam i socijalizam gube utemeljenje u realnom životu (uspoređuje socijalizam i liberalizam kao vodeće ideologije 19.st. s velikim religijama koje se priklanjaju nužnosti događaja te usađuju odanost svojim članovima) 🡪 ideološka strast se seli na istok na kojem je još podnošljiv entuzijazam za **utopijom**

- Bell nije protiv svake utopije i on drži da kraj ideologije nije obvezno i kraj utopije kao vizije težnji koje su u skladu s vlastitim mogućnostima, utopija je korisna ljudima koji su postali svjesni opasnih zamki ideologije(pa odbacuju ideologiju već samim time što ne trasiraju svoju budućnost na vjerovanje,već na empirijskoj spoznaji) 🡪utopija treba imati sve karakteristike **znanstvenog predviđanja**

- Bellov opis postindustrijskog društva polazi od novijih približavanja znanstvenika i tehničara političkoj sferi

- znanstveni centri i kapaciteti postaju najvažniji,znanost i znanje presudni čimbenici razvoja i u prvi plan izbija pojedinac

- Bell je impresioniran modernom telekomunikacijom(brži razvoj tijekom 70-ih i 80-ih g.) 🡪 u tome vidi zaokret u kojem se centar infrastrukture prenosi s načina transporta i izvora energije na sisteme komuniciranja što ubrzava razvoj postindustrijskog društva

- veliku pozornost je privukla knjiga **Alvina Tofflera: Future Schock** iz 1970.g. (kod nas objavljena 1975.g.) 🡪 djelo prikazuje što se događa ljudima kada ih pregazi vrijeme,pa ne mogu slijediti događaje i nagli razvoj sredine u kojoj žive

- Toffler je istakao sintagmu **„šok budućnosti“** kojom izražava i oslikava stanje društva u kojem silna brzina učestalih promjena života nailazi na nerazumijevanje i prepreke zbog spore prilagodljivosti ljudi tim novinama

- Toffler prilazi vladajućoj zbilji sa sustavnom predodžbom o budućnosti koju uvjetuje i nameće dostignuti razvitak tehnike i tehnologije

- prvi udes koji silovito pogađa sadašnjost je **smrt stalnosti** i sve podliježe „kratkoj privremenosti“

- dinamičkoj organizaciji društva, Toffler suprostavlja bogatstvo života što ga donosi svjetska znanstveno-tehnička revolucija

-najpoznatije opise vizije mračne budućnosti daje **G.Orwell**(1984.g.) i **A.Huxly**(Vrli novi svijet)

- Orwell vidi budućnost u podjeli svijeta na Euroaziju i Oceaniju,a u tom podijeljenom svijetu znanost i tehnika služe totalitarnoj vladavini Velikog brata u kojoj se sve odvija pod motom „Neznanje je moć“

- Huxly nudi sretniju budućnost u kojoj su svi zadovoljni zbog masovnog drogiranja

- Toffler je uvjeren da optimističnu viziju budućnosti može izgraditi na materijalističkoj osnovi 🡪 izgrađuje model novog društva koje podliježe stalnim promjenama

- te promjene će biti popraćene sustavnim otklanjanjem mnogih otuđenosti koje su u prošlosti dijelile ljude i sputavale njihovo djelovanje i kreativnost

- optimistični pogled dolazi do izražaja u Tofflerovom djelu **The Third Wawe** koji se pojavio u vrijeme u kojem su krizne posljedice zastarjele klasne civilizacije još više zahvatile svijet (on još dramatičnije gleda na sukob informacijskog društva i industrijalizma)

- javljaju se i kritičari nadolazećeg informacijskog društva s prijetećim tvrdnjama da će virtualni svijet raskinuti veze među ljudima koje se najbolje ostvaruju u komunikaciji i kontaktu ljudi

*\* pročitati Tofflerov opis zajedništva na 51.str.*

- Tofflerova vizija se već neko vrijeme ostvaruje putem Web 2.0 tehnologija koje omogućuju korisniku neposredno sudjelovanje u stvaranju i oblikovanju vlastitih sadržaja kroz interaktivnu komunikaciju s drugim sudionicima na internetu

- u intervjuu danom listu „Le Nouvel Observateur“ krajem 1984.g., Toffler ističe da je na djelu razbijanje industrijske ere,trenutak decentralizacije i razlaganja svijeta standardiziranog i tipiziranog djelovanja i ponašanja 🡪 to naziva **demistifikacijom** (bliži se kraj masovne distribucije proizvoda preko velikih trgovina i robnih kuća)

- s revolucijom informacija dolazi sve više do izražaja diferencijacija i razlikovanje,a svojstveno joj je da ne može biti usmjeravana,dirigirana,rukovođena (industrijska poduzeća se robotiziraju i automatiziraju, tejlorizam i fordizam zastarjevaju,nestaje parcijalni rutinski rad,a time i tradicionalni radnik skupa s „mitologijom plavog ovratnika“)

- problem se može valjano rješiti samo širenjem zanimanja budućnosti koja neće biti zaglupljujuća kao zanimanja rutinske industrijske proizvodnje

- u postindustrijskoj zajednici dominirat će komponenta stvaralaštva,a ona se ne može razvijati i napredovati uz pomoć sile te će odnos pojedinca i zajednica prema budućnosti biti pitanje preživljavanja(po Toffleru prijelome godine su bile od 1957. do 1959.g. kada je prvi put broj umnih radnika premašio broj rutinskih radnika)

- čovječanstvo kreće prema demistifikaciji svoga zajedništv, što znači prema društvima koja razbijaju masu u manje jedinice koje više ne djeluju hijerarhijski već umreženo i mreža postaje temeljna jedinica društva

- birokratskoj vladavini i intervenciji odgovara masovnost i pogoduje joj „uniformiranost populacije“,a postindustrijskom razvoju odgovara odmasovljenje i „neuniformiranost“

- u novom društvu nema klasa, vlasništvo prestaje biti povezano s vlašću,a zaposleni obrazuju **kongitarijat** , kulturne skupine koje posjeduju znanje i proizvodne ideje

- 1980.g. u Parizu je izišla knjiga **Jean-Jacquesa Servan-Schreibera: Le defi mondial** (Svjetski izazov), koja otkriva golema postignuća u gospodarskoj informatizaciji vodećih svjetskih zemalja,pogotovo SAD-a i Japana(najveće postignuće tog razvoja je **„tvornica bez radnika“** koja se mogla tada već razgledati u gradu Toyota)

- Japan je uspio zadržati načelo da tehnološke inovacije „ne smiju ostaviti ljude nezaposlenima“

- praktički gotovo neiscrpan izvor zaposlenja pružaju nove „tvornice softvera“ koje hrane strojeve što potiskuju ljude iz neposredne proizvodnje

- postepeno se stvara jedinstveno i cjelovito **informacijsko društvo**

- Servan-Schreiber ističe kako je informatizacija temeljna preobrazba prozvodnje,potrošnje i načina života,društevnih potreba i društvenog tkiva

- informatizirano društvo počiva na punoj uporabi sposobnosti svakog pojedinca prema njegovim sklonostima

- što će se brže društvo kretati prema individualizaciji,to će ljudski um biti sposobniji za nova dostignuća

- informatizacija je ekponencijalna što omogućuje stalan razvoj osobnih sposobnosti

- **Christopher Evans** se brzo afirmirao kao jedan od vodećih autoriteta na području kompjutorizacije, osobito knjigom **The Myghty Micro** (Kompjutorski izazov) koja govori o budućnosti koja je prisutna u uzburkanim vodama našeg svakodnevnog života,a glavno obilježje te svakodnevnice čini promjena svjetskog društva na svim razinama

-sva su Evansova razmatranja prožeta zanosom i optimizmom u procjenama nadolazećeg informacijskog društva kojeg prati eksponencijalni rast

- svijet se postepeno približava inteligentnom stroju koji će multiplicirati čovjekove mentalne sposobnosti i djelotvornosti u svakoj životnoj angažiranosti

- **Evans razlikuje 6 čimbenika od kojih se sastoji inteligencija:**

**1)** sposobnost prihvaćanja informacija

**2)** mogućnost spremanja podataka

**3)** brzina obrade podataka

**4)** promjenljivost programa

**5)** učinkovitost programiranja

**6)** raspon programa

- mnogobrojni uspjesi na tom području pokazuju da svijet ide prema **ultra-inteligentnom stroju** (važna uloga na čovjekovom putu u svemir)

- **John Naisbitt** objavljuje knjigu o velikim društvenim promjenama što ih donosi informatička revolucija

- 1982.g. Naisbitt objavljuje knjigu **Megatrends: Ten New Directions Transforming Our Lives** u kojoj prvi piše o globalizaciji (izbio u redove najpoznatijih teoretičara informac. društva)- oslanja se na zaključke Tofflera i upušta se u znanstvena predviđanja društvenih promjena na temelju proučavanja tehnološkog i ekonomskog revoluciranja

- Naisbitt (poput Tofflera) razlikuje **3 velike revolucije u razvoju društva:**

**1)** poljoprivrednu

**2)** industrijsku

**3)** informacijsku

- početak postindustrijskog društva povezuje s lansiranjem prvog satelita- sovjetskog „Sputnika“ u Zemljinu orbitu 1957.g. (početak svemirskog doba i globalno komuniciranje putem satelita)

- za Naisbitta je važna i 1981.g. kad je lansiran space shuttle

- **Naisbitt razlikuje 10 smjerova zaokreta:**

**1)** prešli smo na privredu koja se temelji na stvaranju i raspodjeli informacija

**2)** razvoj teče u 2 smjera: u smjeru visoke tehnologije i emotivnog prožimanja(hightech)

**3)** moramo priznati da smo dio globalne privrede i prestajemo misliti da su SAD vodeća industrijska zemlja svijeta

**4)** pretvaramo se u društvo koje daje prednost bavljenju stvarima u dužem vremenu

**5)** otkrivamo sposobnost inovatorskog djelovanja i postizanja rezultata

**6)** pomoć institucija zamjenjujemo većim uzdanjem u sebe u svim oblicima života

**7)** otkrivamo da su okviri predstavničke demokrac. u eri brze raspodjele informacija zastarjeli

**8)**postajemo neovisni o hijerarhijskim strukturama i dajemo prednost neformalnim mrežama

**9)** sve više Amerikanaca napušta stare industrijske gradove sjevera

**10)** prerastamo u neposredno društvo višestrukih mogućnosti biranja

- u Naisbittovom pristupu se uočava materijalistički svjetonazor

- tehnika nameće prisilno preseljenje radnika iz agrarnog u industrijsko društvo,a tehnologija potiče dragovoljno preseljavanje radnika iz industrijskog u informacijsko društvo – zato ga prvi teoretičari informacionalizma nazivaju **postindustrijskim društvom**

- Naisbitt je prvi predložio da se razdoblje u kojem industrijsko zamjenjuje postindustrijsko društvo zove **doba parenteze**

- u svom najboljem djelu **Megatrendovi,**Naisbitt prati kako se u 10 smjerova odvija taj svjetski proces i mijenja naš život

- prijeti opasnost da dualističku kompleksnost međurazdoblja zahvati kaos popraćen stagnacijom, recesijom i krizom (to se dogodilo krajem prve dekade 21.st.)

- svijet plaća grijehe neshvaćene i neprovedene socijalne emancipacije čovječanstva

- Međunarodna organizacija rada(ILO) predviđala je početkom 2009.g. da će samo u toj godini nestati 51 milijun radnih mjesta

- nacionalna gospodarstva se sve više povezuju,pa njihova društva postaju međuovisna

- Naisbitt ne vjeruje mnogo u trajno rješenje svjetskih problema političkim akcijama, on smatra da su ekonomski obziri mnogo važniji od političkih(o sebi kaže da je ekonomski determinist) 🡪 argumentira to i sve većim prijelazom radnog stanovništva iz industrijskog sektora u sektor usluga i informacija(društvo se decentralizira i individualizira na informatičkim resursima)

- postindustrijsko društvo razara masovno privređivanje i okreće se od ekonomske proizvodnje k ekonomici proizvoda,a najviše je u tom pogledu učinio **Peter Drucker**

- njegovo djelo **Inovacije i poduzetništvo** je najbolji opis revitalizacije proizvodnog i poduzetničkog zamaha na osnovi visoko tehnološkog revoluciranja

- privređivanje poprima znanstveni pristup, selektivnu kreaciju, tehnološku inovaciju, fleksibilno upravljanje i agresivni marketing

- proizvodnja se odvija po proizvodnim programima u koje su utkani kreativni i inovativni elementi

- sred. 80-ih g. 20.st. u časopisu „Foreign Affairs“ je izašla Druckerova rasprava u kojoj dokazuje da su već nastupile dramatične promjene u gospodarskom životu visoko informatiziranih zajednica

- **svjetska privreda se nepovratno izmijenila u 3 temeljna pravca:**

**1)** ekonomija primarnih proizvoda odvojila se od industrijske prerađivačke privrede

**2)** industrijska ekonomija se odvojila od zaposlenosti

**3)** tokovi kapitala su postali pogonska snaga svjetske privrede

- kao posljedica tih promjena uslijedio je kolaps cijena primarnih proizvoda, a sektor proizvodnje sirovina i repromaterijala postaje sporedan,marginalan

- probleme koje je donijelo industrijsko društvo (poput ekološke krize,fenomena nezaposlenosti,gladi i neishranjenosti, ograničenje čovjekove biosfere) više nije moguće rješavati unutar nacionalnih granica

- izlaz se nadzire u razvoju i širenju informacijskog društva

- **Jeremy Rifkin** je uvjeren da će u 21.st. najveće promjene donijeti genetski inženjering 🡪 pa to stoljeće nosi naziv **biotehnološko stoljeće**

- **Christopher Freeman**- paradigma informatičke tehnologije doživljava promjene te njeno nastajanje i učestalije mijenjanje pokazuje kako se brzo odvija prelazak s tehnike temeljene na jeftinom inputu energije na tehnologiju koja se temelji na jeftinim inputima informacija dobivenih napretkom u mikroelektronici i u elektroničkim komunikacijama

- **Manuel Castells: Informacijsko doba: ekonomija,društvo i kultura** – dokazuje kako usporedno s time nastaju epohalne organizacijske promjene kojima se mrežno povezuju poduzeća,ustanove,nacionalne i regionalne zajednice što vodi globalnom ujedinjenju

- s prevlašću informacijskog društva osnovnu jedinicu ekonomske i svake druge društvene organizacije po prvi put čini mreža sačinjena od mnoštva subjekata i organizacija,čvorišta i odnosa koji dolaze sa svih strana i odlaze u svim pravcima

-s informacionalizmom umrežavanje postaje sveopći oblik društvenog organiziranja

- **Albert Laszlo Barabasi: U mreži** – ukazuje na važnost mrežnog razmišljanja u znanosti, poslovanju i svakodnevnom životu i ukazuje na činjenicu da danas sve više shvaćamo da se ništa ne odvija u izolaciji

- povezivanjem mreža putem informacijsko-komunikacijskih tehnologija stvara se novi virtualni prostor- **kibernetički prostor** ili **kiberprostor** čiju temeljnu infrastrukt. čini internet

- on nadilazi granice nacionalnih država, a time i kontrolu njihove vlasti

- fizički prostor je krut i za sve sudionike pravno jednak

- podliježe upravljanju koje sve svodi na istu mjeru i zahtijeva podjednako ponašanje

- kiberprostor je **regulabiran**,što znači da se različito može regulirati isto ponašanje u različito vrijeme i na raznim mjestima

- fizički prostor je postojan,a kibernetički se lako mijenja,ukida i širi

- **Lavrence Lessing: Kod i drugi zakoni kiberprostora** – uvjeren je da kiberprostor može biti jednako slobodan jer sloboda odgovara njegovoj prirodi

- Lessing ipak ne vjeruje da je regulacija,ostvariva na dostignutom stupnju razvoja, potpuna sloboda informacija i komuniciranja

- vlade mogu nadziranjem podrediti svojim monopolističkim interesima **4 najvažnije društvene vrijednosti:** intelektualno vlasništvo,privatnost,slobodu govora i suverenost

- **kod** regulira umrežavanje i osigurava organiziranje i funkcioniranje virtualnog života izvan pravničke domene

- 1956.g. na konferenciji na koledžu Dorthouth u Hanoveru u SAD-u je **John McCarty** prvi put upotrijebio naziv **umjetne inteligencije**

- **Kurzwill** predviđa da će umjetna inteligencija 2030.g. biti superiornija od ljudske inteligencije i to izlaže u knjizi **The Singularity is Near**

- **Stephen Howking i Elon Musk** su,na stranicama neprofitne organizacije The Future of Life Institute, naveli bojazan da bi nekontroliran rast umjetne inteligencije mogao imati kobne posljedice za čovječanstvo(rast nezaposlenosti)

- Howking kaže da umjetna inteligencija ima potencijal za okončanje ljudske rase ( s tim se slaže **Bill Gates**,ali ne i **Eric Horvitz**,šef istraživačkog centra Microsofta)

- društvo znanja gradi se na intelektualnom kapitalu,na filozofiji inventivnog menadžmenta, na ideji organizacije koja uči i na informacijskoj tehnologiji

**3.2. Digitalna podjela i digitalni jaz**

- selektivnost i brzina širenja novih informacijskih tehnologija je imala za posljedicu da i danas postoje područja i značajan dio stanovništva koji su isključeni iz novog inf.-komunik. tehnološkog sustava

- svijet se sve više raslojava i dijeli se na one koji se koriste suvremenom informacijskom tehnologijom i imaju pristup raznim informacijama i uslugama,te na one koji je nemaju ili ne znaju koristiti

- **Kofi Annan**(generalni tajnik UN-a) na sastanku Generalne skupštine posvećene informacijskoj i komunikacijskoj tehnologiji u New Yorku 2001.g. izjavljuje da se razvoj digitalnog društva postavlja kao jedan od najvećih izazova u svijetu na početku 21.st. te se razlika između onih kojima su tehnologije dostupne i onih kojima nisu -stanje poznato kao **digitalni jaz** -sve više širi

- pokazalo se da dostupnost informacijskih tehnologija ovisi o sredini u kojoj čovjek živi i radi

- digitalna podjela dolazi prvo u zemljama poput SAD-a gdje se ona javlja u prvom redu između bogatih i siromašnih te urbanih i ruralnih sredina

- poč. 90-ih 20.st. – Clintonova administracija je projektom stvaranja **Nacionalne informacijske infrastrukture**,radi ostvarenja širokog kruga ekonomskih i socijalnih ciljeva, namjeravala stvoriti **informacijsku superprometnicu** putem koje bi svim građanima omogućila širi pristup informacijama i raznim uslugama

*\** ***Informacijska superprometnica*** *(information superhighway) je komunikacijski sustav velike brzine koji je predlagala Clintonova administracija u predizbornoj kampanji radi unapređivanja obrazovanja u SAD-u na prijelazu u 21.st.,a namjera je bila pomoći svim građanima da dođu do informacija bez obzira na njihov materijalni položaj (WWW je postao informacijska superprometnica)*

- počinje se poticati ulaganje u informatička istraživanja i obrazovanje informatičkih stručnjaka na sveučilištima,razvoj novih aplikacija i usluga te snižavanje cijena novih tehnologija i pristupa internetu

- uočilo se da bi se stvaranjem nacionalnih infrastruktura širom svijeta i njihovim povezivanjem u **Globalnu informacijsku infrastrukturu** moglo ostvariti i druge ciljeve poput: izlaska na nova tržišta,intenziviranja gospodarskog rasta,unapređivanja infrastrukture, otvaranja novih radnih mjesta,promicanja demokracije,slobode izražavanja i slobode informiranja, većeg stupnja obrazovanosti i kulturne raznolikosti te globalne stabilnosti

- da bi se to postiglo trebalo je postići međunarodni konsenzus i stvoriti zajedničke osnove za nastanak i funkcioniranje takve infrastrukture

- tako je **organizacija G-7**,grupa sedmorice vodećih industrijskih zemalja,na ministarskoj konferenciji o informacijskom društvu dogovorila suradnju na stvaranju Globalne informacijske infrastrukture da bi se ostvarile zajedničke vizije o Globalnom informacijskom društvu

- **Globalno informacijsko društvo bi se temeljilo na načelima:**

**a)** promicanja dinamične konkurencije

**b)** poticanja privatnih investicija

**c)** definiranja odgovarajuće regulacijske osnovice

**d)** omogućavanja otvorenog pristupa mrežama uz osiguranje pristupa i dostupnosti usluga

**e)** promicanja jednakih mogućnosti za građane

**f)** promicanja raznolikosti sadržaja,ukljućujući kulturne i jezične raznolikosti

**g)** prepoznavanja nužnosti međunarodne suradnje uz posebnu pažnju na manje razvijene zemlje

- ovim načelima se nastoji i povećati učinkovitost takve infrastrukture te ostvariti jednakost i ravnopravnost građana pri njenom korištenju

- ta načela bi se trebala primijeniti na Globalnu informacijsku infrastrukturu **sredstvima**: promicanja međupovezanosti i međuoperabilnosti,razvojem globalnih tržišta za mreže, usluge i aplikacije,osiguranjem privatnosti i sigurnosti podataka,zaštitom intelektualnog vlasništva,suradnjom na istraživanju i razvoju te nadzorom socijalnih i društvenih učinaka i posljedica informacijskog društva

- njihov put su slijedile i druge zemlje,s razlikom da se u Europi uvriježio naziv **informacijsko društvo** (koristi se kao sinonim za niz projekata kojima se nastoji prevladati digitalni jaz unutar Europske unije i ostatka razvijenog svijeta)

- prvi dokument u kojem se spominje važnost stvaranja informacijskog društva pomoću transeuropske mreže bio je izvještaj **White Paper on Growth,competitiveness,employment- The challenges and ways forward into the 21st century** (poznat i pod nazivom **The Delors Report**) 🡪 upozorava na potrebu slobodnog protoka informacija između pojedinaca**,** organizacija i organa javne vlasti uz istovremenu nužnost zaštite privatnosti i intelektualnog vlasništva te upućuje na utjecaj novih informacijskih tehnologija na području zapošljavanja i na hitnost stvaranja Pan-europske informacijske infrastrukture

- nakon toga je Europsko vijeće imenovalo grupu istaknutih stručnjaka na čelu s **Martinom Bangemannom**, sa zadatkom da utvrde mjere potrebne za stvaranje inform. infrastrukture

- u izvještaju **Europe and the Global information society** (poznat kao **Bangemann Report**) Vijeću je preporučeno stvaranje transeuropskih telekomunikacijskih mreža i njihovo povezivanje na području cijele Unije

- ukazano je na hitnost privatizacije i liberalizacije informacijske infrastrukture i potrebu uspostave novih općih usluga

- Europska komisija(polazeći od Bangemannovog izvještaja i preporuka) je donijela akcijski plan **Europe's way to the information society** (1994.g.) 🡪 potiče inicijative na području izgradnje transeuropskih mreža,usluga,aplikacija i sadržaja te potrebu liberalizacije infrastrukture,uspostavu općih usluga i njihovo financiranje,zaštitu intelektualnog vlasništva, nadzor medija te elektroničku i pravnu zaštitu

- tim planom su osnovane grupe stručnjaka sa zadatkom da utvrde utjecaj informacijskog društva na osobni,profesionalni i javni život građana te načine promicanja informacijskog društva jačanjem svijesti o mogućnostima i opasnostima koje ga prate

- 1995.g. je Europska komisija osnovala **Information Society Forum**- savjetodavnu organizaciju sa zadatkom proučavanja utjecaja novih informatičkih i komunikacijskih tehnologija na informacijsko društvo,ljude i poslovanje

- forum danas broji 88 članica, podijeljen u 6 radnih grupa koje proučavaju: utjecaj na ekonomiju i zapošljavanje; temeljne socijalne i demokratske vrijednosti u „virtualnoj zajendici“,utjecaj na javne službe; odgoj,obrazovanje i učenje u informacijskom društvu; kulturnu dimenziju i budućnost medija; kontinuirani razvoj tehnologije i infrastrukture

- u njihovom prvom izvještaju 1996.g. pod nazivom **Networks for People and their Communities: Making the Most of Information Society in the European Union** uočeno je da ljudi,institucije i tvrtke nisu pripremljeni za nove tehnologije zbog čega ne mogu iskoristiti ono što nude te je potrebno izvršiti radikalne promjene da bi se ostvario brži gospodarski rast,veće zapošljavanje i bolju kvalitetu života

- posebno se ističe nužnost permanentnog obrazovanja i tako bi informacijsko društvo moralo postati **društvo doživotnog učenja (Lifelong Learning Society)** što znači da se izvori obrazovanja i odgoja moraju proširiti izvan tradicionalnih institucija

- pristup on-line javnim uslugama i informacijama mora biti opći,sveobuhvatan,a javna vlast mora iskoristiti mogućnost novih tehnologija većom učinkovitošću i fleksibilnošću

- treba omogućiti širi pristup javnim informacijama i participaciju građana u odlučivanju o pitanjima od javnog interesa

- u izvještaju se navodi da informacija nije obično dobro ili usluga,već je ona izraz kulturnog identiteta što bi moglo dovesti do „druge renesanse“ u Europi većim iskorištavanjem njenih kulturnih i jezičnih različitosti te posebno omogućavanjem svakoj osobi šireg pristupa njenoj i drugim kulturama

- istaknuta je i uloga **daljinskog rada**,tj. **telerada** (Teleworking) u otvaranju novih radnih mjesta te potreba za stvaranjem i širenjem korisnog i pristupačnog tržišta interaktivnih usluga,čiji razvoj treba potaknuti javni sektor većim ulaganjima u njih(potrebno je stvoriti normativnu osnovicu koja će pozitivno utjecati na razvoj tržišta,konkurenciju,pluralizam i demokraciju te očuvanje i promicanje europske kulture uz sprječavanje monopolističkog položaja, osiguranje općeg pristupa mrežama davatelja usluga i zaštite prava potrošača

- na taj način,privatizacija i liberalizacija tržišta uz istovremeno sprječavanje monopola postaju prioritet uz uvjet daljnjeg razvoja informacijskog društva

- 1999.g. Europska komisija je dala inicijativu **eEurope an Information Society for All** s ciljem da Europa što prije iskoristi potencijale informacijskih tehnologija

- **ciljevi te inicijative su bili:**

**1)** online povezivanje svih građana,doma ili škole,svake tvrtke i administracije i njihovo uvođenje u digitalno doba

**2)** digitalno opismenjivanje Europe,podržano poduzetničkom kulturnom spremom da financira i razvija nove ideje

**3)** osiguranje društvene prihvatljivosti cijelog procesa,jačanjem povjerenja potrošača i društvene povezanosti

- da bi se to ostvarilo,komisija je preporučila **10 prioritetnih područja djelovanja** (s ciljevima koje treba postići zajedničkim djelovanjem Komisije,zemalja članica,industrije i građana Europe):

**1)** Europska mladost u digitalnom dobu(dovođenjem interneta i multimedijskih alata u škole i prilagođavanjem obrazovanja digitalnom dobu)

**2)** jeftiniji pristup internetu(povećanjem konkurencije)

**3)** ubrzanje elektroničkog poslovanja(bržom implementacijm zakonskih rješenja i povećanim korištenjem elektroničkom nabavom)

**4)** brži internet za istraživače i studente (da bi se potakla suradnja obrazovnih institucija i prakse)

**5)** pametne kartice za elektronički pristup(omogućavanjem uspostave široke europske infrastukture radi što šireg prihvaćanja)

**6)** rizični kapital za visoko-tehnološka mala i srednja poduzeća(razvoj inovativnih pristupa)

**7)** „elektroničko sudjelovanje“ za invalide

**8)** online zdravstvena zaštita

**9)** inteligentni transport (siguran,efikasniji prijevoz korištenjem digitalnim tehnologijama)

**10)** online vlast(da građani imaju jednostavan online pristup informacijama o javnoj vlasti)

- 2000.g. usvojili su sveobuhvatan akcijski plan **eEurope Action Plan** pozivajući na njegovu implementaciju do kraja 2002.g.

- aktivnost je trebalo usmjeriti na **3 glavna cilja:**

**1)** jeftiniji,brži i sigurniji internet (jeftiniji i brži pristup internetu,brži internet za istraživače i studente,sigurne mreže i pametne kartice)

**2)** investiranje u ljude i umijeća(Europska mladost u digitalnom dobu,rad u ekonomiji temeljenoj na znanju,sudjelovanje svih u ekonomiji temeljenoj na znanju)

**3)** poticanje korištenja interneta( brži razvoj elektroničkog poslovanja, online vlast: elektronički pristup javnim uslugama,online zdravstvo; europski digitalni sadržaji za globalne mreže,inteligentni sustavi prijenosa)

- jedan od temeljnih prioriteta Europske komisije je stvaranje jedinstvenog digitalnog tržišta

- prvi od 7 stupova **Strategije Europa 2020.,**kojom se definiraju ciljevi za rast EU do 2020.g., **Digitalna agenda** je kojom se ostvaruju uvjeti za bolje iskorištavanje potencijala inform.-komunik. tehnologija radi poticanja inovacija,gospodarskog rasta i napretka

- **Digitalnom agendom u Strategiji Europa 2020. postavljeni su ciljevi:**

**a)** stvaranje jedinstvenog digitalnog tržišta

**b)** unapređivanje interoperabilnosti i standarda

**c)** jačanje online povjerenja i sigurnosti

**d)** promicanje brzog i ultrabrzog pristupa internetu svima

**e)** ulaganje u istraživanje i inovacije

**f)** promocija digitalne pismenosti,vještina i uključivanje

- da bi se to ostvarilo,poč. svibnja 2015.g. Europska komisija je donijela novu **Strategiju jedinstvenog digitalnog tržišta** za Europu kojom je predložila smjernice i aktivnosti za iduće razdoblje

- **cilj Strategije** je stvoriti slobodno online tržište roba,osoba,usluga i kapitala u cijeloj Europi tako da građani i poslovni subjekti mogu jednostavno provoditi on-line aktivnosti bez obzira na nacionalnost ili mjesto prebivališta (cilj je uklanjanje prepreka koje vode do toga)

- **ključni prijedlozi Komisije se odnose na mjere i aktivnosti kojima će se osigurati:**

**a)** bolji pristup potrošačima i poslovnim subjektima online robama i uslugama u Europi

**b)** stvaranje uvjeta za rast digitalnih mreža i usluga

**c)** maksimalno povećanje potencijala digitalne ekonomije

- **procjene Komisije su da:**

**a)** bi potrošači u EU bi mogli svake godine uštedjeti 11,7 mlrd. eura kada bi mogli birati iz cijelog niza EU roba i usluga pri online kupovini

**b)** 61% potrošača u EU imaju povjerenje u kupovinu putem interneta od prodavača koji se nalaze u njihovoj državi članici, a samo 38% se osjeća sigurnim pri kupnji iz druge zemlje

**c)** samo 7% malih i srednjih poduzeća u EU prodaju robu i usluge prekogranično

- uklanjanje prepreka bi moglo popuniti proračun EU s dodatnih 415 mlrd. eura

- posebno mjesto u razvoju digitalnog tržišta imaju visoko-tehnološke tvrtke i industrije koje se temelje na autorskom pravu i srodnim pravima

- u takve industrije spada niz djelatnosti koje su izravno ili posredno povezane s proizvodnjom,ponudom i distribucijom autorskih djela ili objekata srodnih prava poput industrije softvera,audio,audiovizualnih i drugih digitalnih djela kao i one koji nude gotove proizvode ili prizvode za njihov razvoj,korištenje i distribuciju(tvrtke koje posluju na tom području ostvaruju veći udio u BDP-u zemlje u kojoj imaju sjedište)

- napretkom tehnologije, sektor elektroničkih komunikacija i elektroničkih melodija, dramatično se promijenio nudeći nove usluge poput kabelske televizije,satelitske televizije, IPTV-a,pametne televizije i Pay TV-a

- to je utjecalo i na potrošačke navike koje su se promijenile pojavom širokopojasnog interneta i tzv.streaming usluga namijenjenih onima koji žele prijenos audio ili video sadržaja u realnom vremenu ili video sadržaja na zahtjev preko interneta

- **razvoj kreativne ekonomije** i **poticanje inovativnosti** postaje sve više prioritet i važan čimbenik gospodarskog razvoja svih razvijenih zemalja

- u sljedećem razdoblju očekuje se da će se takvo jedinstveno digitalno tržište EU morati sve više integrirati u globalno tržište što nameće globalizacija i sama priroda interneta koji ne poznaje granice

- na putu stvaranja jedinstvenog digitalnog tržišta stoje **brojne prepreke**: nedostatak ulaganja u mreže, interoperabilnosti,vještina,nedovoljno istraživanje i razvoj,fragmentirani odgovori na društvene izazove,povećanje kibernetičkog kriminala i nisko povjerenje, fagmentirana digitalna tržišta

- razvojem nacionalnih i nadnacionalnih informacijskih infrastruktura i njihovim povezivanjem stvaraju se pretpostavke buduće **globalne informacijske infrastrukture**

- EU ubrzano radi na projektu Informacijskog društva kako bi u prvom redu prevladala digitalni jaz u odnosu na SAD,Japan i dr.visokotehnološki napredne zemlje,ali i dalje mnoga područja ostaju komunikacijski i prostorno nepovezana

- nerazvijene i manje razvijene zemlje suočene su s problemom **„odljeva mozgova“ (Brain drain)**,tj.odlaska visokokvalificiranih kadrova u razvijenije zemlje što još više povećava digitalni jaz između njih

- premošćivanje digitalne podjele je globalni problem,a pri tome obrazovanje,sustavom neformalnog izvaninstitucionalnog i interaktivnog daljinskog učenja, mora postati opći interes međunarodne zajednice

- ključnu ulogu u tome imaju najrazvijenije zemlje koje bi sredstvima,znanjem i kadrovima trebale ubrzati razvoj i uspostavljanje globalne informacijske infrastrukture(GII), što bi omogućilo širenje edukacije i boljih zdravstvenih usluga putem daljinskog učenja i telemedicine,a poslije bi potaklo i gospodarski rast

**3.3. Pravna infrastruktura informacijskog društva u RH**

- RH zadnjih 10-ak godina usklađuje svoje zakonodavstvo s pravnom stečevinom EU te stvara pravno okruženje koje će potaknuti gospodarski rast,otvoriti nova radna mjesta i omogućiti građanima i poslovnim subjektima da iskoriste potencijale digitalnih tehnologija i da se aktivno uključe u jedinstveno digitalno tržište EU

- RH je donijela niz zakonskih i podzakonskih propisa koji čine temeljnu pravnu infrastrukturu za razvoj informacijskog društva:

**1) Zakon o zaštiti osobnih podataka (ZZOP)** – zaštita osobnih podataka o fizičkim osobama te nadzor nad prikupljanjem,obradom i upotrebom osobnih podataka u RH

**2) Zakon o elektroničkim komunikacijama (ZEK)** – uređuje se područje elektroničkih komunikacija i to korištenje elektr.komunikac. mrežama i pružanje elektr.komunik.usluga, pružanje univerzalnih usluga te zaštita prava korisnika usluga,gradnja,postavljanje, održavanje i upotreba elektr.komunik.infrastrukture i povezane opreme,uvjeti tržišnog natjecanja te prava i obveze sudionika na tržištu elektr.komunik.mreža i usluga, djelotvorno upravljanje radiofrekvencijskim spektrom te adresnim i brojevnim prostorom,digitalni radio i televizija,zaštita podataka,sigurnost i cjelovitost elektr.komuni.mreža i usluga, obavljanje inspekcijskog nadzora i kontrole,osnivanje nacionalnog regulatornog tijela,poštanske i željezničke usluge,njihovo ustrojstvo,djelokrug i nadležnosti te postupak donošenja odluka i rješavanja sporova

**3) Zakon o elektroničkim medijima (ZEM)**- prava,obveze i odgovornosti fizič. i pr.osoba koje obavljaju djelatnost pružanja audio i audiovizualnih medijskih usluga elektroničkih publikacija putem elektroničkih komunikacijskih mreža te interes RH u području el.medija (audiovizualni programi,radijski programi i elektroničke publikacije)

**4) Zakon o elektroničkom potpisu (ZEP)** – pravo fizičkih i pravnih osoba na uporabu elektroničkog potpisa u upravnim,sudskim i dr.postupcima,poslovnim i drugim radnjama te prava,obveze i odgovornosti fizičkih i pravnih osoba u vezi s davanjem usluga certificiramka elektr.potpisa,ako posebnim zakonom nije drukčije uređeno

**5) Zakon o elektroničkoj ispravi (ZEI)** – pravo fiz.i pr.osoba na uporabu elektr.isprave u svim poslovnim radnjama i djelatnostima te u postupcima koji se vode pred tijelima javne vlasti u kojima se elekt. oprema i programi mogu primijenjivati u izradi,prijenosu,pohrani i čuvanju inform, u elektr.obliku,pravna valjanost elektr.isprave te uporaba i promet elektr.isprava,izuzev slučajeva gdje se drugim zakonima izričito traži uporaba isprava na papiru

**6) Zakon o pravu na pristup informacijama (ZPPI)** – pravo na pristup inform. i ponovnu uporabu informacija koje posjeduju tijela javne vlasti,propisuju se načela ograničenja, postupak i način ostvarivanja i olakšavanja pristupa i ponovne uporabe inform.,djelokrug, način rada i uvjeti za imenovanje i razrješenje Povjerenika za informiranje te inspekcijski nadzor nad provedbom ovog Zakona

**7) Zakon o tajnosti podataka (ZTP)** – utvrđuje se pojam klasificiranih i neklasificiranih podataka,stupnjevi tajnosti,postupak klasifikacije i deklasifikacije, pristup klasific.i neklasif. podacima,njihova zaštita,nadzor nad provedbom ovog zakona; primjenjuje se na državna tijela,tijela jedinica lokalne i područne samouprave,pravne osobe s javnim ovlastima te pr. i fiz. osobe koje ostvare pristup ili postupaju s klasif.i neklasif.podacima

**8) Zakon o informacijskoj sigurnosti (ZIS)** – utvrđuje se pojam inform.sigurnosti,mjere i standardi inf.sig.,područja inf.sig. te nadležna tijela za donošenje,provođenje i nadzor mjera i standarda informacijske sigurnosti; primjenjuje se na državna tijela,tijela jedinica lokalne i područne samouprave,pravne osobe s javnim ovlastima koje se u svom djelokrugu koriste kvalif. i nekvalif.podacima,kao i na pravne i fiz.osobe koje ostvaruju pristup ili postupaju s klasif.i neklasif.podacima

**9) Zakon o kritičnim infrastrukturama (ZKI)** – uređuju se nacionalne i europske kritične infrastr.,sektori nacion.kritičnih infrastrukt.,upravljanje kritičnim infrastr.,izrada analize rizika, sigurnosni plan vlasnika/upravitelja,sigurnosni koordinator za kritičnu infrastr., postupanje s osjetljivim i klasificiranim podacima te nadzor nad provedbom ovog Zakona

**10) Zakon o državnoj informacijskoj infrastrukturi (ZDII)** - utvrđuje prava,obveze i odgovornosti nadležnih tijela javnog sektora vezano uz ispostavu,razvoj i uspravljanje sustavom državne informacijske infrastrukture,uspostavljanje i upravljanje sustavom javnih registra i uvjeti koje državna inf.infrastr. mora osigurati u odnosu na javne registre kao i korištenje zajedničkom osnovicom za sigurnu razmjenu podataka unutar sustava državne inform.infrastr.,zajedničkog sustava identifikacije i autentifikacije,jedinstvene točke interakcije s građanima i dr.korisnicima

**11) Zakon o autorskom pravu i srodnim pravima (ZAPSP)**- autorsko rpavo,tj.pravo autora na njihovim djelima iz književnog,znanstvenog i umjetničkog područja te srodna prava umjetnika izvođača na njihovim izvedbama,proizvođača fonograma na njuihovim fonogramima,filmskih producenata na njihovim videoigrama,organizacija za radiodifuziju na njihovim emitiranjima,nakladnika na njihovim izdanjima i proizvođača baza podataka na njihovim bazama; uređuje i individualno i kolektivno ostvarenje autorksog prava i srodnih prava,njihovu zaštitu u slučaju povrede te područje primjene ovog zakona

**12) Zakon o elektroničkoj trgovini (ZET)** –pružanje usluga informacijskog društva, odgovornost davatelja usluga informacijskog društva te pravila u vezi sa sklapanjem ugovora u elektroničkom obliku

- **Zakonom o potvrđivanju Konvencije o kibernetičkom kriminalu** te **Kaznenim zakonom** se materijalno kazneno zakonodavstvo usklađuje s navedenom konvencijom

- **Zakonom o zaštiti potrošača** je predviđena zaštita potrošača kada je riječ o ugovorima sklopljenim izvan poslovnih prostorija i ugovorima sklopljenim na daljinu

**4.CJELINA: Pravo i informatika**

- 3. i 4.informacijska revolucija imale su **dvojak učinak na pravo**:

**1)** nove inform.-komunik.tehnologije te inovativna rješenja zasnovana na njihovom korištenju su veoma brzo pronašča primjenu u raznim sektorima javne vlasti,pa tako i u pravosuđu(to se očituje kroz mogućnost automatizacije postojećih poslovnih procesa koje se u sudstvu odvijaju,stvaranje velikih baza podataka sa zakonodavstvom,sudskom praksom, stručnom i znanstvenom literaturom i razvoj ekspertnih sustava na području prava)

*\* ekspertni sustavi su računalni programi temeljeni na znanju iz nekog specijalističkog područja koji pripadaju području umjetne inteligencije*

**2)** sve šire uvođenje inf.-komunik.tehnologija je rezultiralo novim pravnim problemima,a to je postavilo zahtjev pred pravnu struku da se novonastali odnosi pravno urede

- od 60-ih g. 20.st. odvijaju se informatičle i pravne aktivnosti usmjerene na što širu šrimjenu informacijskih tehnologija u pravu i stvaraju se pravne osnove za znanstveni pristup izučavanja tog područja,a to prate nastojanja međunarodnih organizacija da se suzbiju neželjene posljedice i zakonski urede ona područja na kojima se tehnologije najviše koriste,a zloporabe javljaju

- iz te interakcije prava i informatike proizašao je zahtjev i potreba da se ta 2 područja izučavaju interdisciplinarno,na znanstveni i sustavni način

- znamstveni pristup takvim odnosima i problemima se odvija već desteljećima pomoću znanstvene discipline nazvane **pravna informatika**

- u početku se predmet izučavanja odnosio na mogućnosti primjene novih tehnologija u pravu,ali ubrzo se uočilo da takav pristup nije dostatan

- zbog toga,pravna informatika danas na interdisciplinarni način izučava mogućnosti primjene inf.-komunik.tehnologije u pravu te prati promjene,potrebe i mogućnosti da se taj razvoj odvija u željenim okvirima koje prati odgovarajuća pravna infrastruktura

- prema tome njezine sastavnice čine **pravna informatika i pravo informacijskih tehnologija**

**4.1. Osnove informatike**

**4.1.1. O nastanku i pojmu informatike**

- iako se naziv **informatika** u literaturi najčešće pripisuje **Phillipe Dreyfusu** koji ga je u radu objavljenom 1962.g. upotrijebio kao kovanicu dviju riječi: L'INFORMATIQUE = l'INFORmation + L'autoMATIQUE (informacija+automatika),već 1957.g. **Karl Steinbuch** ga je koristio u naslovu rada koji je objavio pod nazivom **Informatik: Automatische Informationsverarbeitung (Informatika: Automatska obrada podataka)**

- u engl. govornom području informatika se koristi kao sinonim za računalnu znanost (Computer Science)

- **2 pristupa definiranja pojma informatika s obzirom na predmet izučavanja:**

**1)** predmet informatike je izučavanje sastava,fukcija,provedbe i rada informacijskih sustava uz pomoć računala

**2)** drugi polaze od samih informacija i načina njihova prikupljanja,pohrane,prenošenja i uporabe uz pomoć tehničkih uređaja

- treba razlikovati podatke,informacije i znanje

- prema **Poratu** informacije su prganizirani podaci preneseni komunikacijom

- **Bell** smatra da je znanje skup organiziranih izjava o činjenicama ili idejama koji predstavlja promišljeni sud ili rezultat eksperimenta koji se drugima prenosi putem nekog medija komunikacije u nekom sustavnom obliku

**4.1.2. Pojam,svrha i struktura informacijskog sustava**

- u 2. polovici 20.st. započinje epohalni prijelaz iz starog industrijskog društva u novo postindustrijsko zajedništvo (posebno su važne njegove 50-te godine)

- na poč. toga razdoblja ulazi u upotrebu 1.generacija kompjutora s elektronskim cijevima i kablovskim vezama,a na kraju 2.generacija koja se koristi tranzistorima i tiskanim krugovima s magnetskom jezgrom

- sredinom tog desetljeća prvi put su u SAD-u „bijeli ovratnici“(umni i uslužni djelatnici) nadvladali „plave ovratnike“ (rutinski radnici)

- u to razdoblje spada i zaokret od analitičkog k sustavnom pristupu i metoda znanstvenog istraživanja i izlaganja

- na poticaj **Ludwiga von Bertalanffyja, Kenetha Bouldinga i Ralpha Gerarda**, Američka asocijacija za unapređenje znanosti je 1954.g. osnovala Društvo za opću teoriju sustava **(General Systems Theory**,kasnije nazvano **General Systems Research**) 🡪imanentno mu je znanstveno predviđanje sutrašnjice

- opća teorija sustava bavi se onim što im je zajedničko i što treba svima olakšati pristup i metode proučavanja pojedinih sustava

- **osnivači opće teorije odmah ističu njezine osnovne ciljeve:**

**1)** istražiti izomorfiju raznih koncepcija,doktrina i teorija,modela i zakonitosti na pojedinim znanstvenim područjima

**2)** stimulirati formiranje teoretskih modela u sustavnim istraživanjima

**3)** otkloniti paralelna istraživanja na raznim znanstvenim područjima

**4)** unaprijediti komuniciranje među različito specijaliziranim znanstvenicima

**5)** poticati i unapređivati organiziranje timskog rada na njihovim zajedničkim projektima

- sve se u prirodi i društvu dvija kao proces formiranja,funkcioniranja i razvijanja mnogobrojnih samostalnih i na razne načine povezanih,međuovisnih i uzajamno utjecajnih sustava

- sve veću važnost imaju informacijski sustavi koji su međusobno povezani i utjecajni te tvore lanac djelatno isprepletenih nadsustava,sustava i podsustava u ovisnosti o mjestu što ga zauzimaju i uloge koja im pripada u međusobnim odnosima i djelovanju

- njihovu netjelesnu strukturu čine podaci i komunikacijski tokovi koji nam daju informacije

- u definiranju informacijskog sustava najbolje je slijediti stav **V.Sriće i A.Klimenta**, te zaključiti da se to može najpotpunije postići odgovorom na 3 pitanja:

**1)** što mu je cilj

**2)** koje su mu funkcije

**3)** od čega se sastoji

- obično se kaže da mu je cilj da nam da pravu informaciju u pravo vrijeme i na pravom mjestu uz minimalne troškove

- važno je defnirati granice između promatranog informacijskog sustava i okoline koja ga okružuje,tj.nadsustava kojem pripada

- svaki sustav ima 4 elementa: ulaz,izlaz,proces i povratnu spregu(vezu)

- teoretski su moguća **3 stanja u kojima se može zateći informacijski sustav:**

**1)** kad ima samo ulaz u pitanju je **informirani sustav**

**2)** kad ima samo izlaz u pitanju je **informirajući sustav**

**3)** kad ima ulaz i izlaz u pitanju je **cjeloviti informacijski sustav**

- u praksi nema ograničenih informiranih i informirajućih sustava,postoje i djeluju samo informacijski sustavi

- i podjela na otvorene i zatvorene je samo teoretska jer u praksi svaki sustav ostvaruje vezu s drugim sustavima iz okoline

- **upravljanje** je bitna odlika svakog informacijskog sustava i zato o njegovoj djelotvornosti ovisi skladnost funkcioniranja i učnkovitost svih komponenti

- da bismo to mogli postići,moramo imati informacije o funkcioniranju samog sustava, njegovu unutrašnjem ustrojstvu,rezultatima rada i odnosu prema okolini (svaki nedostatak ima za posljedicu nedovoljnu organiziranost što može dovesti u pitanje i opstanak sustava)

- **entropija sustava** - pogrešna ili nedovoljna organiziranost te slaba informiranost o stanju sustava

- što je bolja organiziranost i veća sređenost sustava to je manja mogućnost da se ugrozi njegova cjelovitost,a veća vjerovatnost potpunijeg ostvarivanja normalnog,očekivanog i željenog

*Primjer! Pravosudni sustav*

*- ako ministar/ministrica pravosuđa nema informacija o stanju sustava,njegovim rezultatima i odnosu s drugim sustavima iz njegove okoline,možemo očekivati da će se entropija povećati što bi se moglo odraziti i na opstojnost samog sustava*

- budući da je funkcioniranje svakog sustava,pa tako i informacijskog,neposredno ovisno i ulaznim i izlaznim varijablama,tako **informacijski sustavi mogu biti:**

**a) upravljani** kada je ulaz veći od izlaza

**b) neutralni** kada je ulaz jednak izlazu

**c) upravljački** kada je ulaz manji od izlaza(najvažniji i najugroženiji)

- upravljački inf.sustav se često naziva **integralnim(integriranim) informacijskim sustavom** koji ima **4 temeljne aktivnosti:**

**1)** prikupljanje podataka i informacija

**2)** obrada podataka i informacija te proizvodnja potrebnih informacija

**3)** memoriranje podataka i informacija

**4)** distribucija informacija prema krajnjem korisniku

- tek će krajnji korinsik moći učinkovito odlučivati i upravljati

- u suvremenim uvjetima rada se sve više javlja **komunikacija**( pred informacijske sustave se stavljaju novi zadaci,tako da se postojeće funkcije-prikupljanja,obrade,pohranjivanja i distribucije- proširuju svestranom komunikacijom s dr.sustavima)

- u suvremenim uvjetima rada funkcija komunikacije ima šire zahtjeve i ciljeve : osiguranje komunikacije između djelatnika,zajednički rad na projektima,koordinaciju zajedničkih poslovnih aktivnosti,komunikaciju s vanjskim suradnicima,informiranje,reklamiranje i poslovanje s komitentima,..

- da bi ispunio te funkcije i zadatke informacijski sustav mora bti tako izgrađen i organiziran da posjeduje sve dijelove i elemnte koji su za to potrebni,a oni zajednički čine sređenu strukturu informacijskog sustava

- sastoji se od **6 glavnih dijelova** koji u ustaljenoj praksi nose nazive u kojima se kao prefiks koristi izraz **ware**(roba) :

**a) hardware-** materijalna osnovica koju čini informatička tehnologija

**b) software-** nematerijalni elementi u obliku programskih rješenja i „paketa“ rutina i metoda u primjeni hardvera

**c) lifeware-** informacijski djelatnici koji rade s inform.tehnol. kao profesionalni informatičari ili korisnici sustava

**d) orgware-** organizacijski postupci,metode i načini povezivanja navedene 3 komponente u skladnu i funkcionalnu cjelinu

- sastavni dio orgawarea čine i interni propisi koji se odnose na način i uvjete korištenja informacijskim sustavom te odgovornost onih koji su ovlašteni pristupiti samom sustavu poput djelatnika,administratora,vanjskih suradnika i dobavljača

**e) netware-** koncepcija i realizacija komunikacijskog povezivanja elemenata sustava u skladnu cjelovitu informatičku mrežu

**f) dataware-** koncepcija i organizacija baza podataka i svih raspoloživih informacijskih resursa

- za uspješno funkcioniranje inform.sustava potrebno je da svi ti dijelovi imaju podjednaku razinu kvalitete i međusobne usklađenosti

- njihovo uzajamno povezano i međuzavisno djelovanje tvori jedinstveni proces transformacije ulaza u izlaze,primanja i prerađivanja sirovih podataka,njihovo obrađivanje i memoriranje te dostavljanje podataka i informacija zainteresiranim korisnicima

- to pretpostavlja angažiranje odgovarajućih kadrova – menadžera,pravnika i informatičara u prvom redu 🡪 o tome ovisi uspješnost djelujućeg inf.sustava(provodi se veća demokratizacija informacijskih i komunikacijskih aktivnosti)

**4.1.3. Načela informacijskog sustava**

- u **tehničkom smislu**,informacijski sustav čine kompjutori,komunikacijski uređaji, kompjutorske i komunikacijske mreže te podaci i informacije koje se mogu pohraniti, obraditi,ponovo koristiti ili njima prenijeti,ukljućujući programe,dokumentaciju i postupke za njihov rad,korištenje ili održavanje

- pri funkcionalnom određenju inf.sustava valja poći od tradicionalnih aktivnosti koje se obavljaju unutar tog sustava,ali i novih zahtjeva koje suvremeni način rada i poslovanja stavlja pred njih

- to se odnosi ponajviše na zahtjeve u odnosu na komunikacije unutar same oragnizacije kao i organizacije s okolinom

- informacijski sustav u **funkcionalnom smislu** je takav sustav koji nam omogućava da prikupljanjem i obradom podataka dobijemo i pohranimo informacije koje će poslužiti ovlaštenim osobama da na osnovi njih odlučuju i upravljaju,komuniciraju i razmjenjuju podatke unutar organizacije i organizacije s okolinom

- u našem zakonodavstvu određenje pojma inform.sustava može naći u Zakonu o informacijskoj sigurnosti koji ga definira kao „komunikacijski,računalni ili drugi elektronički sustav u kojem se podaci obrađuju,pohranjuju ili prenose,tako da budu dostupni i upotrebljivi za ovlaštene korisnike“

- sastav,djelatnost i cilj inf.sustava određuju **3 temeljna načela**

**1) načelo učinkovitosti**

**2) načelo ekonomičnosti**

**3) načelo sigurnosti**

**Načelo učinkovitosti**

- odnosi se u 1.redu na pravovremenost,dostupnost i valjanost informacija

- zahtjevi za pravovremenošću i dostupnošću informacija razumljivi su s aspekta njihovih korisnika koji na osnovu njih odlučuju

- problem valjanosti informacija se u tijeku 21.st. promijenio

- **David Shenk: Data Smog** **(Pretjerane informacije)** (dok je informacija prije bila nešto dragocjeno poput kavijara,danas je ima u izobilju poput krumpira(to utječe na poslovne i međuljudske odnose)

- u zadnjih 30 godina je proizvedeno više informacija nego u zadnjih 5000 godina (dnevno svijet bilježi 20 milijuna tehničkih informacija)

- u tim uvijetima više nije pitanje kako doći do informacija,nego kako iz tog mnoštva odabrati one prave informacije (to danas postaje primaran cilj svakog informacijskog sustava)

- od „informacijske krize“ na poč.stoljeća došli smo na njegovom kraju do „informacijskog zagađenja“ čemu je ponajviše pridonijeo Internet neselktivnošću sadržaja koje nudi

- traže se tehnička rješenja,a velike nade se polažu u programska rješenja koja se zasnivaju na umjetnoj inteligenciji

- primjer takvog kompjutorskog programa su tzv. **inteligentni agenti**,koji za korisnika prikupljaju informacije iz njegovog okruženja,najčešće s interneta (vrlo su pokretljivi jer u pravilu nisu vezani za hardversku ili softversku platformu na kojoj rade,mogu uzajamno djelovati s drugim agentima,a njihov autor ili korisnik ne mora ni znati kuda se pritom kreću)

- na prvi pogled je to vrlo djelotvorno rješenje za novonastale probleme,ali suprotno pokazuje dopis iz japanskih novina Nikkei Weekly o prvom **„korisnom virusu“** prema kojem je „grupa s Tokyo Institute razvila virus koji putuje širom kompjutorske mreže,prikuplja informacije, rješava probleme i izvještava o svojim nalazima rukovoditelje mreže“

- usporedimo li ih s kompjutorskim virusima,uočavamo sličnosti:samostalnost,orjentiranost ciljnoj aktivnosti,samopokretljivost,vremenska stalnost,pokretljivosti prilagodljivost

- **njihovim djelovanjem može doći do:**

**1)** neovlaštenog pribavljanja poslovnih tajni

**2)** narušavanja zakona o autorskom pravu

**3)** narušavanje prava na privatnost

**4)** neovlaštenog pristupa tuđim kompjutorskim sustavima i presretanja komunikacija

- budući da je riječ o manipulacijama koje u većini razvijenih zemalja jesu kaznena djela, njihovo buduće korištenje će biti upitno,a pribavljanje informacija otežano 🡪 biti će potrebno naći kompromis između tih oprečnih zahtjeva pri čemu odlučujuću ulogu imaju proizvođači softvera

- drugi problem koji se javlja je bojazan da će koločina informacija premašiti postojeće kapacitete njihove pohrane,a to je rezultat ekponencijalnog rasta količine informacija,a time i samog znanja

- **Buckminster Fuller,** tvorac tzv. **„Krivulje udvostručenja znanja“** , je zaključio da se od 1900.g. ljudsko znanje udvostručavalo približno svakog stoljeća(do kraja 2.Svj.rata znanje se udvostručavalo svakih 25 godina)

- danas različite vrste znanja imaju različite stope rasta(npr. znanje iz nanotehnologije se udvostručuje svake 2 god., klinička znanja svakih 18 mjeseci,a ljudsko znanje se u prosjeku udvostručuje svakih 13 mjeseci,prema IBM-u izgradnja „Interneta stavri“ dovest će do udvostručenja svakih 12 sati)

- **International Data Corporation** (IDC,tvrtka koja se bavi istraživanjem globalnog tržišta) je izvijestila da je granica od jednog zetabajta premašena već 2010.g.,a 2011.g. količina inf. je nadmašila 1,8 zetabajta(1,8 trilijuna gigabajta) te prognozira da će količina podataka do 2020.g. porasti na 40 zetabajta

- **Eric Schmidt** (glavni izvršni direktor tvrtke Google,Inc.) je izjavio da je od početka civilizacije do 2003.g. stvoreno oko 5 eksabajta informacija,dok se danas toliko stvara svaka 2 dana

- pojam **Velikih podataka (Big Data)** se koristi za opisivanje tako velikih i složenih setova podataka tako da oni postaju problem za rad korištenjem standardnim statističkim softverom

- to je rezultat hipertrofije podataka i sve veće povezanosti inf.-komun. sustava,zbog čega dolazi do tzv.**informacijske krize**

- u takvim uvjetima nastaju nova inovativna tehnička rješenja koja omogućuja da se kriza prebrodi,a rješenje je električni **tabulirajući stroj Hermanna Holleritha**

**Načelo ekonomičnosti**

- proizlazi iz zahtjeva da ulaganja u razvoj,održavanje i rad informacijskog sustava budu razmjerni koristima koje od njihova rada imaju korisnici,tj.nadsustav čiji su sastavni dio

- to proizlazi iz činjenice da je uvođenje,održavanje i upotreba informatičke tehnologije vrlo skupo,dok ona istovremeno zastarijeva

- neposredne troškove same implementacije,održavanja i upotreba informacijskog sustava je lako utvrditi uvidom u izdatke učinjene u tom pogledu što nije slučaj s procjenom koristi koju do njihova rada imaju korisnici,tj.organizacija čiji je on dio

- **neposredne koristi** moguće je procijeniti i kvantificirati jer izravno utječu na samo poslovanje organizacije,dok su **posredni učinci** teško mjerljivi jer ih je teško sagledati i kvantificirati,a mogu djelovati tijekom nekog dužegili kraćeg razdoblja

- analizu i specifikaciju troškova i koristi potrebno je napraviti prije početka rada,ali i naknadno ponavljati,pa se u tu svrhu primijenjuju na razne načine metode kvantifikacije neposrednih i posrednih troškova informacijskog sustava,kako bi se utvrdila ekonomičnost

**Načelo sigurnosti**

- prije se pitanjima sigurnosti nije pridavala velika pažnja jer se sigurnost postizala već samom kontrolom i fizičkim ograničenjem pristupa sustavima

- prelaskom na daljisnki rad,potom na mrežni,a poslije i na uporabu interneta u radu,inform. sustavi se sve više otvaraju prema okolini što otvara nove načine manipulacije i manju sigurnost

- nesmetan rad je moguć samo prividom načela sigurnosti

- pri definiranju načela sigurnosti valja poći od **Smjernica za sigurnost informacijskih sustava** Organizacije za ekonomsku suradnju i razvoj koje se **temelje na 9 načela:**

**1) načelo odgovornosti** (odgovornost i obveze moraju biti jasne)

**2) načelo svjesnosti** (osobe bi odmah trebale biti sposobne i odlučne održavati sigurnost)

**3) načelo etičnosti** (inf.sustavi i sigurnost inf.sust. trebaju biti osigurani i korišteni tako da se poštuju prava i legitimni interesi drugih)

**4) načelo multidiscipliniranosti** (mjere,radnje i postupci sigurnosti trebaju voditi računa i uzeti u obzir sva relevantna razmatranja i stajališta)

**5) načelo proporcionalnosti** (sigurnosni nivoi,troškovi,mjere,radnje i postupci trebaju biti razmjerni vrijednosti i stupnju očekivanja od inf.sustava i odgovarati jačini,vjerovatnosti i širini potencijalne štete)

**6) načelo integracije** (mjere,radnje i postupci sigurnosti moraju biti usklađeni i spojeni međusobno kao i s drugim mjerama,radnjama i postupcima organizacije)

**7) načelo pravodobnosti** (javne i privatne stranke moraju postuapti na pravovremen i usklađen način)

**8) načelo ponovne procjene** (sigurnost inf.sust. treba periodično preispitati)

**9) načelo demokratičnosti** (sigurnost inf.sustava mora biti u skladu s demokratskim društvom)

- **načelo sigurnosti podrazumijeva** utvrđivanje odgovornosti za sigurnost inform. sustava i razvoj svijesti o mogućim opasnostima i protumjerema,pri čemu valja uzeti u obzir sva razmatranja i stavove te primiejniti suvremene mjere zaštite koje će biti usklađene s drugim mjerama unutar organizacije

**4.1.4. Mjesto i uloga informacijskih sustava u izgradnji informacijskog društva**

- informacijsko društvo je posve nova ljudska zajednica izrasla na postindustrijskom visokotehnološkom revoluciranju,s načinom proizvodnje i odnosima proizvodnje i komuniciranja koji donose radikalan zaokret u povezivanju,organiziranju i sve interaktivnijem nastupu i djelovanju društvenih subjekata u lokalnim,nacionalnim,širim regionalnim globalnim razmjerima

- sada se u doba brzog informacijskog transformiranja sve mijenjanjem čvršće povezuje i sjedinjuje,tj.integrira u jedinstveni inform.sustav na svim razinama i u svim sredinama

- njegovi se elementi i dijelovi mogu shvatiti i objasniti samo proučavanjem i izlaganjem koje od samog početka uzima u obzir i stalno ima na umu cjelinu i njenu okolinu,radi čega primijenjuje sistematsku metodu,a za polazište ima holističku paradigmu

- samo se zbog te promjene može funkcioniranje i djelotvornost suremenih informacijskih sustava smišljeno anticipirati i planski odvijati na temelju unaprijed izrađenog računalnog programa

- uz to ide druga značajna osobina informacijskog društva koja zahtijeva da se umjesto propitivanja prošlosti isadašnjosti prijeđe na kibernetičko proučavanje sadašnjosti i budućnosti

- danas se promjene događaju u desetljetnim,godišnjim,mjesečnim ili čak kraćim razdobljima te je proučavanje cjeline sistemskom metodom jedini put kojim se ona može sagledati i po potrebi mijenjati

- proučavanje i skladno razvijanje informacijskih sustava u pojedinačnim,grupnim,lokalnim, nacionalnim,regionalnim i globalnim društvenim djelovanjima ima istaknuto mjesto i prvorazrednu ulogu u teoriji i praksi modernog zajedništva,tj.u izgradnji i sve ubrzanijem razvoju informacijskog društva

- smatra se da je njegova izgradnja počela već 50-ih 20.st. u najrazvijenijim sredinama kad je broj „bijelih ovratnika“ nadmašio broj „plavih ovratnika“ (1991.g. se oblikovalo dominantno informacijsko društvo i ta se godina uzima kao godina razgraničenja starog industrijskog društva i novog informatičkog društva)🡪 taj zaokret je vidljiv iz odnosa cijena sirovina i usluga

- taj razvoj nije jednak u svim zemljama što potvrđuje da je još na snazi zakon neravnomjernog razvitka pojedinih poduzeća,drugih organizacija,nacionalnih zajednica,pa i širih svjetskih regija

- u transferu informatičke tehnologije,njezinom monopolističkom iskorištavanju i širenju kompjutorskih mreža, je prisutna pojava tehnološkog imperijalizma,kolonijalizma i hegemonizma

- starim oblicima i metodama iskorištavanja,zakidanja i zloupotrebljavanja međusobnih transakcija,priključuju se sada i novi,teži i opasniji oblici kibernetičkog kriminala neovlaštenim upadom u računalne sustave,telekomunikacijske mreže i baze podataka

**4.2. Pravna informatika**

- razvoj pravne informatike možemo pratiti od početka 50-ih g. 20.st.

- paralelno s razvojem informacijske tehnologije dolazi do njihove primjene u pravu

- informacijski sustavi sred.80-ih 20.st. postaju neizostavno pomagalo pravnoj struci ( digitalizacija pravnih izvora,razvoj specijaliziranih inform.sustava poput Celex-a i Westlaw-a, izrada prvih baza podataka u javnoj upravi)

- nove tehnologije za pohranu podataka i napredak na području primijenjene umjetne inteligencije 90-ih su temelj za sveobuhvatnu informatizaciju i integraciju infor.tehn. u poslovne procese

- u budućnosti se očekuje šira primjena specijaliziranih ekspertnih sustava u pravu na području simulacije postupka i rješavanja pravnih pitanja

- promjene u RH su započele 2002.g. kada je Vlada donijela strateški dokument **Informacijska i komunikacijska tehnologija-Hrvatska u 21.stoljeću**

- 2002.g. je potpisan **Dnevni red za jugoistočnu Europu** (eSEE Agenda) kojim je preuzeta obveza usklađivanja zakonodavstva s pravnom stečevinom EU na području informacijskog društva

- krajem 2003.g. Vlada je usvojila **Program e-Hrvatska 2007.** koji obuhvaća preporuke kako da se hrvatsko društvo transformira u informacijsko društvo sukladno preporukama i odrednicama Akcijskog plana e-Europe 2005. Europske unije

- **temeljni ciljevi tog programa**:

**a)** omogućiti građanima i poduzetnicima pravovremeno primanje informacija i aktivno sudjelovanje u društvu preko umreženog informacijskog sustava

**b)** osnaženje i povezivanje hrvatskog gospodarstva

**c)** sveobuhvatna razmjena informacija i iskustava u poslovnome svijetu i poduzetništvu

**d)** opremanje države da pstane transparentan,brz i učikovit servis

- od tada do danas se ostavruju razni programi,od kojih su **najznačajniji:**

**1) e-Uprava**- projekti poput e-Matice,Popis birača, Središnjeg registra zbirki osobnih podataka te Projekta uspostave višenamjenskog prostornog informacijskog sustava

**2) e-Pravosuđe**- e-Zemljišni izvadak, e-Katastar, e-Sudski registar, e-Sudska praksa, e-Oglasna ploča i umrežavanje sudova, Sudačka mreža te e-Ovrha

**3) e-Obrazovanje**- uključuje Hrvatski nacionalni obrazovni standard,povezivanje osnovnih i srednjih škola na internet,pokretanje osnovne edukacije na području informatike i novih tehnologija te stjecanja znanja temeljenog na ECDL standardu

**4) e-Zdravstvo** – HZZO portal usklađen s projektom informatizacije zdravstvene zaštite

**5) e-Poslovanje-** e-REGOS, e-PDV, e-Nautika, e-Carina

- u kratkom razdoblju doneseni su mnogi zakoni poput ZET,ZZOP,ZEK,ZEM,ZAPSP,ZEI,ZEP, ZTP,..

**4.2.1. Ciljevi i dosezi projekta e-Pravosuđe**

- proteklih se godina pristupilo intezivnoj reformi i reorganizaciji pravosudnog sustava

- reforma se nastoji provesti racionalizacijom sudačke mreže u skladu s kriterijima učinkovitosti i svrsishodnosti,povećanjem fleksibilnosti u sudskim postupcima ustupanjem predmeta s preopterećenih na manje opterećene sudove,učinkovitim upravnim nadzorom nad radom sudaca,njihovim rasterećenjem od administrativnih i pomoćnih poslova,razvojem alternativnih načina rješavanja sporova te permamnentnom edukacijom pravosudnih djelatnika radi usavršavanja i daljnjeg napredovanja u karijeri

- **važan cilj takve reforme** je uspostava modernog,učinkovitog i transparentnog hrvatskog pravosuđa koje će omogućiti brzo rješavanja sudskih predmeta u skladu s ustavnim pravom na pravično suđenje u razumnom roku

- važno je provođenje programa **e-Pravosuđe,**kao integralnog dijela cjelovitog programa e-**Government Republike Hrvatske**

- provedbom programa e-Pravosuđe omogućeno je da se efikasnije počne s rješavanjem nagomilanih neriješenih predmeta te pretvorbe i verifikacije zemljišnih knjiga u digitalni oblik (time su stvoreni pravni i tehnički uvjeti za stvaranje zajedničke Baze zemljišnih podataka)

- prednosti uvođenja elektroničkog poslovanja i umrežavanja ogledaju se u reorganizaciji dostave,uključujući i dostavu podnesaka putem e-pošte,kao i međusobnu komunikaciju izgradnjom informacijsko-komunik. infrastrukture pravosudnog sustava i uvođenja automatiziranog sustava poslovanja

- Ministarstvo pravosuđa je proteklih godina pokrenulo niz projekata(digitalizacija zemljišnih knjiga,jednostavnija registracija poslovnih subjekata s pomoću elektroničkog suskog registra trgovačkih sudova te digitalizacija kaznene i prekršajne evidencije)

- jedna od bitnih komponenti e-Pravosuđa je projekt **Jedinstvenog informacijkog sustava za upravljanje sudskim spisima- e-Spis**

- zadatak e-Spisa,kao i dr. sličnih sustava poput **JCMS**-a (**Joint Court Managment System**,tj. sustav **Prekršajnog upisnika**) ili sustava koji razvija i rabi Državno odvjetništvo RH(**CTS,case tracking system**) neposredno će utjecati na povećanje učinkovitosti rada sudova i državnog odvjetništva te racionalizirati,automatizirati i ubrzati sudske i druge postupke

- **cilj svih sustava za upravljanje predmetima je:**

**1)** omogućiti efikasnije praćenje predmeta od podneska kojim se pokreće postupak do odluke kojom se predmet zatvara te smanjiti mogućnost postupovnih grešaka

**2)** omogućiti sucima i državnim odvjetnicima veću sposobnost upravljanja radnjama u predmetu

**3)** omogućiti višu razinu transparentnosti u radu sudova te uvid u stanje postupka fizičkim i pravnim osobama

**4)** osigurati uvjete za kontrolu kvalitete i brzine rada sudaca i djelatnika u pravosuđu te preventivno utjecati na pojave poput korupcije

- informatizacija rada sudova uključuje elektroničku komunikaciju sudova,stranaka, odvjetnika,državnih odvjetnika i dr.subjekata u postupcima,a ujedno uključuje i elektroničku komunikaciju sudova i tijela državne uprave poput ministarstava,agencija,državnih upravnih organizacija te tijela lokalne i regionalne uprave i samouprave te mogućnost dohvaćanja podataka iz raznik elektroničkih registara

- uvođenjem jedinstvenog internetskog portala Ministarstva pravosuđa omogućen je izravan pristup raznim pravnim izvorima i registrima,poput online oglasnih ploča svih sudova u RH, dok je građanima omogućen brz pristup informacijama o funkcioniranju pravosudnog sustava

- postojeći portali(uključujući portal MP-a) imaju bitno ograničen domet i obuhvat te ne daju pravi i cjelovit uvid u to područje,niti mogu zadovoljiti sve veće potrebe širokog kruga domaćih i stranih pravnih i fizičkih osoba

**4.2.2. Potreba izgradnje cjelovitog pravnog informacijskog sustava RH**

- budući da suvremeno,postmoderno informacijsko društvo uvelike ovisi o dostupnosti i opotrebi digitalnih informacija i elektroničkih servisa ,nedostatak jedinstvenog i sveobuhvatnog pravnog internetskog portala utječe na ostvarivanje prava i ispunjavanje obveza pravnih i fizičkih osoba u RH

- osnovu pravnog internetskog portala činile bi postojeće elektroničke baze podataka Narodnik novina i sudova koje bi trebalo sustavno obuhvatiti,obraditi,klasificirati i dopuniti postojećim domaćim i stranim pravnim izvorima

- trebalo bi ponuditi i nove elektroničke usluge,odnosne sadržaje koji ne postoje na našem tržištu,a prilagođeni su suvremenim oblicima elektroničke komunikacije i poslovanja

- tijekom proteklih godina u RH pokrenuti su razni projekti i poduzete brojne aktivnosti jedinstvenog pravnog internetskog portala (taj cilj još nije postignut jer je pravosuđe ponajviše zaokupljen implementacijom **Integriranog sustava upravljanja sudskim predmetima(ICMS)** namijenjenog praćenju kretanja predmeta od zaprimanja do donošenja presude te uspostavom jedinstvene i sveobuhvatne računalne mreže između sudova i drugih organa i institucija javne vlasti)

- taj projekt je bio teško provediv,a i neučinkovit i neracionalan u praksi,pa se pristupilo izgradnji i implementaciji informacijskih sustava koji su primjereniji našim mogućnostima,a trebaju pridonijeti većoj učinkovitosti pravosuđa

- **to se odnosi na:**

**1) e-Spis** – jedinstven sustav za upravljanje sudskim predmetima(ICMS-Integrated Court Case Managment System)

- **svrha e-Spisa** je izgradnja informacijskog sustava koji će omogućiti: efikasnije upravljanje sudskim predmetima,učinkovitiji rad sudskog osoblja,bržu i bolju uslugu građanima, transparentno upravljanje i otklanjanje korupcijskih učinaka,pomoć pri donošenju odluka i učinkovitiju zaštitu prava građana

**2) CTS(Case Tracking System)** – sustav za praćenje kaznenih prdmeta Državnom odvjetništvu kojim se poboljšava njihova učinkovitost u redovnom obavljanju poslova iz njihovog djelokruga

- **sustav CTS omogućava**: pristup informacijama o statusu predmeta u realnom vremenu, kontrolu kretanja predmeta po poslovnim procesima,kvalitetniji nadzor nad radom državnih odvjetnika i objektivnu procjenu njihovog rada i učinkovitiju administraciju i upravljanje operacijama

- prisutne su brojne slabosti poput nepostojanja elektroničke komunikacije između suda i stranaka,odnosno njihovih zastupnika te nepotpune digitalizacije cijelih sudskih spisa

- u sustav se ne pohranjuje tekst podnesaka,priloga i ostalih dokumenata

- bilo je pokušaja da se uspostavi **Jedinstveni pravni internetski portal MP-a**

- **pravni internetski informacijski sustavi mogu se podijeliti s obzirom na vlasništvo na:**

**a)** javne

**b)** privatne

**- javni elektronički izvori pravnih podataka u RH:**

**1)** e-portal Ministarstva pravosuđa

**2)** e-Zemljišni izvadak

**3)** e-Katastar

**4)** e-Oglasna ploča sudova

**5)** Sudačka mreža

**6)** e-Sudski registar trgovačkih društava

**7)** e-Sudska praksa Vrhovnog suda

**8)** Državno odvjetništvo RH

**9)** Ustavni sud RH

**10)** Upravni sud RH

**11)** Visoki trgovački sud RH

**12)** Pučki pravobranitelj RH

- **privatni elektronički izvori pravnih podataka u RH:**

**1)** Hrvatski portal „Legalis“

**2)** ANDALL pravni portal

**3)** IUS-INFO

**4)** Inženjerski biro

**5)** Intelectio Iuris

**6)** Korekt d.o.o.

**7)** Lex info d.o.o.

**8)** Centar za managment i savjetovanje-komercijalni

**- najvažniji strani elektronički izvori pravnih podataka u EU:**

**1) SCADPlus** Summaries of Legislation –nužni sažetak zakonodavstva u 32 područja aktivnosti EU

**2) EUR-Lex**- Ured za službene publikacije Eurospkih zajednica je novi elektronički servis nastao spajanjem pravne baze podataka Celex i prijašnje verzije EurLexa čime se nastojalo objediniti dobre strane te 2 baze podataka i ponuditi jedinstveni servis za pristup europskom pravu

- sadrži podatke o osnivačkim ugovorima,pripremnom,usvojenom i konsolidiranom zakonodavstvu,sudskoj praksi Europskog suda,pitanjima postavljenima u Europskom Parlamentu i dokumentima od općeg interesa

**3) Praksa Suda EU** –omogućava pretraživanje sudske prakse Europskog suda pravde

**4) Praksa Europskog suda za ljudska prava**- omogućava uvid u važeće međunarodne ugovore i sudsku praksu Europskog suda za ljudska prava

- osim navedenih,važni su i drugi izvori poput **Opće uprave za proširenje Europske komisije** (TAIEX National Legislative Databases) koja sadrži veze na elektroničke baze s nacionalnim zakonodavstvima zemalja EU,te **JHA baze** Vijeća EU s raznim dokumentima iz područja pravosuđa i unutarnjih poslova

- postojeći elektronički izvori podataka u RH su jako slabi,pa je potrebno izgraditi novi internetski portal koji bi obuhvaćao,osim postojeće elektroničke građe Narodnik novina, i javno dostupne podatke iz ostalih domaćih i stranih elektroničkih izvora te podatke dobivene od relevantnih znanstvenih,pravosudnih i dr.izvora koji takve podatke prikupljaju,obrađuju i javno prezentiraju

- **svrha i cilj jedinstvenog pravnog internetskog portala e-pravosuđa** mogla bi se sažeti u 6 točaka:

**1)** ažurno objavljivanje tekstova novih zakona i podzak.akata,pročišćenih zakonskih tekstova i obavještavanje o njihovom stupanju na snagu kao i informiranje o propisima koji su prestali vrijediti

**2)** brz pristup pročišćenim zakonskim tekstovima i podzakonskim aktima koji su doneseni na temelju njih

**3)** jednostavno i složeno pretraživanje podataka s pomoću jedinstvenog pretraživača koji omogućava pretragu po raznim kriterijima,kako u naslovima tekstova tako i unutar samih dokumenata

**4)** uvidom u relevantnu sudsku praksu omogućiti ujednačavanje sudske prakse sa upoznavanjem sudaca sa sadržajem pravomoćnih sudskih odluka,posebno odluka Ustavnog suda,Vrhovnog suda,Visokog trgovačkog suda i Upravnog suda RH

**5)** dostupnost važećih obrazaca u e-obliku te upute o njihovom popunjavanju i načinu podnošenja trebaju olakšati građanima ispunjavanje njihovih obveza i ostavrivanje njihovih prava

**6)** uspostavljanje novih elektroničkih usluga i servisa koje se još nude u RH

**4.3. Pravo informacijskih tehnologija**

**4.3.1. Pravo agrarnog i industrijskog društva**

- u doba agrarizma i industrijalizma glavna zadaća prava je da održi i sačuva vladajući društveni poredak

- u doba informacionalizma glavna zadaća prava je omogućiti permanentni materijalni i društveni razvitak,tj.stvoriti uvjete za revulucionarne društvene promjene koje se sve brže i češće događaju

- zbog toga se na pravo može gledati kao skup normi koje primjenom državne prisile reguliraju ponašanje fizičkih i pravnih osoba te kao komunikacijski i informacijski fenomen koji stvara mogućnost da se čovjekovo ponašanje predvidi i pravovremeno usmjeri

- zloporabe u agrarnim i indutrijskim društvima uspješno se obuzdavalo zakonskim propisima koji su precizno razdvajali dopušteno od nedopuštenog,korisno od štetnog,zdravo od bolesnog

- središnje mjesto u svim tim zbivanjima ima **vlasništvo**,kojemu je ishodišna točka,sadržajna jezgra i metafora - **fizička „imovina“**

**-** zakonodavstvo agrarnog i industrijskog društva je potanko uređivalo uvjete i granice njegova prisvajanja i korištenja te se svako nepoštivanje i prekoračenje toga smatralo kažnjivim djelom

- tako „ograničena“ stvarnost odgovarala je tadašnjem stupnju materijalnog i društvenog razvoja,omogućavala je osamostaljenje individuuma i funkcioniranje društvenih organizacija i zajednica te osiguravala na taj način ostvarivanje i zaštitu pojedinačnih,grupnih i općih interesa

- kad su u predmet ušle i netjelesne stvari (nevidljiva prava poput naknada za pronalaske, pohranjene novčane iznose,neostvarenu dobit),pravni sustavi proširuju svoju nadležnost i svoj utjecaj na to područje

- to područje ubrzo postaje njihova preokupacija,pa već tijekom 2.svj.rata **A.Schumpter** konstatira(u knjizi **Kapitalizam,socijalizam i demokracija**) da je „papirnato vlasništvo“ prevladalo i da je pravna regulativa ponajviše njime zaokupljena

- intelektualno vlasništvo je uskoro postalo objektom zaštite zakonodavstva gotovo svih zemalja

- sve više je stvari,prava i potraživanja smješteno u digitalnom i umreženom svijetu

**4.3.2. Pravo informacijskog društva**

- današnja digitalna kultura be podnosi stalnost i nepromjenjivost

- svojstvene su joj neprekidne mutacije,skokovite promjene i sve složenije inovacije i kombinacije digitalnih podataka,programa i usluga

- pravni sustavi nisu toliko fleksibilni da bi se toj promjeni istom brzinom prilagođavali i tako brzo mijenjali zbog čega treba težiti pravovremenoj **transformaciji** postojećeg pravnog sustava na način i u mjeri koja prati transformiranje industrijskog u informacijsko društvo

- pravo nikad nije bilo pasivni suputnik društvenog razvoja

- aktivno je u tome sudjelovalo: stvaranjem povoljnijih uvjeta i okvira napretka,poticanjem i angažiranjem gospodarskih i društvenih subjekata te sprječavanjem i kažnjavanjem zloupotreba

- takva uloga prava u informacijskom društvu nailazi na brojne poteškoće koje proizlaze iz okolnosti da su sada glavni objekt zaštite netjelesna dobra i nevidljive veze kojima se ona razmjenjuju

- virtualna elektronička realnost je postojeća društvena stvarnost,podjednako prisutna u stvarima,dužnostima,pravima i odnosima kao i sam fizički svijet koji nas okružuje

- prisutna digitalna kultura egzistira kao i naslijeđeni fizički svijet u svemu što je objekt i učinak čovjekova svakodnevnog djelovanja i življenja i ona se izražava pomoću naše aktivnosti i makar ne podliježe fizičkim i prirodnim zakonima,objekt je pravnog interesa

- najveća prijetnja razvoju je „kašnjenje“ pravne regulative,a ono je upravo obilježilo cijelu drugu polovinu 20.st. kada je riječ o inf.-komunik. tehnologijama i njima izazavanim društvenim promjenama

- te promjene i nove odnose te njihove mnogobrojne interakcije izučava **Pravo informacijskih tehnologija**

**4.3.3. Područje regulacije**

- pravo informacijskih tehnologija izučava pravnu regulativu kojom se uređuju prava, obveze i odgovornosti pravnih i fizičkih osoba na područjima koji su rezultat raznih aspekata interakcije prava i informacijskih tehnologija,kao i mogućnost njenog unapređivanja

- **aktivnosti nacionalnih zakonodavstava i međunarodnih i regionalnih organizacija i udruženja osvijale su se slijedećim rasporedom:**

**1)** zaštita baza podataka s osobnim podacima građana

**2)** zaštita od računalnih,odnosno kibernetičkih zloporaba

**3)** zaštita intelektualnog vlasništva

**4)** zaštita drugih prava i interesa na području elektroničkog poslovanja

**5)** informacijska sigurnost i strategije kibersigurnosti i kiberkriminala

**6)** upravljanje internetom i regulacija interneta

**5.CJELINA: Privatnost i zaštita osobnih podataka u digitalnom okruženju**

- političke korijene ljudskih prava nalazimo već u Velikoj povelji koju je 1215.g. bio prisiljen potpisati engleski kralj,priznajući građanima određena prava

- neka prava su priznata u Deklaraciji o nezavisnosti 1776.g., Deklaraciji o pravima čovjeka i građanina 1789.g., Općoj deklaraciji o ljudskim pravma UN-a 1948.g. te u Konvenciji za zaštitu ljudskih prava i temeljnih sloboda Vijeća Europe 1950.g. 🡪 njima je priznato neotuđivo pravo svakog pojedinca na određene osobne,socijalne,političke,kulturne i gospodarske slobode i prava te uspostavljen međunarodni sustav zaštite

- zajedničke vrijednosti priznate su i u Povelji o temeljnim pravima EU 🡪 Unija se temelji na nedjeljivim,univerzalnim vrijednostima ljudskog dostojanstva,slobode,jednakosti i solidarsnosti te na načelima demokracije i vladavine prava

- ljudska prava nisu nepromjenjiva kategorija,već su podložna stalnom preispitivanju,širenju i prilagođavanju pod utjecajem neprekidnih promjena u odnosima komuniciranja i ranih oblika gospodarskog,političkog,socijanog i duhovnog života i interakcije

**5.1. Pravo na privatnost i zaštitu osobnih podataka**

**5.1.1. O pojmu i nastanku prava na privatnost**

- privatnost ima korijene iz davnina(npr. u Bibliji,hebrejska kultura,stara Grčka,drevna Kina)- u početku se najčešće radilo o pravu pojedinaca na nepovredivost doma

- danas nema općeprihvaćene definicije privatnosti

- za **Westina** je privatnost „želja ljudi da slobodno biraju pod kojim uvijetima i u kojoj mjeri će izložiti sebe,svoje stavove i svoje ponašanje drugima“

- za **Michaela** je privatnost „pravo pojedinca da bude zaštićen od nedopuštenog zadiranja u njegov osobni život ili posao,njegove obitelji,neposrednim fizičkim mjerama ili objavljivanjem informacija“

- definicija privatnosti u **Black's Law Dictionaryju**, po kojoj je to „pravo biti ostavljen na miru; pravo pojedinca da bude pošteđen od nepravednog publiciteta; i pravo na život bez ovlaštenog miješanja javnosti u stavri koje se javnosti nužno ne tiču“, ukazuje na složenost tog pojma i na razne aspekte tog prava

- **informacijska privatnost** uključuje uspostavu pravila upravljanja,prikupljanja i korištenja osobnim podacima kao što su kreditne informacije ili zdravstveni podaci

- **tjelesna privatnost** se odnosi na fizičku zaštitu pojedinca od raznih postupaka kao što su testiranje na drogu ili pretraživanje

**- komunikacijska privatnost** se odnosi na sigurnost i privatnost pošte,telefona,e-pošte i dr.

**- prostorna privatnost** se odnosi na određivanje granica nedopuštenog miješanja u obiteljsko i drugo okruženje (radno mjesto ili javni prostor)

- **Roger Clark** tome dodaje **medijsku privatnost** koja obuhvaća razne aspekte ljudskog ponašanja,a posebno ono najosjetljivije poput seksualnih slonosti i navika,političkih aktivnosti i vjerskih običaja u privatnom i javnom životu čovjeka

-međunarodno priznanje prava na privatnost uslijedilo je u okviru UN-a izglasavanjem **Opće deklaracije o ljudskim pravima** 1948.g. 🡪 nitko ne smije biti izvrgnut samovoljnom mijepanju u njegov privatni život,obitelj,dom ili prepisku,niti napadima na njegovu čast i ugled te svatko ima pravo na zaštitu zakona protiv ovakvog mješanja ili napada

- 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 RH** jamči se pravo privatnosti svakom njezinom građaninu u svakim njenim aspektima, jamči pravo na prostornu (čl.34.), informacijsku (čl.37.), komunikacijsku (čl.36.) i tjelesnu (čl.23.) privatnost

- u **Deklaraciji o sredstvima javnog priopćavanja i ljudskim pravima** iz 1970.g. 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,nepredstavljanje u krivom svjetlu,neobjavljivanje nepotrebnih i neugodnih podataka,neovlasšteno 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“

- neke od važnijih osobnih razloga općeg priznanja provatnosti nalazimo u radu **Lynn Gillam: Ethics, Privacy and Confidentiality** 🡪 **po njoj je privatnost :**

**a) 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 raznim društvenim okruženjima i s raznim stupnjevima intimnosti u odnosu na druge ljude

**b) važna je za osobni identitet** jer je nužna pri njegovu kreiranju,razlikovanju od drugih ljudi te otkrivanju i kreiranju nas samih

**c)** važna je za **društvene odnose** u koje stupamo jer razne međuljudske odnose karakterizira različit stupanj intimnosti

- **opći razlozi** u prilog cjelovite privatnosti proizlaze iz zajedničkih interesa građana,tj. interesa regionalnih ili nacionalnih zajednica,a neki od njih su:

**a)** ispravljanje nepravdi zbog kršenja ljudskih prava u prošlosti

**b)** promicanje elektroničkog poslovanja,tj.zaštite korisnika od zloporaba njihovih osobnih podataka

**c)** nužnost usklađivanja zakonodavstava s pravnim sustavom EU

**5.1.2. Ograničenja osobnih prava**

- pravo na privatnost i zaštitu, kao i ostala osobna prava, nisu apsolutna, već se mogu ograničiti u točno propisanim uvijetima i to tuđim pravom i slobodama te zakonom

- zakonsko ograničenje nalazimo već u Ustavu koji predviđa da 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 2/3 odlukom Hrvatskog sabora (čl.17.)

- 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 slobodu izražavanja

- Ustav jamći pravo na slobodu mišljenja i izražavanja misli,dok istovremeno zabranjuje cenzuru (čl.38.)

- 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.)

- sloboda izražavanja često ima za posljedicu zadiranje u čast,ugled i privatnost pojedinaca

- **Brandeis i Warren** u radu **The Right to Privacy**,objavljenom u „Harvard Law Review“ 1890.g., po nekima „najutjecajnijem pravnom članku ikad objavljenom“, postavili su temelje prava na privatnost,utvrdili razlike u odnosu na druga prava i prvi odredili njezina ograničenja (ukazali su na potrebu pravne zaštite od slučajeva ugrožavanja i zadiranja žutog tiska u intimni život pojedinca te na nužnost zaštite osobnosti i osiguranja pojedincima onog što je sudac **Cooley** nazvao pravom „biti ostavljen na miru“)

- posebno pitanje se postavlja u vidu privatnosti javnih osoba – po Deklaraciji to predstavlja poseban problem i formula prema kojoj privatni život prestaje tamo gdje počinje javni je nedovoljna za rješenje ovog problema

- po Deklaraciji,osobe koje igraju neku ulogu u javnom životu imaju pravo na zaštitu privantog života osim u slučajevima kada se privatni odražava na javni život te time pto pojedinac ima neku javnu funkciju ne uskraćuje mu se pravo na privatnost

- u praksi Europskog suda za ljudska prava zauzet je 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

- odgovornost za takve informacije ovisit će o istinitosti samih informacija,načinu na koji su prikupljene,mediju putem kojih su priopćene te osobi koja ih je priopćila kao i osobnom pravu koje je time povrijeđeno

- pravo pojedinca na slobodu izražavanja podrazumijeva i njegovo pravo da,osim slobodnog širenja ideja i informacija,prima takve inf. i ideje iz okoline u čemu je djelatnost javnog priopćavanja i javnog glasila od neprocijenjive važnosti

- o dostupnosti informacija ovisi aktivno sudjelovanje građana u političkom,socijalnom, kulturnom i svakom drugom životu

- ova prava se međusobno ne isključuju,nego su komplementarna

- pravo na slobodu izražavanja se odnosi na najrazličitije oblike izražavnja što u praksi može dovesti do uklanjanja ili ograničavanja raznih zabrana

*Primjer! Zabrana izvoza kriptografskog softvera u SAD-u*

*- sud u Kaliforniji je u slučaju Bernstein v. United States Department of Justice proglasio zabranu izvoza kriptografskog softvera neustavnom jer se njome ograničava ustavno pravo slobode govora*

*- Daniel Bernstein(profesor na Sveučilištu Illinois) je razvio enkripcijsku metodu poznatu pod nazivom „Snuffle“,napisao je program koji omogućava njezino korištenje i namjeravao je objaviti izvorni kod na internetu 🡪 tome se suprostavlja niz državnih agencija i ministarstava tvrdeći da to predstavlja povredu Zakona o kontroli izvoza naoružanja(AECA-Arms Export Control Act) u kojem je jaki enkripcijski softver na isto listi s nuklearnim oružjem*

*- nakon što je Bernstein tužio ministarstvo,okružni i žalbeni sud doniejli su presude u njegovu korist*

*- na taj način je prvi put izjednačen programski jezik 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 je imao **dvojak utjecaj:**

**1)** imala je odlučujuću ulogu u širenju informacija i znanja,promicanju ljudskih prava i razvoju svijesti o potrebi njihova priznanja i zaštite

**2)** sveje više poticala i razvijala svijest o potrebi priznanja i zaštite ljudskih prava i temeljnih sloboda

- 2.infor. revolucija je omogućila da se pitanju ljudskih prava pristupi zajednički i ujednačeno

- od 90-ih 20.st.,razvojem,slanjem i komercijalnim korištenjem komunikacijskih satelita za potrebe medija,stvorene su pretpostavke za dostupnost informacijskih tehnologija na širem području 🡪 poznato kao **„CNN efekt“**

- iako CNN-ovim televizijskim prijenosom nasilja i masakra studenata s trga Tiananmen (1989.g.) nije ugrožena kineska vlast i suverenost,može se kazati da su urodili takvim stupnjem reakcije svijeta do koje ne bi došlo da nije bilo tog javnog priopćavanja

- dostupnost i brzina širenja informacija omogućava brzu reakciju svijeta na suzbijanja i sprječavanje takvih pojava

- danas se pojmom CNN efekta koristi kao sinonimom za utjecaj medija na formuliranje vanjske politike kada u nekim regijama i zemljama dođe do humanitarne ili ratne krize (Afganistan,Irak,Sirija)

- odlučujući utjecaj donosi informatička revolucija i širenje interneta (globalnost,otvorenost, dostupnost,decentraliziranost i neovisnost o posebnoj infrastrukturi čine internet jedinstevnim i po mišljenju nekih najdemokratskijim medijem)

- događaji od 11.9.2001.g. u New Yorku,kao i opasnost od informacijskog i kibernetičkog terorizma su pridonijeli nadzoru sve većeg broja ljudi

- sve je više onih koji smatraju da treba ograničiti pristup internetu zbog velikog broja negativnih sadržaja koji pozivaju na rat,nasilje,ubojstva,razne oblike mržnje..

- 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 za suzbijanje aktivnosti političkih neistomišljenika

- **kršenju privatnosti pridonose i brojni trendovi poput:**

**a) globalizacija** – uklanja zemljopisna ograničenja protoku podataka

**b) konvergencija** – vodi ukidanju tehnoloških barijera između sustava koji na taj način međusobno komuniciraju,izmjenjuju i obrađuju razne oblike podataka

**c) multimedija** – spaja razne oblike prijenosa i izražavanja podataka i slika tako da se informacije prikupljene u jednom obliku mogu lakše prevestu u drugi

**d) antiterorizam** – posebno nakon 11.9.2001. ima za posljedicu 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

- tome treba dodati i razne oblike **kiberkriminala** i **kiberterorizma**

- najveća opasnost privatnosti prijeti od javnog sektora,tj.vlasti koje ih mogu ograničiti zakonom ili ugroziti zloporabom tehnologija 🡪 Castells takve tehnologije naziva **tehnologijama kontrole** jer je „kontrola informacija srž državne moći tijekom cijele povijesti“

**5.1.4. Tehnologije kontrole**

- **tehnologije kontrole obuhvaćaju:**

**a) tehnologiju identifikacije** – upotreba lozinki,cookie-datoteka i procedura za provjeru autentičnosti

**b) tehnologiju nadzora** – omogućuju lociranje korisnika,presretanje poruka,praćenje komunikacijskih tokova te nadzor aktivnosti udaljenih računala

**c) tehnologiju istrage** – vezane uz izgradnju baza podataka prikupljenih pomoću obrade rezultata nadzora i pohranjivanja informacija radi njihove daljnje obrade i uparivanja

**a) Tehnologije identifikacije**

- u praksi brojnih zemalja sve se češće koriste identifikacijski sustavi koji omogućavaju fizički ili daljinski pristup nekom računalnom servisu,njegovim resursima i internetskim servisima

- u virtualnom svijetu čovjek ostavlja elektronički trag o svom prisustvu,navikama i interesima bilo na tuđim ili vlastitim računalnim sustavima 🡪 takav je npr. slučaj s **„kolačićima“ (Cookies)** – tekstualnim informacijama pohranjenima u formi datoteka na disku našeg kompjutora kada posjetimo neku internetsku stranicu i oni omogućavaju automatsko spajanje na web-poslužitelj,izbor onoga što želimo vidjeti na stranici,prikazivanje željenih informacija bez dodatnog traženja,prikazivanje oglasa i dr.sadržaja koji nas zanimaju

- korisnici na internetu često daju osobne podatke ili poduzimaju one radnje koje ne bi poduzeli u fizičkom svijetu 🡪 tome posebno pridonose tzv. **web registracijski formulari** koji se ispunjavaju kako bi se moglo pristupiti nekoj internet stranici,tj.sadržajima koje nudi

- prikupljanje,analiziranje i povezivanje takvih podataka uz pomoć informatičke tehnologije te njihovo kombiniranje s već postojećim podacima omogućavaju stvaranje **profila** ljudi, pa zato ne iznenađuje da je sve veći broj tvrtki i pojedinaca,tzv. **informacijskih brokera**, koji prodajom osobnih podataka do kojih su došli nesmotrenošću korisnika,ostvaruju profit

- tržište osobnih podataka je već 1999.g. premašilo vrijednost od 1,5 mlrd. dolara

- osim za markentiške potrebe,ovakvi podaci mogu dovesti i do „krađe identiteta“ i lažnog predstavljanja(najčešća zloporaba za vršenje kaznenih djela poput kompjutorske prijevare)

- sve je veća količina osobnih podataka koji se prikupljaju na raznim web-stranicama,pri čemu je opasnost da se tim podacima koriste i potencijalni poslodavci odlučujući o nečijem zaposlenju

- tako se otvaraju mogućnosti stvaranja tzv. **„podatkovnih utočišta“ (data haven) ili „kriminalnih podatkovnih utočišta“ (criminal data haven)** u manje razvijenim zemljama

- **profiliranje** pojma data haven u najširem smislu uključuje rudarenje (**data mining**) velike količine podataka koji se prikupljaju u postupku skladištenja podataka (**data warehousing**) da bi se potom donijeli zaključci o poveznicama između određenih sadržaja koji se odnose na konkretne osobe da bi se postigao cilj

- pritom se koriste modernom tehnologijom kao što su GPS tehnologija,videonadzor, dubinsko pregledavanje sadržaja paketa prometa koji se prenose mrežom (Deep Packet Inspection,DPI)

- osim u komercijalne svrhe,profiliranje se koristi u svrhu borbe protiv teških kaznenih djela poput terorizma ili upotrebe i nezakonite reprodukcije autorskih djela (postupci profiliranja nisu skupi,a mogu uključivati i praćenje ponašanja pojedinca tijekom upotrebe usluga informacijskog društva kako bi se u odnosu na njih poduzimale ciljane radnje poput ponude personaliziranih oglasa-**online ciljano ili bihevioralno oglašavanja**)

- razmatraju se i pitanja u vezi s primjenom **tehnologije identifikacije putem radiofrekvencije** (**RFID**),posebno RFID uređaja i aplikacija za obradu osobnih podataka i povezivanja u komunikacijske mreže

- ugradnjom RFID etikete svakoj se stvari dodjeljuje jedinstveni identitet 🡪 riječ je o elektroničkom čipu s pohranjenim informacijama koji ima mogućnost komunikacije s radiosignalima s RFID čitačem

- tako RFID čitač može učitati npr. svojstva stvari u kojoj se etiketa ugrađuje

- u RFID etiketi se mogu pohranjivati i osobni podaci koje RFID uređaji/aplikacije mogu čitati, tj. obrađivati,a uz povezivanje na komunikacijsku mrežu ti se podaci mogu i dalje prenositi i obrađivati i u javnoj elektroničkoj komunikacijskoj mreži

**b) Tehnologije nadzora**

- sustav nadzora e-pošte pod nazivom **Carnivore** je razvijen za potrebe FBI-a u SAD-u (mogućnosti zlouporabe izazvale su bojazan i kritike) 🡪 ovim se sustavom automatski pregledavaju i pohranjuju sve e-poruke koje sadrže masovno praćenje,nadzor,presretanje komunikacija,njihovu trajnu pohranu na digitalnim medijima i povezivanje s drugim podacima o nekoj osobi kao i podatke o njihovim pošiljateljima

- sličan sustav **Echelon** je nastao sporazumom VB,SAD-a,Kanade,Australije i Novog Zelanda za vrijeme hladnog rata,sa svrhom prikupljanja i razmjene obavještajnih podataka

- njegovim usavršavanjem je stvoren sustav za masovni nadzor komunikacija diljem svijeta (ako poruke sadrže neku od ključnih riječi,odmah se presreću i pohranjuju radi analize)

- bojazan od ovakvih tehnologija i njihove zloporabe,navode se u izvještaju Europskog parlamenta pod nazivom **An Apprasial of the Technologies of Political Control** kao i u izvještaju Komisije za ljudske slobode Europskog parlamenta **Assessing the Technologies of Political Control** iz 1977.g.

- pravdajući to potrebama nacinalne digurnosti i borbe protiv terorizma SAD tvrde da se tim sustavom koriste samo radi prevencije i sprječavanja tih pojava,što su **Julian Assange** (glavni urednik i osnivač WikiLeaksa) i **Edward Snowden** (bivši zaposlenik CIA-e) opovrgli objavom tajnih dokumenata iz arhiva obavještajnih agencija

- ove tehnologije se mogu iskoristiti,osim za prisluškivanje čelnika država i progona političkih neistomišljenika, i za stvaranje kompleksnih dosijea o najširem krugu građana

*\* pročitati 2 primjera na dnu 113.str.*

- sve više ljudi koristi opremu za priskuškivanje,a neki to pravdaju razlogom sigurnosti i tajnosti poslovanja te sprječavanja tzv.“krađe vremena“,tj.korištenja informacijskom tehnologijom od strane korisnika za vlastite potrebe

- realna opasnost prijeti od toga da se takva komunikacija presretne ili da se preuzme nadzor nad tim uređajima

**c) Tehnologije istrage**

- uključuje stvaranje golemih baza podataka s osobnim podacima građana (u javnom sektoru te baze koje stavraju hakeri,informacijski brokeri i kriminalci )

- stvaraju se nove mogućnosti zloporabe te se otvaraju brojna pitanja🡪 takav je slučaj s uslugom **računarstva u oblaku (cloud computing)** koja ovisno o pojedinom modelu podrazumijeva pohranu osobnih podataka na poslužiteljima koji se nalaze pod kontrolom trećih strana i kojima korisnik koji je ugovorio korištenje tom uslugom pristupa daljinski ne znajući za lokaciju gdje su mu podaci pohranjeni

- 2012. je donesena jedinstvena europska strategija za razvoj računarstva u oblaku

- posebno su opasne moguće zloporabe tzv.**biometrije** kao postupka „prikupljanja, obrađivanja i pohranjivanja podataka o čovjekovim fizičkim karakteristikama za potrebe identifikacije i autorizacije“

- te metode se 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 pri utvrđivanju njihovih prava (takva su npr. razna tehnička i programska rješenja kojima se identificira osoba otiskom prstiju, dlana,potpisom ili načinom pisanja,glasom,snimanjem zjenice oka,..

- najopasniji oblik biometrije je tzv. DNA identifikacija usporedbom temeljenog genetskog materijala s onim koji je o građanima prethodno prikupljen i pohranjen u tzv. **genetičkim bazama podataka** (postoji u SAD-u,VB,Njemačkoj,Kanadi) 🡪 njihovom analizom se može utvrditi sadašnje ili prošlo stanje,sklonosti osobe k obolijevanju te njeno buduće zdravstveno stanje

- velika su očekivanja od tehnologije **trodimenzionalnog ispisa** što korisnicima omogućava da postanu kreatori tjelesnih stvari( pomoću 3D pisača je 2013.g. izrađen pištolj)

**5.1.5. Aktivnosti na pravnoj zaštiti komunikacijske i informacijske privatnosti**

- počinju se donositi zakoni o zaštiti podataka (prvi donesen 1970. u njem.pokrajini Hessen)

- **moguće je razlikovati 2 pristupa zaštiti:**

**1) opći pristup** – podrazumijeva donošenje zakona o zaštiti osobnih podataka koji se temelje na osnovim načelima utvrđenim u Smjernicama OECD-a iz 1980.g. i Europskoj konvenciji Vijeća Europe iz 1981.g.

- karakterističan je za zemlje Europe + Australija,NZ,Hong Kong,Kanada

- takvim zakonom određuju se stroga pravila u pogledu prikupljanja,obrade i prijenosa podataka u javnom i privatnom sektoru, uređuje zaštitu pojedinaca

- o provođenju zakona brine povjerenik ili **ombudsman**

**-** donošenje ovakvog zakona n eisključuje donošenje posebnih zakona ili propisa kojima se pruža zaštita na određenim područjima

**2) područni pristup** – podrazumijeva donošenje posebnih zakona kojima se uređuju razni aspekti privatnosti,tj. područja ili djelatnosti u kojima se pokazuje veća potreba za zaštitom

- karakterističan za SAD,a primijenjuje se i kod nas

- ne postoji 1 opći zakon,nego se donosi poseban zakon ili nadopunjava neki postojeći (npr. u SAD-u su doneseni Privacy Potection Act, The Federal Wiretap Statute,..)

- problem s ovim pristupom je da zaštita najčešće kasni i najčešće ne postoji niti poseban službenik ili ured koji nadgleda provođenje zakona,nego je to prepušteno građanima

- ova 2 pristupa moguće je kombinirati s raznim oblicima **samoregulacije** koja podrazumijeva uspostavljanje pravila ponašanja i standarda od strane tvrtki i raznih udruženja proizvođača,davatelja usluga te udruga kupaca i dr.korisnika usluga čiji podaci se skupljaju

- ovakav oblik regulacije nije polučio rezultate jer nedostaju mehanizmi za sankcioniranje onih koji to zloporabe

- **tehnička samopomoć** se odnosi na uporabu raznih kriptografskih proizvoda,usluga koje korisnicima omogućavaju anonimnost,niza besplatnih programa kojima se štiti privatnost

- razlike postoje na području kaznenopravne zaštite (zemlje kontinentalnog prava su češće pribjegavale sankcijama za razliku od zemalja običajnog prava) 🡪 neki smatraju da treba provesti dekriminalizaciju

**5.2. Opći okvir zaštite osobnih podataka**

- u pravu RH zaštita osobnih podataka uživa status temeljnog ljudskog prava od donošenja Ustava iz 1990.g.

- **čl.37. Ustava propisuje** : „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 njihovog prikupljanja.“

- 2003.g. je donesen **Zakon o zaštiti osobnih podataka** koji uređuje zaštitu osobnih podataka o fizičkim osobama te nador nad prikupljanjem,obradom i korištenjem osobnih podataka

- donesen je sa svrhom zaštite privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju i daljnoj obradi osobnih podataka(*dalje u tekstu OP*)

- zaštita OP-a jamči se svim fizičkim osobama u RH bez obzira na njihovo državljanstvo i prebivalište te neovisno o rasi,boji kože,spolu,jeziku,vjeri,političkomi drugom uvjerenju, nacionalnom ili socijalnom podrijetlu,imovini,rođenju,naobrazbi,društvenom položaju ili dr.

**- Agencija za zaštitu osobnih podataka** je nacionalno tijelo zaduženo za nadzor nad provedbom zaštite OP-a u RH

- sustav zaštite OP-a u RH se razvija u skladu s Direktivom 95/46/EZ o zaštiti pojedinaca u pogledu obrade OP-a i slobodnog kolanja takvih podataka (**Opća Direktiva o zaštiti osobnih podataka**)

- u čl. 1a. se utvrđuje da taj zakon sadrži odredbe koje su u skladu s navedenim aktom

- u zakonu su ugrađena i osnovna načela zaštite podataka iz **Europske konvencije o zaštiti pojedinaca u pogledu automatske obrade osobnih podataka**, koju je RH potpisala 2003.g. te ratificirala 2005.g. zajedno s **Dodatnim protokolom u vezi nadzornih tijela i međunarodne razmjene podataka**

- po stupanju na snagu Lisabonskog ugovora 2009.g. stvoreni su uvijeti za temeljite izmjene u pristupu regulaciji zaštite OP-a na razini prava EU

- **Ugovorom o funckioniranju Europske unije(UFEU)** se svima jamči pravo na zaštitu osobnih podataka(čl.16.st.1.),a riječ je i o samostalnom temeljnom pravu prema članku 8. **Povelje temeljnih prava EU** ( OP se moraju obrađivati pošteno u za to utvrđene svrhe,na temelju pristanka osobe o kojoj je riječ ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom te se svakome 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 neovisnih tijela)

- Direktiva ZOP je donesena sa svrhom postizanja ujednačene razine zaštite prava i sloboda pojedinaca u država članicama EU-a,poglavito prava na privatnost u vezi s obradom njihovih OP-a sukladno članku 8. Konvencije o zaštiti ljudskih prava i teemljnih sloboda te u skladu s temeljnim načelima zaštite OP-a iz Europske konvencije o zaštiti pojedinaca u pogledu automatske obrade osobnih podataka

- cilj Direktive ZOP je i uklanjanje prepreka slobodnom protoku OP,tj.slobodnom razvoju unutarnjeg tržišta

- sustav prijenosa OP između država članica EU-a/EGP-a funkcionira s početnom vrijednosti da sve spomenute zemlje imaju **odgovarajuću razinu zaštite osobnih podataka** (to podrazumijeva neometani prijenos podataka između tih zemalja kao država s uređenom zaštitom OP što je temeljni ekonomski smisao Direktive ZOP-neometani razvoj unut.tržišta)

- to načelo će vrijediti kod izvoza OP u 3.zemlje za koje je Europska komisija utvrdila da imaju dgovarajuću razinu zaštite osobnih podataka(izvoz podataka moguć i u drugim slučajevima)

- države članice EU nisu bile dužne provesti Direktivu ZOP u domaći pravni okvir u područjima vanjske i sigurnosne politike te policijske i pravosudne suradnje u kaznenim stvarima🡪 zaštita OP vezana za to je uređena **Okvirnom odlukom Vijeća 2008/977/PUP o zaštiti osobnih podataka obrađivanih u policijske i pravosudne suradnje u kaznenim predmetima**

- zaštita OP u vezi s njihovom obradom u tijelima i institucijama EU-a posebno je uređena **Uredbom br. 45/2001 Europskog parlamente i Vijeća o zaštiti osoba pri obradi osobnih podataka u institucijama i tijelima Zajednice te o slobodnome protoku takvih podataka**

- posebna pravila zaštite OP i privatnosti u području elektroničkih komunikaicja na razini prava EU sadržana su u **Direktivi 2002/58/EZ o obradi osobnih podataka i zaštiti privatnosti u sektoru elektroničkih komunikacija**

- u sustavu EU zaštite OP ističu se radna skupina za zaštitu pojeidnaca u vezi s obradom OP i europski nadzornik zaštite OP

- **Radna skupina za zaštitu pojedinaca u vezi s obradom osobnih podataka (**skraćeno: **Article 29 Data Protection Working Party, radna skupina članka 29.)** je osnovana člankom 29. Direktive ZOP kao neovisno savjetodavno tijelo za zaštitu podataka i privatnosti,a njeni članovi su predstavnici nadzornih tijela za zaštitu OP država članica EU,europski nadzornik zaštite OP u svojstvu predstavnika institucija i tijela EU te predstavnik Europske komisije

- ovlaštena je ispitati bilo koje pitanje u vezi s primjenom domaćih mjera koje se usvajaju na temelju Direktive ZOP kao bi doprinijela njihovoj usklađenoj primjeni,kao i davati mišljenje Europskoj komisiji o razini zaštite podataka u EU i u trećim zemljama

- može donositi preporuke,na vlastitu inicijativu,os vim pitanjima koja se tiču zaštite pojedinaca u vezi s obradom OP u EU

- iako nisu pravno obvezujući,usvojeni zajednički stavovi radne skupine djeluju snagom svoje pravne uvjerljivosti

- **Europski nadzornik zaštite osobnih podataka (European Data Protection Supervisor)** uspostavljen je Uredbom br. 45/2001 i on je odgovoran za praćenje i osiguravanje primjene Uredbe kao i drugih akata EU koji se odnose na zaštitu temeljnih prava i sloboda fizičkih osoba u vezi s obradom OP od strane institucija ili tijela EU

- on ima važnu savjetodavnu ulogu u sustavu zaštite podataka na razini prava EU –savjetuje institucije i tijela EU u pogledu svih pitanja koja se tiču obrade OP,ima pravo posredovanja pred Sudom pravde EU,savjetuje se s Europskom komisijom pri usvajanju zakonskih prijedloga koji se odnose na zaštitu prava i sloboda u vezi s obradom OP

- poč.2012.g. je Europska komisija podnijela prijedlog **Uredbe o općoj zaštiti osobnih podataka** koja bi zamijenila Direktivu ZOP(danas je u zakonodavnom postupku)

- danas je u zakonodavnom postupku i prijedlog **Direktive o zaštiti pojedinaca pri obradi osobnih podataka od strane nadležnih tijela u svrhe sprječavanja,istrage,otkrivanja ili progona kaznenih djela ili izvršavanja kaznenopravnih sankcija te slobodnom kretanju takvih podataka** (zamijenila bi Okvirnu odluku Vijeća 2008/977/PUP)

**5.2.1. Osnovni pojmovi**

- definirani u čl.2. ZZOP-a

- **osobni podatak** označava svaku infomaciju koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati(ispitanik)

- **osoba koja se može identificirati** je ona 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

- **obrada(osobnih podataka)** je 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

- **zbirka osobnih podataka** se u našem zakonu definira kao svaki strukturirani skup OP koji je dostupan prema posebnim kriterijima,bilo centraliziranim,decentraliz. ili raspršenim na funkcionalnom ili zemljopisnom temelju i bez obzira je li sadržan u računalnim bazama OP ili se vodi primjenom drugih tehničkih pomagala ili ručno

- **voditelj zbirke osobnih podataka**- fizička ili pravna osoba,državno ili drugo tijelo koje utvrđuje svrhu i način obrade OP (kada su svrha i način obrade propisani zakonom,tim se zakonom određuje i voditelj zbirke)

- u OP spadaju npr.podaci o plaćama fizičkih osoba,OP stranih državljana u službenim registrima, evidencije radnog vremena

-podaci koji se genereiraju korištenjem elektroničkim komunikacijskim uslugama mogu se odnositi na identificirane fizičke osobe ili fizičke osobe koje mogu biti identificirane

- Sud pravde EU je odredio da je zadržavanje prometnih podataka i podataka o lokaciji koji se odnose na korisnike elektroničkih komunikacijskih usluga,zajedno s podacima potrebnim za njihovu identifikaciju,obrada OP te je potvrdio da IP adrese koje davatelji usluge pristupa internetu izdaju korisnicima svojih usluga predstavljaju OP u odnosu a te davatelje

- u Direktivi ZOP se radi o OP ako je identifikacija moguća korištenjem bilo kojeg načina kojeg bi voditelj zbirke ili neka druga osoba razumno mogla poduzeti (to primijenjuje radna skupina čl.29.)

- u praksi Suda pravde EU obradu OP označava objava OP na internetskim stranicama,a to predstavljaju i aktivnosti davatelja usluge internetskog pretraživanja u vezi s OP

*Primjer! Google Spain predmet*

*- u tom predmetu tražilo se tumačenje Suda može li se smarati da davatelj usluge internetskog pretraživanja u okviru pružanja te usluge obrađuje OP,kada je riječ o OP izvorno objavljenim na internetskim stranicama trećih te smatra li se davatelj usluge int.pretr. voditeljem zbirke tih OP*

*- Sud je utvrdio da pružanje te usluge obuhvaća pretraživanje OP objavljenih na internetu,njihovo indeksiranje,privremenu pohranu i prikaz,tj. činjenje tih podataka dostupnima trećima prema određenom redoslijedu na stranici s rezultatima pretraživanja*

*- Sud je utvrdio da Google odlučuje o svrhama i načinima obrade OP i da je on voditelj zbirke OP*

- obradu predstavlja i uzimanje otisaka prstiju te spremanje na medij za pohranu podataka te radnje gdje se podaci o prihodima i imovini fizičkih osoba prenose na CD-ROM-u te obrađuju za potrebe SMS usluga

- neki OP su osjetljivije prirode,pa se propisuju posebna pravila za njihovo prikupljanje i obradu 🡪**posebna katergorija osobnih podataka** (tu spadaju OP koji se odnose na rasno ili etničko podrijetlo,politička stajališta,vjerska i druga uvjerenja,sindikalno članstvo,zdravlje ili spolni život te OP o kaznenom i prekršajnom postupku)- posebno označeni i zaštićeni u zakonu **( Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podatak**a)

- obrada OP su kaznenom i prekršajnom postupku se dopušta pod kontrolom nadležnih tijela

- voditelji zbirki OP imaju niz obveza prpisanih u ZZOP-u te su dužni uspostaviti i voditi evidencije s temeljnim i potpunim informacijama o relevantnim zbirkama OP ( obveze propisane u **Uredbi o načinu vođenja i obrascu evidencije o zbirkama osobnih podatka**) 🡪 evidencije su javno dostupne i objedinjavaju se u Središnjem registru Agencije uz pojedine posebno propisane iznimke u zakonu(čl.14.-16a.)

- obvezi objedinjavanja evidencija u online registru Agencije **ne podliježu** one evidencije koje vode nadležna državna tijela u okviru aktivnosti obrade OP radi državne sigurnosti,obrane i suzbijanja pojava koje su određene kao sigurnosni rizik te se ne moraju dostaviti one evidencije koje se vode premea radnopravnim propisima ako se OP u pitanju ne iznose iz RH, no to samo u slučaju kada voditelj zbirke u pitanju ima najviše 5 zaposlenih te onda kada je voditelj imenovao službenika za zaštitu OP i o tome obavijetsio AZOP

- **izvršitelj obrade osobnih podataka** je fizička ili pravna osoba,državno ili drugo tijelo koje obrađuje OP u ime voditelja zbirke OP(prema ZZOP-u voditelj zbirke može povjeriti neke ili sve poslove izvršitelju obrade koji je registriran za obavljanje takve djelatnosti i koji osigurava dovoljno jamstva u pogledu ostvarivanja odgovarajućih mjera zaštite OP,tj. klasificiranih podataka ako ispunjava uvjete utvrđene posebnim propisima koji uređuju područje informacijske sigurnosti)

- voditelj zbirke mora sklopiti pisani **ugovor o** **povjerenju poslova obrade podataka** s izvršiteljem obrade(uređuje njihova međusobna prava i obveze) – dužan je ugovorno obvezati izvršitelja obrade da obavlja poslove obrade podataka samo po njegovom nalogu,da ne daje OP na korištenje primateljima,da ih ne obrađuje za bilo koju drugu svrhu osim ugovorene te da ne provodi odgovarajuće tehničke,organizacijske i kadrovske mjere zaštite

- **primatelj podataka je** svaka fizička ili pravna osoba,državno ili drugo tijelo kojem se OP otkrivaju,neovisno o tome je li on ujedno treća strana ili ne (državna tijela koja mogu primati podatke u okviru provođenja istrage ne smatraju se primateljima)

- u našem zakonu pojam primatelja podataka se veže uz radnju davanja podataka na korištenje 🡪 primatelj koji dobiva pristup podacima,bilo na zakonit ili nezakonit način, u pravilu postaje novi voditelj zbirke tih podataka i time preuzima odgovornost

- naš zakon propisuje određene posebne uvjete za slučaj davanja OP na korištenje u čl.11. kao što su pisani zahtjev primatelja sa svrhom i pravnim na temelju za korištenje OP te vrstom podataka koje traži te utvrđena potreba za podacima radi obavljanja poslova u okviru primateljeve zakonom određene djelatnosti

- pojam **treće osobe** (unesen ZZOP-om 2011.g.) je fizička ili pravna osoba,državno ili drugo tijelo,osim ispitanika,voditelja zbirke ili izvršitelja obrade i osoba koje voditelj zbirke ili izvršitelj obrade ovlasti na obradu OP (može uključivati i primatelja)

- **čl.9.** : obveza obavještavanja ispitanika o primateljima ili kategorijama primatelja prije prikupljanja OP ; ti se podaci moraju navoditi i u evidenciji o zbirkama OP **(čl.14.)** te središnjem registru Agencije za zaštitu OP (**čl.17.**)

- voditelj zbirke je dužan pružiti informacije o primateljima i danim podacima na zahtjev ispitanika u kontekstu prava na pristup njegovim OP (**čl.19.**),a dužan je i obavijestiti primatelje i u slučaju dopune,izmjene ili brisanja OP u pitanju (**čl.20.**)

- u krug primatelja može spadati i izvršitelj obrade

- prema Direktivi ZOP voditelj zbirke može imenovati **službenika za zaštitu osobnih podataka** koji vodi brigu o zakonitosti obrade OP i ostvarivanju prava na zaštitu OP i ta je mogućnost uvedena u ZZOP-u izmjenama i dopunama 2008.g.

- u okviru izmjena 2011.g. imenovanje navedenih službenika je postalo obvezno ako voditelj zbirke zapošljava više od 20 radnika te su dodane detaljnije odredbe o imenovanju službenika i njegovim zadacima **(čl.18a.)**

**5.2.2. Područje primjene**

- pravni okvir zaštite OP u RH se primijenjuje na automatiziane i ručno vođene zbirke OP te se uz iznimku obrade OP koju fizičke osobe obavljaju isključivo za osobnu primjenu ili za potrebe kućanstva,primjenjuje na sve aktivnosti u javnom i privatnom sektoru(tu ne spada objava OP na internetu,tj.omogućavanje njihove dostupnosti neodređenom broju osoba)

- takva obrada OP spada pod materijalno područje Direktive ZOP

- ta odredba se treba tumačiti u smislu da korištenje sustavom nadzornih kamera,zobg kojeg je snimljeni videozapis pohranjen na uređaj za kontinuirano snimanje ka što je tvrdi disk,a koji je fizička osoba ugradila u svoju obiteljsku kuću radi zaštite imovine,zdravlja i života vlasnika kuće te se taj sustav nadzire i javni prostor,ne predstavlja obradu podataka koja se provodi za obavljanje isključivo osobnih ili domaćih aktivnosti

- **teritorijalno područje primjene propisa** o općoj zaštiti OP-mjerodavno će biti pravo države članice EU gdje voditelj zbirke OP ima poslovni nastan ako se obrada OP provodi u kontekstu aktivnosti tog poslovnog nastana

- ako voditelj zbirke ima poslovni nastan u više teritorija država članica,on mora poduzeti potrebne mjere kako bi osigurao usklađenost svakog od tih poslovnih nastana s obvezama propisanima mjerodavnim domaćim pravom

- pravo države članice EU bit će mjerodavno i onda kada voditelj zbirke nema poslovni nastan na njezinu području ako se njeno domaće pravo primijenjuje na temelju međun.javnog prava

- ako voditelj zbirke nam poslovni nastan u EU,ali se oprema kojom se koristi u svrhe obrade OP nalazi na području 1 od država članica EU,tada će biti mjerodavno pravo te države članice (osim ako se tom opremom iskljuičivo koristi za svrhe prijenosa podataka preko teritorija EU (u tom slučaju voditelj zbirke mora imenovati zastupnika s poslovnim nastanom na području te države članice ne dovodeći u pitanje pravne radnje koje se mogu poduzimati protiv samog voditelja zbirke)

- oprema kojom se voditelj zbirke koristi u svrhu obrade OP je terminalna oprema ispitanika

- u naš ZZOP **(čl.3.)** je unesena odredba koja utvrđuje primjenu tog zakona i kad voditelj zbirke nema prebivalište ili sjedište u nekoj od država članica EU,ali se koristi automatiziranom i drugom opremom koja se nalazi na području RH za potrebe obrade OP,ali je u tom slučaju voditelj zbirke dužan imenovati zastupnika u RH

**5.2.3. Nadzorna tijela za zaštitu osobnih podataka - Agencija za zaštitu osobnih podataka**

- sve države članice EU su prema Direktivi ZOP dužne uspostaviti tijela koja obavljaju nadzor nad pravilnom primjenom propisa o zaštiti OP s **potpunom neovisnošću**

- osnivanje nadležnih tijela propisuje i Europska konvencija o zaštiti pojedinaca u pogledu automatske obrade OP,a u okviru prava EU se uvjet neovisnosti nadzornih tijela posebno utvrđuje i Ugovorom o funkcioniranju EU te Poveljom o temeljnim pravima EU

- o tom uvjetu je odlučivao i Sud pravde EU koji je donio presudu protiv SR Njemačke,Austrije i Mađarske u kojima je utvrdio povredu nezavisnosti nadzornih tijela

- Agencija za zaštitu OP je zadužena za nadzor nad provedbom zaštite OP u RH

- ZZOP predviđa njezinu samostalnost u obavljanju poslova utvrđenih zakonom i odgovornost prema Hrvatskome saboru kojem podnosi izvješća o radu

- sredstva za rad AZOP-a osiguravaju se u državnom proračunu

- ravnatelja i zamjenika ravnatelja AZOP-a imenuje i razrješava Hrvatski sabor na prijedlog Vlade RH,a uvijeti za njihov izbor odnose se na to da oni moraju biti hrvatski državljani visoke stručne spreme te imati najmanje 10 godina radnog iskustva

- **AZOP obavlja poslove nadzora:**

**a)** po službenoj dužnosti

**b)** na zahtjev ispitanika

**c)** na prijedlog treće osobe

- voditelj zbirke je dužan Agenciji dati pristup svim podacima i dokumentaciji

- AZOP ima pravo pristupa OP koji se nalaze u zbirkama OP,spisima i dokumentaciji te sredstvima e-obrade te ima pravo prikupljati sve podatke potrebne za provedbu nadzora

- ako su podaci stupnjevani po tajnosti,AZOP im može pristupiti samo ako su ispunjeni uvjeti prema posebnim propisima koji uređuju zaštitu tajnosti podataka (to se odnosi na potrebu posjedovanja certifikata,tj. **Uvjerenja o obavljenoj sigurnosnoj provjeri za pristup klasificiranim podacima**)

- AZOP ukazuje i na određene zloporabe prikupljanja OP,nadzire iznošenje OP iz RH,prati uređenje zaštite OP u drugim zemljama i surađuje s tijelima nadležnim za nadzor nad zaštitom OP u drugim zemljama,sastavlja listu država i međun.organizacija koje imaju odgovarajuće uređenu zaštitu OP,rješava u povodu zahtjeva za utvrđivanje povrede prava i vodi Središnji registar,izrađuje metodološke preporuke za unapređenje zaštite OP i dostavlja ih voditeljima zbirke,prati primjenu organizacijskih i tehničkih mjera za zaštitu OP te predlaže njihovo poboljšanje,pruža savjete oko uspostave novih zbirki OP,daje prijedloge i preporuke za unapređenje zaštite OP te surađuje s nadležnim državnim tijelima u izradi prijedloga propisa koji se odnose na zaštitu OP

- ako uoči nezakonitosti,AZOP izdaje upozorenja ,opomene,rješenja,zabrane

- rješenjem može zabraniti nezakonito iznošenje OP iz RH ili njihovo nezakonito davanje na korištenje primateljima

- žalbe protiv rješenja AZOP-a nisu dopuštene,ali se može pokrenuti upravni spor

- Agencija je ovlaštena podnositi prijedloge za pokretanje postupaka za utvrđivanje kaznene i prekršajne odgovornosti pred nadležnim tijelima

**5.2.4. Načela obrade osobnih podataka**

- u našem zakonu utvrđuje se obveza voditelja zbirke OP na obradu OP samo uz uvjete određene tim zakonom,ali i posebnim zakonima(čl.5.)

- daljnja su načela obrade sadržana u čl.6. ZZOP-a,a odgovornost za njihovo poštivanje snosi voditelj zbirke(tako se OP mogu obrađivati pošteno i zakonito)

- oni se mogu prikupljati samo u svrhu s kojom je ispitanik upoznat,koja je izričito navedena i koja je u skladu sa zakonom te se smiju dalje obrađivati samo u svrhu u koju su prikupljeni,tj. u svrhu koja je podudarna sa svrhom prikupljanja 🡪 **načelo određenosti svrhe obrade** (purpose specification principle) **i načelo ograničenja svrhe obrade** (purpose limitation principle)

- dopuštena je daljnja obrada podataka u povijesne,statističke ili znanstvene svrhe pod uvjetom da su poduzete odgovarajuće zaštitne mjere

- tehničkim mjerama zaštite treba se osigurati da osobnim podacima nije moguće koristiti se tako da se na temelju njih može donijeti odluka ili mjera koja se odnosi na konkretnu osobu

- OP se ne smiju čuvati duže no što je potrebno za svrhu u koju su prikupljeni ili se dalje obrađuju

- osnovno načelo u vezi s kvalitetom OP nalaže da OP koji se prikupljaju moraju biti bitni za postizanje utvrđene svrhe,te da se oni ne smiju prikupljati u većem opsegu nego što je to nužno da bi se postigla utvrđena svrha 🡪**načelo razmjernosti/proporcionalnosti** (proportionality principle) i **načelo minimalizacije podataka** (data minimization principle)

- OP moraju biti točni,potpuni i ažurni

**5.2.5. Propisane osnove za dopuštenu obradu osobnih podataka**

- ZZOP propisuje osnove kada je dopušteno obrađivati OP,kao npr. na temelju privole ispitanika,u svrhu ispunjenja zakonske obveze voditelja zbirke OP ,kada je to propisano zakonom i dr. (čl.7.)

- u slučaju obrade podatka na osnovi dane privole,OP se mogu obrađivati samo u svrhu za koju je ispitanik dao privolu (može bilo kada povući danu privolu i zatražiti prestanak obrade)

- u ZZOP-u se privola mora dati izričito pri obradi „običnih“ OP i dopuštena je osnova za obradu OP i u slučaju kada ispitanik sam objavi svoje OP javnosti (odredba posebno dodana 2003.g.,a nije navedeno u Direktivi ZOP)

- jedina slična osnova u Direktivi predviđa se isključivo za obradu posebnih kategorija OP,ali u tom slučaju se treba raditi o **očitoj objavi**

- po ZZOP-u, OP se mogu obrađivati i onda ako je obrada potrebna u svrhu sklapanja te izvršenja ugovora u kojem je ispitanik stranka,ili u svrhu zaštite života ispitanika ili druge osobe ako ispitanik fizički i pravno nije u mogućnosti dati pristanak

- obrada će prema ZZOP-u biti dopuštena i u svrhu ispunjena zakonske obveze voditelja zbirke kao i onda kad je propisano zakonom,ali i kad je obrada OP nužna u svrhu ispunjenja zadataka koji se izvršavaju u javnom interesu

- obrada je i dopuštena ako je ona nužna u svrhu zakonitog interesa voditelja zbirke OP ili treće strane kojoj se podaci otkrivaju,osim kada prevladavaju interesi zaštite relevantnih temeljnih prava i sloboda ispitanika

- ispitanik ima pravo usprotiviti se obradi iz zakonitih razloga kada se ona temelji na osnovi zakonitog interesa kao i na osnovi prema kojoj bi obrada bila nužna radi ispunjenja zadataka koji se izvršavaju u javnom interesu

- ispitanik ima pravo da se usprotic+vi obradi OP u slučaju kada se ti podaci namjeravaju obrađivati u **svrhe marketinga** (voditelj zbirke mora unaprijed obavijestiti ispitanika o namjeravanoj obradi u svrhu marketinga)

- **aktivnost izravnog marketinga** podrazumijeva komuniciranje određenim osobama bilo kojeg oglašivačkog ili marketinškog materijala bilo kojim sredstvima (ne mora biti u komercijalne svrhe)

- što se tiče obrade OP koji se odnose na maloljetnike,ti podaci se smiju prikupljati i dalje obrađivati u skladu s tim zakonom i uz posebne mjere žaštite propisane posebnim zakonima **(čl.7.st.3.)** – potrebna privola zakonskih zastupnika

**5.2.6. Mjere zaštite osobnih podataka**

- **u čl.18. ZZOP-a** utvrđuje se obveza zaštite OP u zbirkama od svake zlopoabe,uništenja, gubitka,neovlaštenih promjena ili dostupa

- ta se obveza utvrđuje za voditelja zbirke i za primatelja,a i radit će se i o obvezi izvršitelja obrade (te osobe su dužne poduzimati tehničke,kadrovske i organizacijske mjere zaštite)

- prema rješenju u ZZOP-u mjere zaštite moraju biti razmjerne naravi djelatnosti voditelja zbirke OP,odnosno primatelja,i sadržaju zbirke OP

- **Uredba o načinu pohranjivanja i posebnim mjerama tehničke zaštite posebnih kategorija osobnih podataka**

- mjerama zaštite mora se osigurati odgovarajuća sigurnost u odnosu na rizike,uzimajući u obzir najnovija dostignuća (state of the art) i troškove provedbe mjera

- te mjere moraju se primijenjivati tijekom obrade OP i u vrijeme dizajniranja sustava za njihovu obradu

- sustavi za obradu trebaju biti oblikovani tako da služe čovjeku i da se njima poštuju njihova temeljna prava i slobode,osobito pravo na privatnost

- **napredna tehnologija za zaštitu privatnosti (PET's – privacy enhancing technologies)** – skup inf.-komunik. mjera kojima se štiti pravo privatnosti tako da se izbjegavaju ili minimaliziraju OP (tako se sprječava nepotrebna i/ili neželjena obrada OP)

- korištenjem tim mjerama bi se moglo pridonijeti tome da se inf.-komunik. sustavi i usluge oblikuju na način kojim se minimalizira prikupljanje i korištenje OP te omogućava postizanje usklađenosti s propisima o zaštiti OP,a može se postići i kontrola ispitanika nad obradom OP

- cilj korištenja naprednih tehnologija je onemogućavanje povreda pravila zaštite OP

- **privatnost po dizajnu (privacy by design)** označava filozofiju i pristup ugrađivanja zaštite prava na privatnost u vezi s obradom OP u specifikacije dizajna raznih tehnologija kojom se osigurava inter alia toga da se u samoj fazi planiranja i oblikovanja sustava za obradu OP ugrade u sustav sve potrebne mjere i kontrole za učinkovitu provedbu temeljnih načela zaštite OP

**5.2.7. Izvoz osobnih podatka**

- sustav prijenosa OP između država članica EU funcionira na pretpostavci da sve spomenute zemlje imaju odgovarajuću razinu zaštite OP

- ako voditelj zbirke sumnja ima li zemlja,u koju želi iznijeti podatke,odgovarajuću razinu zaštite OP,on je o tome dužan zatražiti mišljenje AZOP-a

- za SAD Europska komisija nije utvrdila odgovarajuću razinu zaštite,ali je odlukom odobrila program **„sigurne luke“ (Safe Harbour)** prema kojem se izvoz OP u SAD dopušta ako se primatelj podataka obvezao na primjenu Safe Harbour načela privatnosti

- program se zasniva na dobrovoljnoj i samostalnoj certifikaciji kompanija (uočeni su nedostatci tog programa)

- krajem 2013.g. Europska komisija je izdala niz preporuka radi učinkovite provedbe programa koje ako ne budu usvojene,mogu dovesti i do izmjene ili poništenja njene odluke o Safe Harbouru

- tijekom 2014.g. Europski parlament je zatražio hitnu suspenziju programa Safe Harbour i pozvao nadzorna tijela država članica EU za zaštitu OP da u skladu sa svojim ovlastima trenutačno suspendiraju prijenos OP organizacijama koje su se samostalno certificirale po tom programu,ali i da se revidiraju,osiguravanjem zaštitnih mjera i jamstava radi zaštite temeljnih prava građana EU,drugi instrumenti za prijenos OP

- **program PRISM** – program Agencije za nacionalnu sigurnost SAD-a koji omogućuje masovni nadzor građana EU putem izravnog pristupa središnjim poslužiteljima glavnih internetskih trgovačkih društava u SAD-u

- ZZOP uređuje da se OP mogu izvoziti ako država ili međunarodna organizacija u koju se podaci uvoze ima odgovarajuću razinu zaštite OP

- ako Komisija utvrdi da treća zemlja ne osigurava adekvatnu razinu zaštite OP, AZOP će zabraniti iznošenje OP iz RH u tu zemlju

- to ne znači da voditelju zbirke nikad neće biti dopušteno izvoziti OP u treće zemlje,za koje nije utvrđena određena razina zaštite

- u tim slučajevima će voditelji zbirke morati ispuniti posebne uvjete kojima se nadoknađuje nedostatak odgovarajuće razine zaštite u zemljama ili međunarodnim organizacijama gdje namjeravaju iznijeti OP

- prema ZZOP-u će u takvim slučajevima biti dopušteno iznijeti OP ako je ispunjen 1 od posebno propisanih uvijeta,kako slijedi:

**a)** ako je ispitanik dao privolu za iznošenje podataka koji se na njega odnose samo u svrhu za koju je ispitanik dao privolu

**b)** ako je iznošenje nužno u svrhu zaštite života ili tjelesnog integriteta ispitanika

**c)** ako voditelj zbirki pruži dovoljna jamstva glede zaštite privatnosti i temeljnih prava i sloboda pojedinaca koja mogu proizlaziti iz ugovornih odredaba za koja AZOP utvrdi da su odgovarajuća u skladu s važećim propisima kojima se uređuje zaštita OP

**d)** ako je iznošenje podataka potrebno radi izvršenja ugovora između voditelja zbirke i ispitanika ili provedbe preugovornih mjera poduzetih na zahtjev ispitanika

**e)** ako je iznošenje podataka potrebno za zaključivanje ili izvršenje ugovora između voditelja zbirke i treće osobe,a koji je u interesu ispitanika

**f)** ako je iznošenje podataka potrebno ili određeno zakonom radi zaštite javnog interesa ili radi uspostave,ostvarenja ili zaštite pretraživanja propisanih zakonom

**g)** ako se iznošenje podataka obavlja iz evidencije koja je sukladno zakonu ili drugom propisu namijenjena pružanju informacija javnosti i koja je javnosti ili svakoj osobi koja može dokazati pravni interes otvorena za uvid,u kojem se slučaju podaci mogu iznositi u onoj mjeri u kojoj su ispunjeni zakonom propisani uvjeti za uvid u pojedinom slučaju

- Europska komisja je utvrdila predloške **standardnih ugovornih klauzula** za korištenje u kontekstu ugovora koje u vezi s prijenosom OP sklapaju voditelji zbirki u EU s primateljima podataka u trećim zemljama za koje nije utvrđena odgovarajuća razina zaštite OP

- tu se radi o ugovornim klauzulama za koje je Komisija utvrdila da osiguravaju dovoljna jamstva zaštite privatnosti i temeljnih prava i sloboda pojedinaca,što znači da će u slučaju njihova korištenja prijenos OP biti dopušten

- zadnjih godina je izražen trend usvajanja **obvezujućih korporativnih pravila (BCR's – binding corporate rules)** na razini čitave grupe kompanija

- tim se pravilima želi ostvariti propisana pravna osnova za kontinuirane prijenose OP između članica grupe

- u svojoj praksi je Sud pravde EU utvrdio da nema prijenosa OP u treću zemlju u smislu Direktivve ZOP kada osoba u državi članci objavi osobne podatke na stranici koja se pohranjuje kod davatelja usluge pohrane informaicja osnovanog u toj državi ili drugoj državi članici zbog čega su ti podaci dostupni svima na internetu

**5.2.8. Pravo prisupa podacima i povezana prava ispitanika**

- **omogućavanje kontrole ispitanika** uključuje provjeru vode li se u zbirkama podataka OP ispitanika,jesu li oni točni i obrađuju li se u skladu s propisima,kao i provjeru kome se oni dostavljaju,tj.dostavljaju li se ovlaštenim osobama

- javno dostupan Središnji registar AZOP-a ,u koji su voditelji zbirki dužni prijavti evidencije o zbirkama OP koje vode, služi svrsi osiguravanja transparentnosti obrade OP prema ispitanicima

- ispitanici imaju pravo izravnog obraćanja voditeljima zbirki radi dobivanja uvida u njihove OP koje voditelji zbirki obrađuju,a da bi zatražili ispravljanje netočnih podataka ili njihovo brisanje,npr.ako voditelji obrađuju te podatke nepropisno **(čl.19.-20.)**

- troškove navedenog snosi voditelj zbirke,ako posebnim zakonom nije drugačije uređeno **(čl.22.)**,a tu ne bi ulazili uobičajeni troškovi za ispitanika u vezi s odašiljanjem njegova zahtjeva (npr.trošak uspostave poziva ili slanja pisanog zahtjeva poštom)

**-** Sud pravde EU je odredio da navedena odredba od država članica ne zahtijeva niti im zabranjuje naplatu troškova pri korištenju prava na pristup OP ako iznos troškova nije pretjeran(njihov iznos ne smije prelaziti trošak obavijesti o tim podacima)

**a) Pravo pristupa podacima (čl.19.)**

- ispitanik(ili njegov zakonski zastupnik ili opunomoćenik) ima pravo podnositi zahtjev voditelju zbirke u pogledu toga obrađuje li,i ako da,koje njegove OP

- ima pravo i zatražiti informaciju o izvoru tih podataka,a to podrazumijeva da voditelj zbirke mora paziti da bodi točnu i potpunu evidenciju o tome odakle je OP ispitanika dobio

- ispitanik ima pravo na zahtjev dobiti i uvid u evidenciju zbirke koja sadrži njegove OP kao i zatražiti njihovo prepisivanje

- voditelj zbirke je dužan na zahtjev ispitaniku dostaviti izvatke,potvrde ili ispise njegovih osobnih podataka koji se nalaze u relevantnoj zbirci,s time da sva ta dokumentaicja mora sadržavati naznaku svrhe i pravnog temelja prikupljanja,obrade i korištenja OP ispitanika

- na zahtjev ispitanika se mora dostaviti i ispis informacija o tome tko je i za koje svrhe te po kojem pravnom temelju dobio na korištenje OP ispitanika

- **čl.11.st.5.** kaže da je voditelj zbirke dužan voditi posebnu evidenciju o OP koji su dani na korištenje primatelju,primatelji i svrsi za koju su OP dani

- ispitaniku se na zahtjev mora pružiti i obavijest o logici bilo koje automatske obrade podataka koja se na njega odnose **(čl.22a.)**

- svim vrstama zahtjeva je voditelj zbirke dužan udovoljiti u roku od najviše 30 dana od dana podnošenja zahtjeva

- obveza udovoljenja navedenim zahtjevima ispitanika se može ograničiti posebnim zakonima ako je to potrebno radi zaštite države,obrane,javne sigurnosti,istrage,.. (tu spadaju aktivnosti privatnih detektiva koji djeluju za stručna tijela)

- obveza udovoljavanja zahtjeivma se može ograničiti i ako se OP obrađuju isključivo u svrhu znanstvenog istraživanja ili ako su prikupljeni isključivo u svrhu utvrđivanja statistike i pohranjeni na duže razdoblje isključivo za statističku uporabu **(čl.23.)**

**b) Povezana prava ispitanika (čl.20.-21.)**

- ispitanik može zahtijevati i korekciju svojih OP,tj.zatražiti njihov ispravak ili nadopunu ako je riječ o netočnim ili nepotpunim podacima,kao i njihovo brisanje u određenim slučajevima (zadatak voditelja registra da to učini)

- u našem se zakonu utvrđuje obveza voditelja zbirke da samostalno poduzme određene korake s podacima i to čim utvrdi da su nužni(nepotpuni,netočni ili neažurni)

- pravo na brisanje OP je zadnjih godina aktualna tema što dovodi do razmatranja njegova osnaženja kao tzv. **prava biti zaboravljen** (važna presuda Suda pravde EU u Google Spain predmetu u kojoj je protumačeno inter alia pitanje postojanja te opsega i uvjeta prava ispitanika da zatraži i ishodi brisanje svoji OP iz indeksa,tj.rezultata inter.pretraživanja)

*\* pročitati slučaj Google Spain na 138.str.*

- postavi li ispitanik zahtjev za brisanje njegovih OP,a utvrdi se da u ovom trenutku uključivanje poveznica prema internetskim stranicama s istinitim informacijama o njemu nije u skladu s Direktivom jer se pokazuje da su te informacije nerelevantne ili nisu više relevantne,tj.da su suvišne u odnosu na svrhu obrade koju provodi davatelj usluge internetskog pretraživanja te se informaicje i poveznice trebaju izbrisati iz popisa rezultata pretraživanja

**5.2.9. Zaštita prava ispitanika (sankcije,pravni lijekovi)**

- u Europskoj konvenciji o zaštiti pojedinca u pogledu automatske obrade OP se utvrđuje oveza država ugovornica da osiguraju u svojem unutarnjem pravu uvođenje odgovarajućih sankcija i pravnih lijekova koji bi bili dostupni ispitaniku u vezi s povredama odredbi unutarnjeg prava u kojima su implementirana temeljna načela zaštite OP iz Konvencije (države same određuju sankcije i pravne lijekove)

- u Dodatnom protokolu uz Konvenciju se utvrđuju se i povezana prava ispitanika

- u Direktivi ZOP se utvrđuje obveza država članica EU da osim upravnog lijeka pred nadležnim nadzornim tijelom za zaštitu OP,u domaćim propisima osiguraju i pravo svake osobe ma pravni lijek u slučaju nezakonite obrade njegovih OP ili u slučaju bilo koje povrede njenih relevantnih prava

- u unutarnjem pravu mora se osigurati pravo ispitanika na postavljanje zahtjeva za naknadu štete od voditelja zbirke u slučaju nezakonite obrade njegovih OP ili u slučaju bilo kakve radnje koja nije u skladu s odredbama domaćih propisa donesenih na temelju Direktive

- države članice su dužne osigurati prikladne mjere radi osiguravanja potpune provedbe Direktive te propisati sankcije za povredu domaćih propisa donesenih na temelju Direktive

**a) Prekršaji i domaće kazne**

- u RH nema predviđene ovlasti AZOP-a da izravno izriče sankcije,npr.u obliku prekršajnog naloga,u slučaju utvrđenih povreda propisa o zaštiti OP

- čl.36. ZZOP-a utvrđuje prekršajnu odgovornost za povrede tog zakona i novčane kazne, a ta se odgovornost izričito utvrđuje za slučajeve povreda samo pojedinig odredbi ZZOP-a

- kriteriji koji su uzimani u obzir pri donošenju zakona nisu(isključivo) kriteriji težine i ozbiljnosti povrede zakona(npr. prekršajna odgovornost se izričito ne utvrđuje za slučajeve povreda temeljnih načela zaštite OP (npr.povrede čl.6.-7.) kao ni za slučajeve nezakonite obrade posebne kategorije OP (povrede čl.8.))

- prekršajna odgovornost može posredno nastupiti i kod povreda zakona koje nisu izričito predviđene kao prekršaji

- u ZZOP-u se utvršuje prekršajna odgovor. voditelja zbirke,primatelja ili izvršitelja obrade koji nije postupio po naredbi ili zabrani,tj.izdanom rješenju AZOP-a u zadanome roku,s time da rješenje AZOP-a može donijeti u vezi s uočenim povredama odredbi ZZOP-a

**b) Zahtjev za utvrđivanje povrede prava**

- ZZOP predviđa pravo svake osobe da podnese AZOP-u **zahtjev za utvrđivanje povrede prava** ako smatra da je povrijeđeno neko njeno pravo zajamčeno ovim zakonom

- AZOP o povredi prava te osobe odlučuje rješenjem koji je po pravnoj prirodi upravni akt protiv kojeg nije dopuštena žalba,ali se može pokrenuti upravni spor

- ako ispitanik zatraži u svojem zahtjevu i Agencija smatra da je takav zahtjev opravdan,ona će rješenjem privremeno zabraniti obradu spornih OP sve do pravomoćnog okončanja postupka(protiv to rješenja nije dopuštena žalba,ali se može pokrenuti upravni spor)

**c) Zahtjev za naknadu štete**

- ZZOP predviđa pravo ispitanika da pred sudom opće nadležnosti zatraži od voditelja zbirke naknadu štete koja je nastala uslijed obrade njegovih OP protivno odredbama tog zakona

- ispitanik ima pravo tražiti naknadu štete od voditelja zbirke OP i u slučaju neovlaštenog korištenja njegovim OP, tj.neovlaštenog davanja na korištenje njegovih OP drugim primateljima ili fizičkim i pravnim osobama

**d) Kazneno djelo nedozvoljene uporabe osobnih podataka**

- čl.146. – **kazneno djelo nedozvoljene uporabe osobnih podataka** (pripada djelima protiv privatnosti u KZ RH, a tim djelima pripadaju i 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.))

- kazneno djelo nedozvoljene uporabe OP čini bilo tko tko protivno uvijetima određenima u zakonu prikuplja,obrađuje ili se koristi OP fizičkih osoba ( to kazneno djelo se pokreće po službenoj dužnosti te se kao sankcija predviđa isključivo kazna zatvora koja u osnovnom obliku ovog djela može biti izrečena u najduljem trajanju o 1 godine zatvora)

- kao klasificirani oblici tog djela obrada OP protivno zakonu čime je pribavljena znatna imovinska korist ili prouzročena znatna šteta(koja prelazi 60 000 kn),izvoz OP 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 3 godine

- kvalificirani oblik se predviđa i u slučaju prikupljanja,obrade odnosno korištenja OP djeteta kao i posebne kategorije OP protivno zakonu,a kao daljnji kvantificirani ovlik djela propisuje počinjeneje tih djela od starne službene osobe u obavljanju službe ili odgovorne osobe u obavljanju javne ovlasti(kazna zatvora od najmanje 6 mjeseci do najviše 5 godina)

**5.2.10. Samoregulacija-kodeksi postupanja**

- Europska komisija i države članice promiču izradu tzv. **kodeksa postupanja**

- kodeksi postupanja mogu biti namijenjeni za primjenu u pojedinim sektorima gdje se posebnije izražavaju pojedina pitanja zaštite OP

- pomoću kodeksa se mogu i urediti pitanja u vezi s primjenom pojedinih odredbi direktive na općenitoj razini

- u osnovi je cilj izbjegavanje suvišne regulacije u području zaštite podataka na razini država članica

-u Direktivi se određuje kako bi države članice trebale predvidjeti mogućnost da udruženja trgovaca imaju pravo dostaviti nadležnom nadzornom tijelu za zaštitu podataka na mišljenje nacrte nacionalnih kodeksa koje su izradili

- trebala bi se predvidjeti i ovlast da se utvrdi jesu li takvi nacrti kodeksa u skladu s domaćim propisima

- osim nacionalnih kodeksa,u Direktivi se predviđaju i **europski kodeksi**,tj.kodeksi s područjem primjene unutar EU,a nacrti takvih kodeksa trebaju se dostaviti radnoj skupini članka 29.

- rješenja o samoregulaciji se trenutno predviđaju u ZZOP-u

**5.2.11. Automatske pojedinačne odluke i profiliranje**

- Direktiva ZOP utvrđuje određene obveze voditelja zbirki za slučaj kada oni u pogledu ispitanika donose ili žele doniejti tzv.**automatske pojedinačne odluke**, a to je potaknuto potrebom osiguravanja zaštite ispitanika od odluka koje na njega utječu i koje voditelj zbirke o njemu donosi isključivo upotrebom strojeva,odnosno automatskih sredstava obrade,a da se ispitaniku u isto vrijeme ne omogući pravo utjecaja na ishod takve odluke

- u čl.5. Direktive se utvrđuje obveza država članica da predvide u unutarnjem rpavu pravo ispitanika da ne bude podvrgnut automatskim pojedinačnim oslukama koje se definiraju kao odluke koje proizvode pravne učinke u pogledu ispitanika ili na njega imaju znatan utjecaj i koje se temelje isključivo na automatskoj obradi podataka sa svrhom ocjenjivanja određenih osobnih aspekata u vezi s njegovom osobom

- neka pojašnjenja su dostupna iz teksta prijedloga za donošenje ove direktive u kojem se pojašnjava da se neće raditi o automatskim pojedinačnim odlukama ako postoji čimbenik koji će biti uključen u donošenje odluke (npr. autom.pojed.odluka bi bila zapošljavanje kandidata isključivo na temelju kompjutorizirane psihološke ocjene)

- autom.pojed. odluke se donose u kontekstu utvrđivanja profila osobnosti ispitanika

- u ZZOP-u je pitanje autom.pojed.odluka regulirano od 2011.g.

- prema čl.22a.,donošenje odluke koja proizvodi pravni učinak na ispitanika ili bitno na njega utječe,a temelji se isključivo na automatskoj obradi OP koja je namijenjena procjeni određenih osobnih aspekata ispitanika,dopuštena je samo ako je donošenje takve odluke predviđeno zakonom,tj.ako je odluka donesena u svezi sa zaključivanjem ili izvršenjem ugovora u kojem je ispitanik stranka

- pitanje autom.pojed.odluka se aktualizira posebno u kontekstu postupaka profiliranja pojedinaca,njihove osobnosti i ponašanja

- pri ispitivanju uređenja postupaka profiliranja iz aspekta zaštite OP važne su **Preporuke Odbora ministara Vijeća Europe br.(2010) 13 o zaštiti pojedinaca u vezi s automatskom obradom osobnih podataka u kontekstu profiliranja**

- u njima se **profil** definira kao skup podataka putem kojih se karakterizira kategorija pojedinaca s namjenom primjene na pojedinca

- **profiliranje** označava tehniku automatske obrade podataka koja se sastoji od primjene profila na pojedinca,osobito radi donošenja osluka u vezi tog pojedinca ili radi analiziranja ili predviđanja njegovih osobnih preferencija,ponašanja i stavova

- u Preporukama se kao opće načelo utvrđuje poštivanje temeljnih ljudskih prava i sloboda, načelo da države članice moraju pridržavati dizajniranje i provedbu postupaka i sustava u skladu sa zaštitom OP i privatnosti kao i poduzimati odgovarajuće mjere radi izbjegavanja razvoja i korištenja naprednih tehnologija

- države članice moraju osigurati da s Preporukom budu upoznate sve relevantne osobe, tijela javne vlasti, javna ili privatna tijela,a pogotovo ona koja sudjeluju u postupcima profiliranja i koja ih koriste te nadležna tijela za zaštitu OP i standardizaciju

- one ih trebaju poticati da uvode i promiču samoregulacijske mehanizme,donose kodekse i primijenjuju tehnologije koje se navode u Preporukama

**5.3. Modernizacija međunarodnog i EU pravnog okvira**

- Europska konvencija je danas jedini međunarodnopravno obvezujući instrument s objedinjenim temeljnim načelima zaštite OP(mogu joj pristupiti države koje nisu članice Vijeća Europe)

- 2015.g. je Vijeće UN-a za ljudska prava donijelo **Rezoluciju o pravu na privatnost u digitalno doba** kojom se 1.put u povijesti UN-a uspostavlja funkcija neovisnog stručnjaka za pravo na privatnost u svrhu nadziranja,ispitivanja i izvješćivanja o pravu na privatnost)

- danas je u tijeku zakonodavni postupak u povodu prijedloga novog općeg pravnog okvira kojim bi se stavila izvan snage Direktiva ZOP

**5.3.1. Prijedlozi jačanja sustava zaštite osobnih podatka u digitalnom okruženju**

- to je na prvome mjestu predloženo rješenje vrlo širokog teritorijalnog područja primjene Uredbe o općoj zaštiti osobnih podataka

- njezina se primjena predlaže pri obradi OP u kontekstu aktivnosti poslovnog nastana voditelja zbirke ili izvršitelja obrade u EU i kada obradu OP ispitanika u EU vrše voditelji zbirki bez poslovnog nastana u EU ako se aktivnosti te obrade odnose na ponudu roba ili usluga tim ispitanicima ili na nadzor njihova ponašanja(može uključivati praćenje ispitanika na internetu radi njihova profiliranja)

- izrijekom utvrđeni indifikatori putem kojih je moguće izravno ili neizravno identificirati fizičku osobu uključuje podatke o lokaciji i jedinstvene identifikatore

- Uredba bi se primijenjivala i na obradu koja uključuje identifikatore koje pružaju uređaji, aplikacije,alati i protokoli,kao što su IP adrese,identifikatori kolačića i RFID etikete(osim ako se ti identifikatori ne odnose na identificiranu fiz.osobu ili fiz.osobu koja se može identificirati)

- značajka **pseudonimizacije** je da se OP više ne mogu pripisati određenom ispitaniku bez korištenja dodatnih informaicja sve dok se te dodatne informacije čuvaju odvojeno i dok podliježu tehničkim i organizacijskim mjerama kojima se osigurava nepovezivanje s konkretnim ispitanikom

- u prijedlogu Uredbe se utvrđuju i **odredbe o sigurnosti obrade osobnih podataka** s osnovnom zadaćom voditelja zbirki i izvršitelja obrade da provode odgovarajuće tehničke i organizacijske mjere kako bi osigurali razinu sigurnosti koja odgovara rizicima obrade (pritom se ocjenjuje rizik obrade i uzimaju se u obzir najnovija dostignuća,tj.tehnologije i trošak provedbe)

- **načelo predefinirane zaštite osobnih podataka (data protection by default)** nalaže obvezu voditelja zbirke da osigura to da se kao početna vrijednost obrađuju samo oni OP koji su nužni za svaku određenu svrhu obrade i osobito da se ne prikupljaju,zadržavaju ili šire više od nužnog minimuma za te svrhe

- tim mehanizmom se treba osigurati kao početna vrijednost to da OP ne budu automatski dostupni neodređenom broju osoba i da ispitanici budu u mogućnosti nadzirati dijeljenje svojih OP

- **načelo zaštite osobnih podataka po dizajnu** predstavlja obvezu prema kojoj su voditelj zbirke i vršitelj obrade(ako postoji) dužni u vrijeme utvrđivanja svrha i sredstava obrade OP te u vrijeme njihove obrade,provoditi tehničke i organizacijske mjere i postupketako da ta obrada bude u skladu s Uredbom i da se osigura zaštita prava ispitanika

- u prijedlogu Uredbe se podržavaju i mehanizmi certificiranja te izdavanja tzv.pečata ili žigova za zaštitu OP (omogućava se brza,pouzdana i povjerljiva procjena razine zaštite OP)

**5.4. Zaštita osobnih podataka i privatnost u području elektroničkih komunikacija**

- Direktiva 2002/58/EZ je 1 od 5 direktiva koje zajedno s još 2 uredbe sačinjavaju važeći regulatorni okvir EU za elek.kom. mreže i usluge; **direktive:**

**a)** Direktiva 2002/19/EZ o pristupu i međupovezivanju elek.kom.mreža i pripadajuće opreme- **Direktiva o pristupu**

**b)** Direktiva 2002/20/EZ o ovlaštenjima na području elek.kom.mreža i usluga- **Direktiva o ovlaštenjima**

**c)** Direktiva 2002/21/EZ o zajedničkom regulatornom okviru za elek.komunik.meže i usluge – **Okvirna direktiva –** posljednji put mijenjana **Direktivom o boljoj regulaciji**

**d)** Direktiva 2002/22/EZ o univerzalnim uslugama i pravima korisnika u vezi s elek.komunik. mrežama i uslugama – **Direktiva o univerzalnim uslugama**

- **uredbe:**

**a)** Uredba br.1211/2009 o osnivanju Tijela europskih regulatora za elektr.komunikacije (BEREC) i Ureda

**b)** Uredba br. 531/2012 o roamingu u javnim pokretnim komunik.mrežama u Uniji

- razlog za donošenje Direktive 2002/58/EZ je razvoj interneta

**5.4.1. Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM)**

- HAKOM je domaći regulator tržišta elektroničkih komunikacija,poštanskih i željezničkih usluga u čiju nadležnost spada i davanje stručnih mišljenja i objašnjenja u primjeni ZEK-a i propisa donosenih na temelju tog zakona

- dio njegovih usluga čini promicanje interesa korisnika usluga i osiguravanjem visoke razine zaštite OP i privatnosti kao i osiguravanjem održavanja cjelovitosti i sigurnosti javnih komunikacijskih mreža(čl.5. st.4. t.3. i 6.)

- nadzor nad provedbom usklađenosti poslovanja operatora elek.komunik.mreža i usluga s odredbama zakona o sigurnosti i cjelovitosti elek.komunik. mreža i usluga te zaštiti OP izričito se utvrđuje kao 1 od poslova u nadležnosti HAKOM-a koji se obavlja kao javna ovlast (čl.12. st.1. t.13.)

- HAKOM surađuje s AZOP-om te s tijelima nadležnim za usklađivanje prevencije i zaštitu od računalnih ugroza sigurnosti informacijskih sustava u skladu s preporukama Europske agencije za sigurnost mreža i podataka (ENISA)

- HAKOM i AZOP surađuju u provedbi odredbi ZEK-a u kojima je implementirana Direktiva 2002/58/EZ 🡪 u zakonu se propisuje da oba tijela mogu u skladu sa svojim ovlastima,po službenoj dužnosti ili na zahtjev stranke,odlukom narediti prestanak povreda odredbi tog zakona (čl.99.-107.),a tu odluku donose po službenoj dužnosti ili na zahtjev stranke (čl. 107a.)

- HAKOM (tj.inspektori elek.komunikacija) obavlja inspekcijski nadzor nad primjenom ZEK-a, njegovih prpisa te međunarodnih ugovora i sporazuma iz područja elek.komunikacija

- 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 nije dopuštena žalba,ali je moguć upravni spor pred mjesno nadležnim upravnim sudom)

- protiv rješenja inspektora u vezi s teškim povredama ZEK-a može se pokrenuti upravni spor pred Visokim upravnim sudom RH (čl.111. st.1-2 i čl.116.)

**5.4.2. Tajnost elektroničkih komunikacija i pripadajućih prometnih podataka**

- čl.100. ZEK-a utvrđuje obveze radi osiguravanja tajnosti elek. komunikacija i prometnih podataka u javnim komunikacijskim mrežama i javno dostupnim komunik.uslugama (ta obveza je u vezi s čl.36. Ustava RH) 🡪 zabrana slušanja,prisluškivanja,pohranjivanja te svakog drugog oblika presretanja ili nadzora elektroničkih komunikacija i promet. podataka (tom zabranom nisu obuhvaćane tehnička pohrana podataka te zakonsko ovlašteno bilježenje komunikacija i prometnih podataka tijekom zakonitih poslovnih radnji u svrhu pružanja dokaza o trgovačkim transakcijama ili drugim poslovnim komunikacijama)

- predmet zaštite su komunikacija i pripadajući prometni podaci(definirani u čl.2. ZEK-a)

- **komunikacija** je svaka obavijest razmijenjena ili prenesena između konačnog broja sudionika putem javno dostupne elek.komunik.usluge,a ne obuhvaća obavijesti koje se prenose javnosti elek.komunik. mrežom u sklopu djelatnosti radija i televizija,osim obavijesti koje se mogu povezati s odredivim pretplatnikom ili korisnikom usluga koji ih prima

- **prometni podaci** su bilo koji podaci koji se obrađuju u svrhu prijenosa komunikacije elektroničkom komunikacijsom mrežom ili u svrhu obračuna i naplate troškova

**5.4.3. Obrada prometnih podataka**

- prometni podaci sadrže informacije o privatnom životu fizičkih osoba i tiču se prava na poštovanje dopisivanja fizičkih osoba,ali i određenih legitimnih interesa pravnih osoba

- tipični primjer prometnih podataka je u telefoniji

- u prometne podatke može spadati oblik u kojem se komunikacija prenos 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 i završava te podaci koji se odnose na trajanje,početak i kraj veze

- na temelju prometnih podatak može se dobiti uvid u aktivnosti,interese i lokaciju osobe

- u **Zakonu o elektroničkim komunikacijama** sukladno **Direktivi 2002/58/EZ** (čl.6.) su utvrđene posebne obveze operatora javno dostupnih elektr.komunik.usluga,tj.mreža pri njihovom prikupljanju,odnosno obradi (čl.102.)

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

- postoji niz okolnosti radi kojih će operatori trebati koristiti prometne podatke,a koji nisu anomizirani 🡪 da bi se to realiziralo,potrebno je zadovoljiti određena pravila koja odražavaju temeljna načela zaštite OP kao što su načelo određenosti svrhe obrade podataka i načelo razmjernosti(proporcionalnosti)

- prometni podaci koji se odnose na pretplatnike,odnosno korisnike usluga moraju se obrađivati radi obračuna i naplate troškova pružene usluge

- u ZEK-u se propisuje da operatori smiju obrađivati one prometne podatke koji su potrebni za obračun troškova elektr.-komunik. usluga pretplatnika ili korisnika usluga te troškova međupovezivanja,ali samo do zastare tražbina u skladu s općim propisima o obveznopravnim odnosima

- operatori su dužni obavijestiti pretplatnike,tj.korinsike usluga o vrstama prometnih podataka koji se obrađuju i o trajanju obrade podataka u svrhe obračuna te troškova međupovezivanja(obavještanje je moguće npr. u okviru pretplatničkog ugovora)

- pristup obradi prometnih podataka u takvim slučajevima je 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 🡪 cilje je sprječavanje rizika da neovlaštene osobe obrađuju podatke te osiguravanje da ovlaštene osobe obavljaju samo one potrebne najnužnije radnje

- operatori moraju i obrađivati podatke radi otkrivanja te zaustavljanja prijevara u obliku neplaćenog korištenja elektr.-komunik. uslugom

- u ZEK-u se propisuje da je pristup obradi dopušten samo volaštenim osobama operatora koje između ostaloga rade i na poslovima upravljanja elek.-komunik. mrežom,obrade pritužbi potrošača i otkrivanja prijevara

- prometni podaci se mogu obrađivati i u druge zakonom propisane svrhe i pod posebnim pisanim uvijetima( svrha promidžbe elek.-komunik.usluga i svrha pružanja pojedinih posebnih usluga) 🡪 prema Direktivi 2002/58/EZ je riječ o **uslugama s dodanom vrijednosti** (value-added services) – usluge radi čijeg se pružanja prometni podaci trebaju obrađivati u širem opsegu,odnosno izvan opsega koji je nužan za realizaciju samog prijenosa komunikacije ili obračuna te naplatu njezinih troškova

- u izmjeni ZEP-a 2011. za usluge s dodanom vrijednosti koristi se naziv **usluge s posebnom tarifom**

- propisani uvijet privole pretplatnika ili korisnika usluge se daje nakon što je korisnik obaviješten o vrstama podataka i trajanju obrade u svrhu promidžbe elek.-kom. usluga te u svrhu pružanja usluga s dodatnom vrijednošću( i tu vrijedi pravilo ograničenog pristupa podacima)

**5.4.4. Obrada podataka o lokaciji bez prometnih podataka**

- prema čl.2. ZEK-a **podaci o lokaciji** označavaju bilo koje podatke obrađene u elek.komunik. mreži ili putem elek.komunik.usluge (mogu se odnositi na geografsku širinu,duljinu i visinu korisnikove terminalne opreme,smjer putovanja,razzinu preciznosti inf.o lokaciji,itd.)

- podaci o lokaciji se obrađuju zajedno s prometnim podacima

- u digitalnim mobilnim mrežama će podatak o zemljopisnom položaju terminalne opreme korisnika biti obrađivan kako bi se komunikacija mogla prenijeti između pozivatelja i pozvane strane (tu se podaci o lokaciji smatraju prometnim podacima)

- u **Preporuci Vijeća Europe br.R(95) o zaštiti osobnih podataka u području telekomunikacijskih usluga,s posebnim osvrtom na telefonske usluge** (1995.g.) je 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 i radi utvrđivanja identiteta osoba s kojima oni komuniciraju

- dopuštena je obrada podataka o lokaciji bez prometnih podataka ako je to poteebno da bi se omogućilo pružanje usluga s dodanom vrijednosti

- čl.104. ZEK-a – podaci o lokaciji bez prometnih podataka ,koji se odnose na pretplatnike ili korisnike javnih komunikacijskih mreža ili usluga,se smiju obrađivati samo ako su anonimizirani,a u suprotnom samo na temelju prethodne privole pretplatnika ili korisnika

- kada se podaci o lokaciji bez prometnih podataka obrađuju u neanonimiziranom obliku, podrazumijeva se da se oni obrađuju radi pružanja usluga s dodanom vrijednosti,što se dopušta samo uz prethodnu privolu pretplatnika,tj.korisnika koji je uslugu zatražio

- prije pribavljanja privole,obvezno je obavještavanje pretplatnika ili korisnika usluge kojima se u svako doba mora omogućiti da uskrate svoju privolu za obradu podataka o lokaciji bez prometnih podataka radi pružanja usluge i treba im se omogućiti privremeno odbijanje obrade i nakon što je pribavljena privola (na besplatan i jednostavan način)

- prikupljeni i dalje obrađivani podaci se moraju zaštititi od svake neovlaštene obrade

- u čl.106. ZEK-a se propisuje obveza operatora javno dostupnih telefonskih usluga da onemoguće privremeno odbijanje ili izostanak privole i to za svaki pozivni broj nadležnih državnih tijela i hitnih služba u skladu s njihovim pisanim zahtjevom

- čl.108. st.4. ZEK-a uređuje slučaj kada operatori javnih komunikacijskih mreža i elek.kom. usluga moraju ispunjavati propisane obveze prema operativno-tehničkom tijelu nadležnom za nadzor elektron.komunikacija i prema tijelima koja su ovlaštena za primjenu mjera tajnog nadzora elekt.komunik.mreža i usluga

**5.4.5. Obvezno zadržavanje podataka u elektroničkim komunikacijama**

- **svrha zadržavanja** prema **Direktivi o zadržavanju podataka** je osiguravanje dostupnosti podataka radi istrage,otkrivanja i progona teških kaznenih djela kako ih svaka država članica EU definira u domaćem pravu

- podaci se pohranjuju u elektroničkim komunikacijama u roku od 6 mjeseci do 2 godine

- utvrđuju se jamstvo poštovanja i ustavnopravne zaštite slobode ,tajnosti dopisivanja i svih drugih oblika općenja (čl.36.),jamstvo poštovanja i ustavnopravne zaštite osobnog života (čl.35.) te pravo na sigurnost i tajnost osobnih podataka (čl.37.)

- obvezno zadržavanja podataka podrazumijeva praćenje i pohranu, na dulji rok,podataka koji se odnose na korištenje elek.komunik.uslugama svih pretplatnika i korisnika usluga

-2014.g. je Direktiva o zadržavanju podataka proglašena nevaljanom(prsuda Suda pravde EU)

- u domaćem okviru je zadržavanje podataka za rok od 12 mjeseci od komunikacije regulirano odredbama:

**1)** ZEK (čl.109.-110.)

**2)** Uredba Vlade RH o obvezama iz područja nacionalne sigurnosti RH za pravne i fizičke osobe u telekomunikacijama

- obvezno zadržavanje i to za rok od 1 godine je u domaćem rpavu uređeno i Zakonom o sigurnosno-obavještajnom sustavu RH

**5.4.6. Pohrana i pristupanje podacima u terminanoj opremi**

- iako se smatra da terminalana oprema pripada korisniku i čine dio njegova privatnog života, oni mogu biti kompromitirani tako da treći bez znanja i privole pristupaju terminalnoj opremi

- štetne posljedice su prisutne kod raznih malicioznih virusa i softvera koji omogućavaju tajni nadzor radnji korisnika terminalne opreme i kontrolu na radom te opreme(poput spywarea)

- danas su posebno aktualna pitanja u vezi s poduzimanjem online ciljanog ili bihevioralnog oglašavanja,tj.praćenja ponašanja na mreži radi poduzimanja ciljanih oglašivačkih aktivnosti

- u Direktivi 2002/58/EZ 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 elektroničkom komunikacijskom mrežom(ZEK ne slijedi takav pristup)

- po ZEK-u se korištenje elekt.-kom.mrežoama 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 OP,a time se ne može spriječiti tehnička pohrana podataka ili pristup podacima isključivo u svrhu obavljanja prijenosa komunikacija putem elek.komunik.mreže ili radi pružanja usluga informacijskog društva na zahtjev pretplatnika ili korisnika usluga

**5.4.7. Sigurnost i cjelovitost elektroničkih komunikacijskih mreža i usluga**

- čl.99. ZEK-a sadrži rješenja važećeg regulatornog okvira EU-a za područje elektr.komunik.

- posebne obveze operatora uključuju primjenu odgovarajućih tehničkih i ustrojstvenih mjera kako bi se zaštitila sigurnost njihovih usluga te obvezu poduzimanja potrebnih mjera zaštite sigurnosti elek.-kom. mreže i usluga

- mjere se osobit provode kako bi se sprječio i umanjio utjecaj sigurnosnih incidenata na korisnike usluga i međupovezane elektroničke komunikacijske mreže

- mjerama se mora osigurati to da OP mogu pristupati samo ovlaštene osobe u zakonom dopuštene svrhe,kao i da se preneseni ili pohranjeni OP 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 OP radi utvrđivanja ranjivosti u sustavu

-operator javno dostupnih elek.-komunik.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 njenih posljedica uključujući naznaku troškova tih mjera

- u slučaju povrede sigurnosti ili gubitka cjelovitosti,operatori su dužni obavijestiti HAKOM pisanim putem,a HAKOM može obavijestiti javnost ili zahtijevati od operatera da obavijeste javnost o problemu ako se utvrdi da je ta obavijest u javnom interesu

- operator javno dostupnih elek.-kom. usluga mora odrediti odgovornu osobu za provedbu mjera -> ovlaštena tijela za nadzor mjera i davanje preporuka su **HAKOM i AZOP**

- **Pravilnik o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga** uređuje način i rokove poduzimanja mjera

- **povreda osobnih podataka** je povreda sigurnosti koje uzrokuju slučajno ili nezakonito uništenje,gubitak,izmjenu,neovlašteno razotkrivanje ili pristup OP što se prenose, pohranjuju ioli na drugi način obrađuju u vezi s obavljanjem javno sostupnih elek.-komun. usluga (ZEK, čl.99a., te Uredba Komisije br.611/2013 )

- propisani postupak u slučaju povrede OP prema ZEK-u uključuje obvezu operatora javno dostupnih elek.-kom.usluga da o povredi bez odgode obavijesti HAKOM i AZOP

- Uredbom se uređuju pojedinosti u vezi s obavještanjem nadzornog tijela,a kao načelni rok se uzima rok od 24h od otkrivanja povrede

- o povredi se treba obavijestiti i korinsika,tj.drugu fizičku osobu čiji su podaci povrijeđeni

- prema Uredbi pri utvrđivanju je li vjerovatno da će povreda štetno utjecati na OP ili privatnost trebaju se uzeti u obzir:

**a)** priroda i sadržaj OP o kojima je riječ(posebno kad su podaci financijske prirode)

**b)** posebne kategorije OP iz Direktive ZOP

**c)** podaci o lokaciji internetske datoteke

**d)** povijest pretraživanja u pregledniku

**e)** podaci o e-pošti

**f)** podrobni ispisi računa

**g)** moguće posljedice povrede

**h)** okolnosti povrede (pogotovo ako su podaci ukradeni ili operator zna da su u posjedu neovlaštene treće strane)

- obveza obavještavanja korisnika se prema ZEK-u ne primijenjuje ako HAKOM utvrdi da je operator na OP primijenio odgovarajuće tehnološke mjere zaštite koje moraju učiniti OP nerazumljivim bilo kojoj osobi koja im neovlašteno pristupa

- HAKOM dostavlja mišljenje o potrebi obavješćivanja korisnika,kao i AZOP-u koji je ovlašten zahtijevati od operatora da obavijesti korinsika ako utvrdi da je to potrebno

- operator može u iznimnim slučajevima odgoditi obavještavanje osobe ako bi to moglo ugroziti istragu povrede nakon što se usuglasilo nadzorno tijelo,sve dok to tijelo ne utvrdi da je takvo obavještavanje moguće

**5.5. Privatnost i kriptografija**

- cilj kriptografskih metoda je osigurati tajnost podataka kako njihov sadržaj ne bi bio dostupan osobama kojima nije namijenjen

- **kriptografija** ( grč. kripto-skriveno i graphein-pisanje) - znači sustavno razmještanje ili zamjenjivanje znakova nekog zapisa ili poruke kako bi se očuvala njihova tajnost od onih kojima unaprijed generiran ključ za dešifriranje nije namijenjen

- **kriptologija** (grč. kryptos-skrivena i logos-riječ) je znanost o sigurnoj komunikaciji,a ona obuhvaća kriptografiju i kriptoanalizu

- **kriptoanaliza** (grč. kryptos i analyein-otvoriti) je znanost o ponovnom dobivanju informacija iz njihovog kriptiranog oblika,tj. znanost o dešifriranju prethodno enkriptiranih poruka

- prve kriptografske metode se razvijaju u antičko doba(do kraja 19.st. nemaju širu primjenu)

- kriptografija se danas koristi za kodiranje(ekripciju,šifriranje) podataka uz pomoć algoritma za ekripciju s namjerom da se tajno i sigurno prenesu komunik. kanalom do primatelja

- algoritmi za enkripciju se koriste „ključevima“ u obliku binarnih brojeva (40,128 ili više bitova) uz pomoć kojih se podaci u binarnom obliku kombiniraju s njegovim bitovima prema određenommatematičkom 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

- **postupak kodiranja se može provesti:**

**a) softverski** –prednos cijena i fleksibilnost

**b) hardverski**- prednost brzina(može biti veća od 10 do čak 100 puta)

- **kriptografske sustave je moguće klasificirati:**

**1)** prema matematičkim operacijama putem kojih se izvirna pouka(tzv.plaintext) skriva primjenom enkripcijskog ključa,a s obzirom na to razlikuju se:

**a)** sustav transpozicije(premještanja)-znakovi se razmještaju unutar poruke po odeđenom ključu,a pritom ne mijenjaju oblik,tj.zanečnje

**b)** sustav supstitucije (izmjene)- znakovi se zamjenjuju drugim znakovima i simbolima preme određenom ključu

**c)** njihova kombinacija

**2)** ovisno o tome koriste li se pošiljatelj i primatelj poruke istim ključem (**simetrični kripto-sustav**) ili različitim ključevima (**asimetrični kripto-sustav**)

- **simetrični algoritam** se koristi **tajnim ključem** koji posjeduju i primatelj i pošiljatelj (takav je **DES algoritam** koji se najčešće koristi 56-bitnim ključem) – ova metoda je najbrža,ali je prijenos ključa nesiguran

- u početku se tvrdilo da ovaj algoritam ne može probiti,ali to se pokazalo krivim 🡪 prvi put je to učinjeno 1993.g. uz pomoć tehnike „**linearna kriptoanaliza**“ za što je bilo potrebno oko 50 dana na samo 1 radnoj stranici,a 2.put 1997.g. za nešto manje od mjesec dana

- danas je DES velikim dijelom zamijenjen algoritmom **AES (Advances Encryption Standard)**

- **asimetrični algoritam** ili metoda **javnog ključa** upotrebljava tajni(privatni) i javni ključ (takav je **RSA algoritam** koji su 1976.g. razvili Rivest,Shamir i Adelman) – sporija,ali sigurnija metoda,prednost je što se koristi različitim ključevima razne dužine za enkripciju i deskripciju

- dok je privatni ključ tajan i ima ga samo primatelj, javni ključ je dostupan svima pa se rako njime mogu koristiti svi putem interneta ili na drugi način

- pošiljatelj se u tom slučaju,koristi javnim ključem kako bi šifrirai podatke koje je moguće dešifrirati samo uz pomoć tajnog ključa koji posjeduje samo primatelj

-posebno visoki stupanj sigurnosti predstavlja 512-bitni ključ za čije bi probijanje trebalo tisuće godina

- ove 2 metode je moguće **kombinirati** tako da se metodom javnog ključa koristi samo za prijenos tajnog ključa,dok se za prijenos podataka koristi metodom tajnog ključa

- **PGP (Pretty Good Privacy)** je jedan od poznatijih kriptografskih programa kojeg je razvio **Phil Zimermann** 🡪 za ekripciju se koristi RSA metodom i pruža odgovarajući stupanj zaštite

- Skype,RedPhone ili Telegram omogućavaju kriptiranu komunikaciju

- **metode koje se koriste u kombinaciji s kriptografijom:**

**a) stenografija**

**b) digitalni potpis**

**c) digitalni certifikat**

**d) digitalni vremenski biljeg**

**5.5.1. Stenografija**

- umijeće i tehnologija skrivenog pisanja čiji je cilj očuvati tajnost komunikacije

- danas se ovom tehnologijom najčešće umeću podaci u neiskorištene dijelove informacijskog paketa koji se prenosi nekim komunikacijskim kanalom

- podaci se putem računalne mreže prenose u paketima koji se sastoje od sadržaja, 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 na korištenje

- prijenos,sigurnost i kontrolu integriteta podataka osiguravaju komunikacijski programi i protokoli

- budući da unutar tih paketa ima neiskorištenih bitova,unutar njih se mogu umetnuti podaci na osnovi kojih će primatelj dobiti neku tekstualnu,video ili audio poruku ili provjeriti vjerodostojnost primljenih podataka ili identite pošiljatelja

- postupak je sličan onome koji se primijenjuje pri zaštiti novca gdje se upotrebljava vodeni žig,umeću zlatne niti i sl., koji na prvi pogled nisu vidljivi korisniku (npr.skrivanje teksta unutar slike) 🡪 sama poruka,slika ili zvučna datoteka ne mora biti uopće zaštićena jer je pretpostavka da treće osobe ne sumnjaju da se u njima krije drugi sadržaj,pa zato ona ne mora biti kriptirana

- postupak se može primijeniti i na neiskorištenim dijelovima magnetskog diska ili diskete

- primjenom ove metode je moguće sakriti i digitalni potpis

**5.5.2. Digitalni certifikat**

- isprava u digitalnom obliku kojom se potvrđuje identitet neke pravne ili fizičke osobe

- izdaju ih za to ovlaštene organizacije (**Certification Authority-CA**) kao što su VeroSign i Mountain View

- sigurnost i povjerljivost podataka iz takve isprave se osigurava 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 elektr. isprava potvrđuje svoj identitet i osigurava nesmetanu i sigurnu komunikaciju (posebno važno u e-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 **sigurnosni protokol** (npr. SSL-Secure Socket Layer ili SET-Secure Electronic Transaction) koji omogućava enkripciju i provjeru takvih digitalnih isprava

**5.5.3. Digitalni potpis**

- **Digital signature** je tehnologija provjere vjerodostojnosti poruka primljenih u komunikaciji koja se odvija između udaljenih kompjutora(takav potpis se nalazi u digitalnom obliku i sastavni je dio šifrirane poruke koja se šalje,a sadrži izračunati zbroj same poruke)

- predstavlja siguran način provjere vjerodostojnosti teksta i komunikacije

- nakon što primatelj dešifrira primljenu poruku i digitalni potpis,sam provjerava zbroj takve poruke i uspoređuje ga s primljenim

- kako digitalni potpis ne potvrđuje identitet osobe,koristi se često 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 zaštićuje sadržaj podataka

**5.5.4. Digitalni vremenski biljeg**

- **Digital time stamping** se koristi za provjeru kada je digitalni dokument kreiran,odnosno posljednji put promijenjen što je važno za utvrđivanje vjerodostojnosti dokumenata primljenih,tj.poslanih putem mreže

- koristi se kriptografijom za stavaranje jedinstvenog koda koji se šalje primatelju,a primatelj uspoređuje primljeni kod s kodom do kojeg je došao sam korištenjem istim algoritmom

**6. cjelina: IZAZOVI KIBERNETIČKOG KRIMINALA**

**6.1. Kibernetički prostor i kibernetički kriminal**

- skraćeno kiberprostor (engl. Cyberspace) 🡪 **Wiliam Gibson** ga prvi upotrebljava u svojoj noveli kao metaforu za globalnu računalnu mrežu na koju se ljudi spajaju svojim umovima

- sve češće je sinonim za ukupnost računalnih mreža, komunikacijskih veza i digitalnih podataka koji se putem njih razmjenjuju, a granice tog nevidljivog svijeta nisu određene i ograničene teritorijalnim granicama zbog čega on obuhvaća sva mjesta na zemaljskoj kugli ili oko nje s kojih se,ili putem kojih se ta komuniakcija odvija neovisno o informacijsko- komunikacijskoj tehnologiji uz pomoć koje se to čini

- u užem smislu kiberprostor je i sinonim za internet, tj. globalni informacijsko-komunikacijski sustav koji povezuje i spaja različte mreže i omogućava ljudima diljem svijeta da komuniciraju međusobno, razmijenjuju podatke, posluju i zadovoljavaju druge potrebe i interese

- često se naziva virtualnim ili prividnom prostorom (zbog nevidljivih veza i netjelesnih podataka koji se putem njih prenose) unatoč tome što počiva na materijalnoj (tehničkoj) infrastrukturi koja omogućava nesmetano odvijanje komunikacije

- kiberprostor obuhvaća najrazličitije informacijske resurse (materijalne i nematerijalne), te digitalne servise i usluge dostupne putem informacijsko-komunikacijskih mreža

- 90-ih godina 20.st. uvidjelo se da kiberprostor u sebi nosi brojne opasnosti kojima se ugrožavaju temeljne vrijednosti čovjeka i društva

- izložen je raznim zlouporabama te napadima kriminala pošto nadilazi granice suverenih država te kontrole i dominantnog utjecaja njihove vlasti što stvara teškoće pri otkrivanju zloporaba, određivanju nadležnosti i izručivanju počinitelja

- **karakteristike kiberprostora** : globalnost, otvorenost, dostupnost, decentraliziranost i neovisnost o posebnoj infrastrukturi 🡪 učinile su kiberprostor izvorom sve brojnijih, nemoralnih i nezakonitih djela

- vrlo je teško otkriti počinitelja radi nepostojanja centralnog autoriteta, rasprostranjenosti, dostupnosti i velikog stupnja anonimnosti

- **kiberkriminal** ima svoje koristi u računalnom kriminalu 🡪 ne postoji općeprihvaćena definicija, ni suglasnost koja djela obuhvaća (često se pogrešno tumači kao sinonim za računalni ili internetski kriminal)

- osim računalnog i telekomunikacijskog kriminala obuhvaća i neke tradicionalne, ali i novije oblike kriminala u kiberprostoru

- dosta brzo se širi uprvo zbog karakteristika samog kiberprostora,pa ne predstavlja zaokruženu i jedinstvenu fenomenološku kategoriju već je on postao „opća forma kroz koju se ispoljavaju različiti oblici kriminalnih aktivnosti, forma koja će u budućnosti postati dominantna“ ( **Donn Parker**, sred. 80-ih)

- suradnja Europskog parlamenta, Vijeća, Europskog gospodarskog i socijalnog odbora i Odbora regija pod nazivom **„Strategija kibersigurnosti Europske unije: Otvoren, siguran i zaštićen kiberprostor“** 🡪 **kiberkriminal** se definira kao širok skup različitih kriminalnih aktivnosti u kojima su računala i informacijski sustavi uključeni ili kao primarni alat ili kao temeljni cilj

- **kiberkriminal obuhvaća:**

**a)** tradicionalna kaznena djela (npr. prijevare, krivotvorenja, krađa identiteta)

**b)** kaznena djela u svezi sa sadržajem (npr. online distribucija dječje pornografije ili poticanje na rasnu mržnju)

**c)** djela jedinstvena za računalne i informacijske sustave (npr. napadi na informacijske sustave, uskraćivanje usluga i malver)

- polazeći od Konvencije o kibernetičkom kriminalu Vijeća Europe i kaznenih djela koja su njome propisana, kiberkriminal se definira kao ukupnosti kaznenih djela počinjenih protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava (nezakoniti pristup, ometanje podataka, ometanje sustava, presretanje nejavnog prijenosa podataka i zloporabu naprava), računalnih kazennih djela (računalne prijevare i računalno krivotvorenje), kaznenih djela u svezi sa sadržajem (dječje pornografije,rasizma i ksenofobije) te kaznenih djela povrede autorskih i srodnih prava

**6.2. Obilježja kibernetičkog kriminala**

- kriminalni potencijal kiberprostora proizlazi iz njegove dostupnosti,masovnosti i sve veće ovisnosti društva o korištenju i nesmetanom radu inf.-komunik. sustava

**6.2.1. Dostupnost naprava za činjenje kaznenih djela**

- kiberkriminalu pogoduje široka rasprostranjenost i dostupnost alata i podataka kojim se koriste za počinjenje kaznenih djela 🡪 ti alati su dostupni na **površinskom** i **dubinskom webu**

- **površinski web –** kriminal dostupan putem hakerskih stranica, tematskih (news) grupa i foruma na kojem se nude i razmjenjuju softverski alati, upute, neovlašteno pribavljanje korisničke lozinke i savjeti kako činiti takva djela

- pri **dubinskom webu** (Deep Web) treba razlokovati njegov anoniman dio koji se ne koristi za nezakonite svrhe i dio koji pogoduje širenju kriminalnih djela u kiberprostoru ili fizičkom svijetu ( **Darkweb ili Darknet** )

- standardni pretraživači prikazuju mali dio internetskih sadržaja koji se nalaze na tzv. površinskom internetu, a najveći dio im je nedostupan 🡪 taj dio intereneta se naziva **Deep Web** (poznat i kao Hidden Web, Deepnet ili Nevidljivi web) – veličina tog prostora 2001.g. prema Bergmanu iznosi oko 7.5. petabajta

**- Darknet** čine privatne mreže za razmjenu datoteka između povjerljivih osoba kojima se pristupa putem nestandardnih pretaživača i protokola 🡪 korisnici mogu sačuvati svoju anonimnost (osobne podatke, IP adresu, lokaciju, online aktivnosti) i učiniti svoj sadržaj nedostupan web-pretraživačima s pomoću mreža i komunikacijskih protokola koristeći se enkripcijom komunikacije

- najčešće se koriste **TOR (The Onion Router), Freenet i Nevidljivi projekt interneta (I2P)** 🡪 čuvaju anonimnost korištenjem kriptografije i slanjem poruka i drugih digitalnih sadržaja preko niza posrednika

- prednosti anonimne komunikacije prepoznali su hakeri i organizirani kriminalci kako bi što neprimjetnije mogli obavljati ilegalne radnje

- značajan slučaj u kojem se koristio Darknet je stranica Silk Road na kojoj su se virtualnom valutom Bitcoin plaćale različite usluge (kupnja ilegalnih droga, pranja novaca i ostala kaznena djela) 🡪 stranicu je ugasio FBI 2013. godine

- dvogodišnjom suradnjom Interpola, Europola, davatelja internetskih usluga i privatnog sektora, Silk Road je ukinut, a Ross Ulbricht (zvani Dread Pirate Roberts, DPR), osnivač i glavni organizator ilegalnog tržišta narkotika na Deep Webu osuđen je u svibnju 2015. na doživotnu kaznu zatvora

- pojavile su se i slične stranice kao Silk Road 2.0

**6.2.2. Rast i rasprostranjenost crnog kibertržišta**

- velika je vjerojatnost da se će se takva tržišta teško u potpunosti zatvoriti jer dok god ima potražnje, bit će i ponude

- tržište obuhvaća: drogu, bitcoin, usluge pranja novca, uradene račune, lažne putovnice i državljanstvo, neovlašteno pribavljene podatke o vladi, policiji, slavnim osobama, izvršenje atentata

- **kiberkriminalci za prikrivanje svojih aktivnosti koriste TOR kako bi distribuirali različit malver poput:**

**a) CryptoLocker** – onemogućuje žrtvama pristup njihovim datotekama dok ne plate otkupninu u iznosu od jednog bitcoina (oko 600$) te se nakon toga datoteke dekriptiraju

**b) P2PZeuS** – novija i sofisticiranija verzija bankarskog malvera Zeus koja krade financijske i druge vjerodajnice koje kriminalci prodaju na crnom kibertržištu

*\*pročitati podatke istraživanja američke tvrtke Trend Micro (169.-170.str.)*

- na osnovi istraživanja korporacije RAND, zaključeno je da će Darknetovi u sljedećim godinama poticati kriminalne aktivnosti, veću uporabu kripto-valuta, veće anonimne sposobnosti malvera i veće korištenje enkripcijom komunikacija i transakcija

- hakerska zajednica i crno kibertržište su u neprekidnom rastu

- **temeljno obilježje crnih kibertržišta** je da brzo odogovaraju i prilagođavaju se ovisno o vanjskim utjecajima

- zbog ukidanja određenih crnih kibertržišta, sve se više transakcija seli na darknetove, provodi se stroža provjera, veća enkripcija, a koriste se i raznim tehnikama anonimizacije

- iako su redarstvene vlasti aktivne te dolazi i do međunarodne suradnje kad je pitanje o crnom kibertržištu, ono ipak ostaje fleksibilno i raste veoma brzo te postaje sve kreativnije i inovativnije

- vrlo važna su i istraživanja na tom područuju koja služe razumijevanju trenutnog stanja i predviđanju budućeg što je osnova za suzbijanje štetnog utjecaja takvih tržišta

**6.2.3. Sofisticiranost napada i znanje počinitelja**

- veća sofisticiranost alata kojim se koriste za napad je obrnuto proporcionalna tehničkom znanju potrebnom da bi se napad izvršio

- istraživanja Sveučilišta Carnegie Mellon i njihovog Instituta za softversko inženjerstvo pokazala su da su alati koji se koriste za napad toliko sofisticirani da više nije potrebno visoko tehničko znanje za izvršavanje napada

**6.2.4. Društvena opasnost i štetnosti kiberkriminala**

- postoji visoka **tamna brojka** kiberkriminala čiji je problem što onemogućava potpuni uvid u stvarno stanje i štete na tom području

- to je pojam koji se u kriminologiji označava kao broj realiziranih kažnjivih ponašanja za koja se ne zna zato što nisu otkrivena, a ne zato što im počinitelj nije poznat

- tamna brojka kiberkriminala je visoka i zato što žrtve ne prijavljuju slučajeve kad je došlo do zloborabe 🡪 najčešći je razlog nepovjerenje u pronalazak počinitelja ili prikrivanje takvih podataka iz poslovnih razloga (npr. tvrtke u financijskom sektoru)

*Primjer! Često tvrtke koje posluju u financijskom sektoru,posebno banke u mnogim slučajevima ne prijavljuju kaznena djela kako be bi izgubili povjerenje svojih komitenata. Tek kada su suočeni s golemim štetama ili gubitkom podataka o klijentima, takvi podaci postaju dostupni javnosti i prijavljeni nadležnim institucijama.*

-sve su brojniji pokušaji upada u informacijske sustave financijskih ustanova, porvale u vojne i obavještajne sustave, krađe identiteta, upadi u sustave i na web-stranice raznih tvrtki, organizacija i institucija, a široko je rasprostanjena dječja pornografija te softversko, audio i audivizualno piratstvo

- američka tvrtka McAfee u izvješću **„The economic ipact of cybercrime and cyber espionage“** ističe kako je zbog nedostupnosti podataka jako teško kvantificirati štetu od kibernetičkog kriminala 🡪 vjeruje se da SAD ima visoku razinu dostupnosti podataka o visini gubitaka zbog kiberkriminala, ali ne mogu biti pouzdano određeni (njihova procjena štete se kreće u rasponu od 70 do 140 milijardi dolara,a to je 0,5 i 1% BDP-a SAD-a)

- na najvećem udaru su razvijene države zbog veće rasporstranjenosti tehnologije, ali to ne znači da nerazvijene zemlje ne mogu biti meta jer se tehnologija sve brže širi svojom financijskom dostupnošću

- ENISA stavlja štetu od kiberkriminala u kontekst štete koja nastane od trgovine drogom

- Velika Britanija štetu od kiberkriminala procjenjuje na više od 11 milijardi dolara u 2013.g. što je 0,47% njezinog ukupnog BDP-a

- šteta za australsku ekonomiju procjenjuje se na 100 milijuna dolara, dok Kina, Njemačka i Japan zajedno broje gubitke u iznosu od 100 milijardi dolara

- ITU u svom izvještaju upozorava na stalni rast šteta od računačnog kriminaliteta 🡪 ona je u 2003. g. na svjetskoj razini iznosila 17 milijardi, a taj iznos se u 2007.g. popeo na 100 milijardi dolara

- izvješće američke tvrtke Symantec pokazuje da je godišnje 380 milijuna ljudi bilo žrtva kiberkriminala

- financijski najveću štetu trpe SAD (38 milijardi $), a za njima ne zaostaje niti Kina (37 milijardi $)

- prema BSA (Business Software Alliance, udruga za kolektivnu zaštitu autorskih prava najvećih softverskih tvrtki) globalna stopa po kojoj je softver instaliran je porasla u 2013.g. s 42% (2011.g.) na 43%

- opasnosti od kiberkriminala negativno utječu na rast gospodarstva EU-a zbog nepovjerenja građana u online poslovanje i bojazni da bi mogle biti žrtvom kiberkriminala

- *pročitati rezultate istraživanja tvrtke TNS Opinion & Social (izvještaj Cyber Security) na 173.-174.str.*

**6.3. Najčešće sigurnosne prijetnje u kiberprostoru**

- 2014. Agencija za mrežnu i informacijsku sigurnost EU objavila je izvještaj s pregledom najčešćih prijetnji i trendova na području kiberkriminala

**Maliciozni kod: računalni crv i trojanski konj**

- **maliciozni programi (eng. Malware)** – računalni programi ili dijelovi programskog koda čije pokretanje dovodi do neželjenih posljedica po korisnika/njegov računalni sustav, podatke ili programe 🡪 to su računalni crv, trojanski konji, računalni virusi, spyware i adware programi

**a)** **Računalni crv** – program koji se sam umnaža na računalu korisnika i velikom brzinom širi putem mreže s jednog računala na drugi te na taj način smanjuje propusnost mreže i ometa rad računalnog sustava i mreže

- **Morrisov crv** – 1988.g. je inficirao tisuće računala pod operativnim sustavom Unix, a mete su uglavnom bila računala u obrazovnim institucijama SAD-a

- **Blaster** – 2003. je inficirao desetke milijuna Microsoft Windows XP/Windows 2000 računala

- **Conficker** – od 2008.g. se širi, još uvijek aktivan i vrlo rasprostranjen

**b) Trojanski konj** – naizgled običan proram koji ima neku skrivenu funkciju nepoznatu njegovu korisniku

- cilj mu može biti omogućavanje neovlaštenog pristupa, krađa podataka, nadzor aktivnosti kosrisnika, izvođenje dDoS (distributed Denial of Service) napada, traženje sigurnosnih propusta u sustavu, itd.

**c)** **Računalni virus** – program ili dio programskog koda koji je učitan na računalo bez znanja njegovog korisnika s određenim funkcijama koje ovise o namjerama autora tog programa

**d) spyware** – program koji se koristi resursima računala ili mreže bez znanja korisnika s ciljem da nadgledaju njegove nevike, posebno na internetu, o čemu zatim šalju podatke prema određenom poslužitelju

**e) adware** – vrsta parazitskog programa koji ovisno o sadržaju neke web-stranice pokazuju reklame, ankete, nude neke proizvode ili sl.

- više od polovine malicioznih programa ostaje neotkriveno upravo zbog svoje prikrivene aktivnosti i visoke složenosti iako postoji antivirusna zaštita koja se pokazala nedostatnom 🡪 teže se uništavaju i zato što u slučaju otkivanja imaju mogućnost promijeniti svoju strukturu i na taj način ostati neotkriveni

- zbog lake dostupnosti takvih programa, broj malwarea se brzo povećava

- malware ima mogućnost promijeniti cilj nakon što je prvobitan izvršen te na taj način nastaviti izvršavati štetne zadaće

**Napadi putem weba**

- izvode se pomoću skupa malwarea, tehnika ili softvera za pronalaženje sigurnosnih slabosti koje preusmjeravaju web preglednik na maliciozne web-stranice gdje se sustav može podvrgnuti daljnjim napadima kao što su:

**a) drive-by downloads** – skidanje neželjenog sadržaja bez znanja i sudjelovanja subjekta koji pristupa stranicama za koje smatra da su sigurne

**b) clickjacking** – zlonamjerna tehnika kojom se web-korisnike navodi da kliknu na maliciozni sadržaj, a da o njegovoj zlonamjernosti nemaju saznanja

- te napade možemo nazvati i napadima preusmjerivanjem preglednika na zaražene stranice

**Napadi putem web aplikacija**

- napadi na programe pohranjene na udaljenom web poslužitelju koji se koriste preko interneta putem sučelja preglednika (npr. pristup mobilnom bankarstvu putem web aplikacije koja se nalazi na web-stranicama banke)

- korisnik takvoj aplikaciji pristupa koristeći se lozinkom, tokenom ili sličnim uređajem za identifikaciju

- **cilj napada** je zaobilaženje provjera i novlašteni pristup web aplikaciji, a zatim i bazi podataka kojoj se putem nje pristupa

- **posljedice su** mogućnost krađe podataka, manipulacija podacima, prenošenje malwarea, preuzimanje kotrole nad računalom

- **Injection napad** je napad kojim haker u sučelje aplikacije umjesto lozinke ili token koda unosi neki izraz u jeziku u kojem je programirana web aplikacija, a koji će se kad ga web aplikacija inerpretira zapravo prenijeti u program same aplikacije promijenivši njegov učinak te omogućiti hakeru da stekne administrativne ovlasti, zaobiđe autentikaciju ili ostvari neki drugi obilk neovlaštenog pristupa ili neku drugu zlouporabu

- **ovakvi napadi su sve češći zbog:**

**1)** zastarjelih verzija softvera Java na kojem je izgrađena većina ugroženih web-stranica

**2)** nedostatno obrazovanje programera u pogledu sigurnostnih standarda u programiranju

**3)** naručitelji često svjesno ignoriraju rizike, inzistirajući na brzom razvoju, nedostatnom testiranju i niskim troškovima rada programera

**Botnetovi**

- skupovi računala koja su zaražena malicioznim programom što omogućava osobi koja ga je stvorila određeni stupanj kontrole nad zaraženim računalima

- korisnik zaraženog računala nije svjestan da mu je računalo zaraženo

- zaraženo računalo postaje tzv. **zombi** ili **bot računalo** koje čeka instrukcije od glavnog računala (engl. **Bot master**)

- nakon nekog vremena dolazi do ujedinjenja industrijskih interesa i političkih interesa što je dovelo do međunarodne suradnje koja je rezultirala ukidanjem nekih većih botnetova

- najveća akcija se vodila protiv ZeroAcces botneta 🡪 smanjen broj botneta koji djeluju putem osobnih računala

-botnetovi i dalje ostaju važno sredstvo koje se može iskoristiti za činjenje različitih zloporaba poput dDOS napada ili slanja SPAM poruka prema velikom broju udaljenih računala

**Napad uskraćivanjem usluga (DOS napad)**

- oblik računalne sabotaže koja se čini slanjem velike količine podataka prema nekom udaljenom računalu (hostu ili serveru) sa svrhom da se oteža ili onemogući korištenje ovlaštenim korisnicima

- ako se to čini automatizirano s većeg broja udaljenih računala onda je riječ o **distribuiranom uskraćivanje usluga** (**Distributed Denial of Service – dDOS**)

- do takvog napada dolazi namjernim, istodobnim slanjem velikog broja upita s brojnih računala uslijed čega dolazi do zagušenja središnjeg računala prema kojem je napad bio usmjeren , a time se ometa i uspora rad sustava, a ovlašteni korisnici su spriječeni redovito ga koristiti

- najugroženije su one tvrtke, organizacije ili institucije koje isključivo koriste elektroničko poslovanje

- mogu se pojaviti u kombinaciji s drugim programima poput Spyware, Adware ili Mail bomb

- **Mail bomb** je program čijim se pokretanjem žrtva upisuje na niz velikih lista elektroničke pošte čime se multiplicira broj poruka koje su usmjerene prema njoj

- uskraćivanje usluge je također jedan oblik kiberkriminala koji raste

- sve veća propusnost mreže dovodi do toga da za DoS napade nisu nužni botnetovi kao prije, već manji broj računala ili servera koji šalju veću količinu podataka na računalo žrtve

- najveći DoS napada koristi se bi se ostvarili prikriveni ciljevi: slanje virusa i drugih malicioznih programa, krađe podataka, krađe intelektualnog vlasništva i krađe financijskih sredstava

- sama prijetnja napadom može poslužiti da bi se drugog prisililo da učini nešto na svoju štetu 🡪 **kiberiznuda (Cyberextortion)** čiji je cilj pribavljanje imovinske koristi (jedan vid kiberiznude je Ransomver)

**Spam**

- neželjena elektronička pošta ili druga elektronička priopćenja koja primamo mimo naše volje

- najčešće se šalju razne reklame i marketinške aktivnosti tvtki koje se na taj način jeftino reklamiraju i obavještavaju veliki broj korisnika o ponudi svojih proizvoda ili usluga

- radi se o zloupotrebi jer su u pitanju poruke koje ne želimo primati, koje nas ometaju u svakodnevnom radu, a dovode i do zagušenja komunikacijskih kanala

- jedan oblik spama koji se smatra posebno opasnim s obzirom na sadržaj su tzv. **hoaxi** 🡪 lažna upozorenja poslana elektroničkom poštom s namjerom da se primatelja prevari, zastraši, kompromitira, dezinformira ili odvrati od korištenja nekim uslugama ili proizvodima

- broj spam poruka se proteklih godina smanjio upravo zbog razvoja sofistiricanih sučelja e-pošte koja sadržavaju filtere za automatsko prepoznavanje i blokiranje neželjene elektroničke pošte

**Phishing (carding, brand spoofing)**

- oblik krađe identiteta i jedan od najčešćih oblika prijevare u kibenetičkom prostoru

- podrazumijeva slanje prijevarnih poruke e-pošte koje izgledaju kao da ih je poslala neka poznata tvrtka ili institucija

- ovakvim se porukama traži od primatelja da iz nekih razloga odgovori na poruku i upiše svoje osobne podatke (ime, broj bankovne ili kreditne kartice, korisničkog imena i lozinke, itd.)

- drugi uvjerljiviji način je da se u poruci nalazi poveznica na lažne stranice koje po izgledu sliče izvornim stranicama te tvrtke ili institucije

- **Simple Mail Transfer Protocol (SMTP)** – komunikacijski protokol koji ne sadrži mehanizme za autentifikaciju (provjeru pošiljatelja) što otvara mogućnost brojnih zloporaba koje se nazivaju **e-mail spoofing**

- nakon toga slijedi upit o traženim podacima koje lakovjerni primatelji daju

**- neke od češćih vrsta prijevare u kibernetičkom prostoru:**

**a) online aukcijske prijevare** – plaćena roba se ne isporučuje ili se isporučuje krivotvorena roba ili roba slabije kvalitete, rezultat je financijski gubitak za osobu koja unprijed plaća robu

**b) online ponude poslova** – od žrtve se traži da uplati određeni iznos za manipulativne troškove ili radne materijale koji će mu biti potrebni za obavljanje posla

**c) online investiranje** – lažni informacijama o mogućim ulaganjima, o rastu ili padu vrijednosti dionica neke tvrtke i sl. želi ostvariti korist

**d) komunikacijska prijevara** – prijevarno se koriste bežićne, satelitske ili telefonske usluge upotrebom malicionznih programa čiji je cilj da, bez znanja korisnika, preusmjere vezu na neki drugi telefonski broj,tj. prema drugom davatelju usluga

**e) prijevara putem e-pošte i lažnih web-stranica**

- najčešći slučajevi ovih prijevara su phishing i nigerijsko pismo (Nigerian 419 Scams)

- **nigerijsko pismo** – primjer iskorištavanja lakovjernosti ljudi putem poruka e-pošte čiji se sadržaj najčešće odnosi na ponudu različitih poslovnih mogućnosti uz laku, brzu i veliku zaradu

**Sredstva za iskorištavanje ranjivosti (Exploit Kits)**

- skup alata koji se upotrebljavaju radi iskorištavanja sigurnosnih propusta u nekom softveru ponajprije radi širenja malwarea

- dolaze zajedno s kodovima namijenjenim iskorištavanju sigurnosnih propusta

- ponajprije su usmjereni na programe koji su najčešće instalirani i korišteni na računalima kao što su Adobe Flash, Java, Microsoft Silverlight ili Internet Explorer

- mogu se prenijeti putem spama, a kad se prenesu, iskorištavaju slabosti određenog programa nakon čega najčešće slijedi ugradnja drugog malicioznog programa namijenjenog krađi podataka

- u protekloj godini zamijećen je privremeni trend smanjenja korištenja ovakvim alatima 🡪 razlog tome je uhićenje autora trenutno **najraširenijeg exploit kita** koji se zove **Blackhole**

- kiberkriminalci su se brzo prilagodili i počeli koristiti drugim sličnim alatima

- omogućeno je implemeniranje malicioznog programa neposredno pri traženju ranjivosti sustava

**Povreda (proboj) podataka**

- pojam kojim se označava napad u kojem su podaci neovlašteno pribavljeni (kopirani) iz sustava bez znanja i odobrenja vlasnika

- **najčešće žrtve:** velike tvrke, organizacije ili državne institucije

- **ukradeni podaci:** brojevi kreditnih kartica, korisnički podaci, poslovne tajne, intelektualno vlastništvo,itd.

- povreda podataka može biti rezultat kiberkriminalnih aktivnosti (ciljanih napada), djelovanja malwareom zaraženih računala ili ljudske nepažnje ili greške

- sve češći motiv ovakvih napada je stjecanje protupravne imovinske koristi prodajom informacija

- tvrtke nastoje prikriti takve povrede, njihov razmjer i bojazan za sigurnost i privatnost klijenata, a u nekim slučajevima i zakonski propisi, tjeraju ih da o tome upozore nadležne institucije i svoje korisnike

- unatoč svim nastojanjima da se oni zaštite, niti najveće visokotehnološke tvrtke nisu imune na proboje u svoje sustave

- neki od razloga zašto dolazi do sve češće povrede podataka sadržani su izvješću ENISA i obuhvaćaju: slabe lozinke, ranjive mreže i aplikacije, maliciozne programe, phishing, nepravilnu autorizaciju korisnika, unutarnje prijetnje i greške unutar baza podataka  
  
**Materijalna šteta/krađa/gubitak**

- dolazi do fizičkog oštećenja, krađe ili gubitka uređaja

- riječ je o jednom obliku **tzv. računalne sabotaže** koja obuhvaća neovlaštene aktivnosti počinjene s namjerom da se onemogući nesmetan rad ili spriječi korištenje komunikacijskim mrežama i/ili računalnim sustavom 🡪tu spadaju brisanje, mijenjanje ili oštećivanje računalnih podataka ili programa, kao i druge aktivnosti usmjerene na podatkovnu, programsku i/ili tehničku osnovicu informacijsko-komunikacijskog sustava

- ovakve manipulacije mogu biti usmjerene na bilo koju bitnu tehničku komponentu sustava, na nesmetano odvijanje procesa obrade podataka, na razmjenu podataka putem komunikacijskih kanala ili onemogućavanje daljinskog rada

- primjer hardverske sabotaže nalazimo već u 80-im i 90-im 20.st.

- u uvjetima kad se suvremeno društvo sve više oslanja na nesmetani rad i korištenje informatičkom i komunikacijskom tehnologijom, ovaj je oblik kriminalnih aktivnosti posebno opasan jer može biti usmjeren na računala velikih informacijskih sustava gospodarskih subjekata ili državnih organizacija iinsitucija i kritičnu informacijsku strukturu

- računalnom sabotažom se bave uglavnom osobe s većim tehničkim znanjem, često koristeći se sofisticiranim sredstvima i metodama napada ili osobe koje ne prezaju ni od najopasnijih djela

- njihova su djela najčešće motivirana ideološkim stavovima ili koristoljubljem

- posebno su opasni autori malicioznih programa (računalnih virusa) jer svojom aktivnošću mogu dovesti do golemih šteta na velikom broju računalnih sustava

- do krađe ili gubitka može doći i nepažnjom ovlaštenih korisnika

**Unutarnje prijetnje**

- maliciozna unutarnja prijetnja organizacijama mogu biti sadašnji ili bivši zaposlenici, poslovni partneri koji imaju ili su imali ovlašten pristup mreži, itd.

- istraživanje provedeno na uzorku 501 organiztacije u SAD-u pokazalo je da je čak 53% ispitanika smatra da je šteta od unutarnjih napada veća od štete nastale vanjskim napadima

- **najčešći kiberincidenti odnose se na:**

**1)** nenamjerno otkrivanje privatnih ili osjetljivih podataka

**2)** krađu intelektualnog vlasništva

**3)** neovlašten pristup i/ili korištenje informacijama, sustavima ili mrežama

**4)** neovlašteno pribavljanje drugih (vlasničkih) informacija

- kod ove vrste prijetnji počinitelji ne moraju zaobilaziti postojeće sigurnosne sustave jer su oni zaposlenici ili vanjski suradnici koji su ovlašteni korisnici informacija i računalnih sustava

- sigurnosni stručnjaci preporučuju pojačanu kontrolu zaposlenika koji su promijenili uobičajeni obrazac ponašanja jer na taj način mogu lako prepoznati one pojedince koji mogu potencijalno nanijeti štetu organizaciji za koju rade

**„Curenje“ informacija**

- odnosi se na niz prijetnji koje se javljaju zbog nenamjernog ili malicioznog otkrivanja vrijednih infomacija neovlaštenim osobama

- na taj način dobivene informacije koriste se za neovlašteni pristup ili počinjenje drugih napada

- curenje je rezultat administrativnih, tehničkih i organizacijskih slabosti, a do toga može doći i korištenjem neke od metoda socijalnog inžinjeringa

- **Društveni inženjering** (Social engineering) – obuhvaća niz metoda i radnji pri čemu se iskorištava nepažnja, neznanje ili lakovjernost ovlaštenih korisnika kako bi se došlo do njihovih lozinki (**Shoulder srufing** - neposredni fizički uvid otkrivenih lozinki te **Dustbin Diving**- kopanje po tuđim bačenim ili slučajno ostavljenim bilješkama) ili drugih podataka koji mogu poslužiti za pristup sustavu

- medijski najpoznatiji hakeri najčešće se koriste metodom pokušaja i promašaja upravo zbog često loše postavljenih lozinki

- povećanje složenosti strukture internetskih mreža, kao i njegova sve veća raslojenost dovodi do jednostavnijeg pristupa određenim podacima koji nakon procesa obrade ostaju nezaštićeni

**Krađa identiteta**

- korištenje tuđim osobnim podacima (imena, identifikacijskih brojeva ili brojeva kreditnih kartica) bez dopuštenja i znanja osobe čiji su to identifikacijski podaci najčešće radi prijevare ili drugog kaznenog djela

- može se nanijeti velika financijska ili druga šteta osobi čijim se podacima koristi 🡪 istraživanje tvrtke Javelin Strategy & Research - krađom identiteta 12,7 milijuna žrtava pribavljena je protutpravna imovinska korist u iznosu od 16 milijardi dolara

- uzrok daljnjem rastu je sve više različitih metoda i alata koje kriminalci koriste ili prodaju na tržištu kako bi se domogli osobnih podataka drugih osoba

- **krađi identiteta mogu poslužiti različiti programi i metode poput:**

**a) keylogger** – program ili kombinacija programa i uređaja koji je namijenjen tajnom praćenju i snimanju pritisnutih tipki na računalu te slanju tako prikupljenih podataka prema nekom udaljenom računalu

**b) trojanac Zeus** – to čini preko financijske transakcije

**c) phising**

**d) skimming** – tehnika snimanja magnetskih zapisa s bankovnih kartica pomoću posebnih računala (skimmera) namijenjenih isključivo toj svrsi

- uređaji se spajaju na utor bankomata u koji se stavlja kartica,a pri unosu kartice, zbog nepažnje korisnika i malih dimenzija uređaja, žrtva nije niti svjesna da je došlo do takvog snimanja

- često se kombiniraju s optičkim špijuniranjem ili snimanjem putem mikrokamera pričvršćenih na bankomat kako bi došli i do PIN-a

**e) near field communication tehnologije (NFC**) – koriste se na bankovnim karticama i mobilnim telefonima za autorizaciju transakcije

**Kibernetička špijunaža**

- radnje, metode i sredstva kojima je cilj neovlašteno pribavljanje poslovnih, profesionalnih, službenih, vojnih ili državnih tajni

- u fizičkom svijetu podatke najčešće neovlašteno pribavljaju i odavaju nelojalni ili bivši zaposlenici radi stjecanja protupravne imovinske koristi ili njihova korištenja u novim tvrtkama

- radi se o iznimno važnim i vrijednim podacima od interesa za gospodarsku ili nacionalnu sigurnost te su zato česta meta napada raznih počinitelja koji njihovom prodajom žele ostvariti imovinsku korist

- „krađom“ tuđih podataka nastoji se steži prednost i ostvariti korist smanjenjem troškova koje bi imali od ulaganja u vlastiti razvoj ili se želi ostvariti prednost u odnosu na druge zemlje

- počinitelji ovakvih djela su uglavnom osobe većeg znanja s područja informatičke i telekomunikacijske tehnologije, a koriste se raznim sofisticiranim metodama i sredstvima kako bi ostvarili svoj cilj 🡪 mogu raditi po narudžbi ili na svoju ruku kako bi naknadno takve podatke ponudili na prodaju na tržištu informacija (informacijski brokeri)

- u fizičkom svijetu špijunaža podrazumijeva krađu medija na kojem se oni nalaze ili neovlašteno kopiranje i njihovo iznošenje uz zaobilaženje posotojećih mjera fizičke zaštite

- često su u pitanju profesionalci, zaposleni u poduzećima i organizacijama koje se nastoje domoći podataka ili su to plaćeni hakeri, a na raspolaganju imaju najraznovrsnija sredstva koja im omogućavaju da takva njihova aktivnost ostane neprimjećena

- posebno se koriste: optičkim promatranjem, prisluškivanjem, kompromitiranjem ovlaštenih korisnika

- poseban oblik kiberšpijunaže je **neovlašteno presretanje komunikacije**,tj. nejavnog prijenosa podataka koje podrazumijeva prikupljanje podataka koji se razmjenjuju pri komunikaciji unutar računalne mreže ili između udaljenih računala

- duže vrijeme koriste se programi koji podatke o korisničkim imenima i lozinkama kopiraju iz paketa u kojima oni putuju mrežom (tzv. **Packet Snifferi**)

- sve veća povezanost informatičke i telekomunikacijske tehnologije omogućava pružanje novih usluga, poput VoIP-a (Voice-over-IP) čime se stvara mogućnost da se zlouporabe na jednom području sve više šire i na drugo područje,pa i na mobilne aplikacije

- sve veća digitalizacija komunikacija i nove usluge pristupa širokopojasnom internetu uklanjaju razlike koje su postojale između različitih tehnologija (telefaksa, felefona, mobilnih telefona i e-pošte) što je dovelo do nastaka sustava za masovni nadzor komunikacija poput Echelona

- tehnologije bežićne komunikacije poput bežićnih mreža WLAN i Bluetootha omogućavaju komunikacijsku i razmjenu podataka između udaljenih stolnih,prijenosnih i ručnih računala, mobitela i dr.prijenosnih uređaja

- sredinom prošlog desetljeća razvoj tehnologije bežične komunikacije doveo je do novih metoda presretanja komunikacija poput **WarDrivinga ili WarWalkinga** 🡪 omogućuju da se pomoću programa (tzv.sniffera), prijenosnog računala ili PDA uređaja i posebnog adaptera, bez znanja korisnika, ostvari veza s nekom od bežičnih mreža koje se nalaze u blizini

- zaštita unutar takvih unutar takvih mreža često je nedostatna zbog čega je moguće brzo i jednostavno doći do podataka o mreži, korisnicima i njihovim lozinkama, e-pošti, itd. koji se prenose u komunikaciji

- prema izvještaju ENISA-e očekuje se nastavak rasta ovog obika prijetnje

**Ransomver/Scarver**

- grupa malicioznih programa koji su namijenjeni iznudi, reketarenju ili zastrašivanju korisnika najčešće s namjerom da se sebi ili drugom pribavi protupravna imovinska korist

- najčešće se prenose putem e-pošte ili botnetova

- aktiviranjem ovih progama može doći do blokiranja rada računala ili mobitela pri čemu se na ekranu ispisuje poruka kojom se traži uplata određenog iznosa kako bi se mogao nesmetano nastaviti rad

- može doći i do kriptiranja podataka koji se nalaze na uređaju

- često se pojavljuje slučaj u kojem se od žrtve traži da plati kaznu zbog toga što je navodno posjećivala stranice s nezakonitim ili nemoralnim sadržajem

- kod Scarvera riječ je o zastrašivanju korisnika da je njegovo računalo ili mobitel zarženo nekim malwerom zbog čega treba kupiti program koji će tu infekciju ukoniti

- izvršenju ovakvih djela pogoduje mogućnost korištenja sofisticiranim, kriptiranim načinima plaćanja otkupnine koje je gotovo nemoguće probiti (npr. Cryptolocker i Ransomscript)

**6.4. Kaznenopravni aspekti zaštite od kibernetičkog kriminala**

**-** kad su se poč. 70-ih godina pojavili prvi sudski postupci protiv počinitelja koji su za cilj imali računala bilo kao sredstvo ili objekt svojih radnji, pravni teoretičari i praktičari smatrali su da aktualno kazneno zakonodavstvo ima odgovore i na takve zloporabe u postojećim inkriminacijama

- ubrzo je sudska praska pokazala da to baš i nije lako (npr. krađa, krivotvorenje, prijevara)

- nisu postojali egzaktni podaci o štetama niti suglasnost oko toga koja bi djela taj novi oblik kriminala trebao obuhvatiti, stoga se proširila svijest da postojeće zakonodavstvo treba izmijeniti i dopuniti novim djelima radi uspješnog suzbijanja i sankcioniranja zloporaba u digitalnom okruženju

- nepostojanje jedinstvene definicije, nesuglasnost koja djela obuhvaća te različite metodologije pri prikupljanju i obradi podataka o štetama na tom području, doveli su do kašnjenja i neujednačene pravne regulacije tog područja

- rane aktivnosti međunarodnih organizacija na suzbijanju računalnog kriminala potaknule su Organizacija za ekonomsku suradnju i razvoje (OECD), Ujedinjeni narodi, Vijeće Europe, G8 i Međunarodno udruženje za kazneno pravo (AIDP)

- trebalo je gotovo 20 godina da se postigne konsenzus u pogledu toga što bi trebalo sankcionirati i koje bi nove ovlasti trebala dobiti tijela kaznenog progona radi učinkovitog suzbijanja računalnog kriminala

- 1983.g. sastavljena je **komisija OECD-a** sa zadatkom da razmotri mogućnosti međunarodne harmonizacije kaznenih zakonodavstava u borbi protiv računalnoga gospodarskog kriminaliteta

- od 1983.-1986.g. komisija provodi analizu postojećeg stanja u zemljama članicama kako bi utvrdila s kojim se problemima susreću njihova zakonodavstva kada je u pitanju računalni kriminalitet

- u rujnu 1985. komisija je predloćila da zemlje članice razmotre mjere kojima bi se poznata djela iz tog područja trebala inkriminirati nacionalnim kaznenim zakonodavstvom

- 1986.g. **izvještaj Computer-Related Crime: Analysis of Legal** **Policy** – sadrži analizu postojećeg stanja u zakonodavstvima zemalja članica te prijedloge izmjena i dopuna koje bi one trebale poduzeti radi sprječavanja i suzbijanja računalnog kriminaliteta

- prijedlog je sadržavao **minimalnu listu****zloupotreba** koje bi sve zemlje članice trebale uzeti u obzir pri dopunama i izmjenama svojih kaznenih zakona

- ta lista obuhvaća: računalnu prijevaru i krivotvorenje, mijenjanje ili brisanje računalnih programa i/ili podataka, zaštitu autorskih prava na računalnim programima i prisluškivanje komunikacija ili na drugi način ometanje rada računalnih ili telekomunikacijskih sustava

- Studija o računalnom kriminalitetu i stanju u zakonodavstvima zemalja članica (Vijeće Europe)- cilj studije je razvijanje i postavljanje smjernica za pomoć zakonodavcima u određivanju koja bi ponašanja trebalo sankcionirati i na koji način

- 1985.-1989.g. posebna komisija stručnjaka Vijeća Europe (Select Committee of Experts on Computer Related Crime of the Conucil of Europe) raspravljala je o pravnim problemima u svezi s računalnim kriminalom

-minimalna lista OECD-a proširena je dodavanjem drugih djela za koje je preporučeno da ih treba kaznenopravno regulirati

- zajedno s Europskom komisijom za probleme kriminala (Commite on Crime Problems) pripremila je **Preporuku broj R(89)9** 🡪 13. 9. 1989. usvaja ju Ministarsko vijeće Vijeća Europe

- sadrži smjernice s prijedlozima za nacionalna zakonodavstva, tako da je vladama zemalja članica preproučeno da pri izmjeni i dopuni svojih zakonodavstava uzmu u obzir smjernice za nacionalna zakonodavstva koje uključjuju minimalnu listu, za koju je postignuta opća suglasnost zemalja, kao i opcijsku (dopunsku) listu, koja sadrži popis djela već sankcioniranih u zakonodavstvima nekih zemalja

- **Minimalna lista obuhvaća:**

**1)** računalnu prijevaru

**2)** računalno krivotvorenje

**3)** oštećivanje računalnih podataka ili programa

**4)** računalnu sabotažu

**5)** neovlašten pristup

**6)** neovlašteno prisluškivanje

**7)** neovlaštenu reprodukciju zaštićenog računalnog programa

**8)** neovlaštenu reprodukciju topografije

- **Opcijska lista sadrži:**

**1)** izmjenu računalnih podataka ili programa

**2)** računalnu špijunažu

**3)** neovlašteno korištenje računalom

**4)** neovlašteno korštenje zaštićenim računalnim programom

- riječ je zapravo o preporuci koja nema obvezujući karakter stoga je situacija u nacionalnim zakonodavstvima i dalje ostala vrlo neujednačena

- ubrzo se uočilo da je jedino rješenje izrada međunarodnog ugovora kao pravnog instrumenta koji će obvezati sve države koje ga ratificiraju

- 1997.g. Vijeće Europe osnovalo je posebnu komisiju (Committee of Experts on Crime in Cyberspace PC-CY) sa zadatkom da utvrde stanje i započnu rad na međunarodnom ugovoru za borbu protiv kriminala na internetu

- komisija je pripremila **Nacrt Konvencije o kibernetičkom kriminalu** (prihvaćena 2001.g.)

- **cilj:**

**a)** usklađivanje nacinalnih zakonodavstava

**b)** propisivanje minimuma kaznenih djela koja treba sankcionirati

**c)** pružanje većih istražnih ovlasti nadležnim tijelima radi učinkovite istrage i progona počinitelja

**d)** uspostava učinkovitog sustava međunarodne suradnje i pravne pomoći

- konvencijom su obuhvaćene zemlje članice Vijeća Europe, SAD, Kanada, Japan i JAR

- predviđeno je sankcioniranje pokušaja, pomaganja i poticanja na činjenje tih djela, kaznena odgovornost pravnih osoba, rješavanje nekih kazneno procesnih pitanja koja se posebno odnose na pretragu i pribavljanje dokaza, ovlasti redarstvenih vlasti, kao i pitanja koja se odnose na nadležnost i izručenje počinitelja, te obvezu uzajamne suradnje i pomoći u otkrivanju i gonjenju počinitelja

- konvencija je značajna u odnosu na „Preporuku R(89)9“ jer je sankcionirala nova djela koja u vrijeme donošenja preporuke nisu postojala ili nisu bila aktualna

- Preporuka je zemljama članicama sugerirala da sankcioniranju samo softversko piratstvo, a Konvencijom je to prošireno i na druga autorska djela

- 2013. donesena je **Direktiva 2013/40/EU o napadima na informacijske sustave** **i o zamjeni Okvirne odluke Vijeća 2005/222/PUP**

- **razlog donošenja:** podvrgavanje napada na informacijske sustave u svim državama članicama učinkovitim, proporicionalnim i odvraćajućim kaznenopravnim sankcijama te poboljšanje i poticanje suradnje između pravosudnih i drugih nadležnih tijela

- nadovezuje se na Konvenciju Vijeća Europe o kibernetičkom kriminalu

- obuhvaća samo ona djela koja predstavljaju jezgru kiberkriminala (djela počinjena protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa i sustava)

- detaljnije su razrađene odredbe o sankcijama, njihovoj visini, otegotnim okolnostima i odgovornostima pravnih osoba za počinjenje tih djela

**6.4.1. Konvencija Vijeća Europe o kibernetičkom kriminalu**

- rad na konvenciji završen je 2001.g. kada je otvorena za potpisivanje

- do sredine 2015.g. ratificiralo ju je 47 zemalja, 7 potpisalo

- ovisno o objektu zaštite ili sredstvu počinjenja, Konvencija propisuje 4 grupe kaznenih djela:

**1)** **kaznena djela protiv tajnosti, cjelovitosti i dostupnosti računalnih podataka i sustava:**

**a)** nezakonit pristup

**b)** nezakonito presretanje

**c)** ometanje podataka

**d)** ometanje sustava

**e)** zloporaba naprava

**2)** **računalna kaznena djela:**

**a)** računalno krivotvorenje

**b)** računalna prijevara

**3) kaznena djela u svezi sa sadržajem:**

**a)** kaznena djela vezana uz dječju pornografiju

**4) kaznena djela povrede autorskih prava i srodnih prava:**

**a)** kaznena djela povrede autorskih prava i srodnih prava

- sankcioniranje navedenih djela ograničeno je samo na djela koja su počinjena s namjerom

- propisuje obvezu sankcioniranja namjernog pomaganja ili poticanja na činjenje navedenih djela, a pokušaj se ograničava na navedena djela

- sankcije nisu izričito definirane, već Konvencija propisuje da stranke moraju osigurati da kaznena djela moraju biti kažnjiva učinkovitim, srazmjernim i odgovarajućim sankcijama

- pravne osobe moraju biti podvrgnute učinkovitim, srazmjernim i odvraćajućim kaznenim ili drugim sankcijama ili mjerama

**O pojmovima**

- pojmovi koji se koriste u Konvenciji definirani su u čl.1. Konvencije – njihova općenitost opravdana je obrazloženjem da oni trebaju bit formulirani tehnološki neutralno kako bi se unaprijed obuhvatilo i nove tehnologije i tehnička otkrića

- naš Kazneni zakon preuzeo je i definirao temeljne pojmove kako je to učinjeno Konvencijom , osim pojma računalnog sustava koji je preuzet iz Direktive

- prema čl.87.st.18. KZ-a računalni sustav je svaka naprava ili skupina međusobno spojenih ili povezanih naprava,od kojih 1 ili više njih na osnovi programa automatski obrađuje podatke kao i računalni podaci koji su u njega spremljeni,obrađeni,učitani ili preneseni za svrhe mkegovog rada,korištenja,zaštite i održavanja

- u Konvenciji i Direktivi **pojmom računalnog podatka** obuhvaćen je i računalni program, za razliku od našeg KZ-a koji računalni program zasebno definira

- **računalni program** je skup računalnih podataka koji su u stanju prouzročiti da računalni sustav izvrši određenu funkciju

- **pojam dječje pornografije** preuzet je iz Konvencije koja je definira u čl.9 st.2. kao „materijal koji vizualno ili na drugi način prikazuje pravo dijete ili realno prikazano nepostojeće dijete ili osobu koja izgleda kao dijete , u pravom ili simuliranom spolno eksplicitnom ponašanju ili koji prikazuje spolne organe djece u spolne svrhe“ ( materijali koji imaju umjetnički, medicinski ili znanstveni značaj ne smatraju se pornografijom u smislu ovog članka)

- **pojam računalne mreže** nije posebno definiran jer je već dugo uvriježen u jeziku

**6.4.2 Implementacija Konvencije o kibernetičkom kriminalu u kaznenom zakonodavstvu RH**

- nakon potpisivanja 2001. i zatim ratifikacije Konvencije u Saboru RH 2002.g. uslijedila je njezina implemetacija u tadašnjem KZ-u iz 1997.g.

- daljnje promjene uslijedile su donošenjem novog Kaznenog zakona 2011. koji je stupio na snagu 1.1.2013.

- pri implementaciji navedenih djela iz Konvencije u naše zakonodavsvo prema trenutno važećem KZ samo su djela iz prve i druge grupe izdvojena u zasebnu glavu XXV KZ-a , dok je kazneno djelo u vezi s dječjom pornografijom propisano u glavi XII pri čemu je to učinjeno u daleko širem opsegu nego što to predviđa Konvencija

- kaznena djela povrede autorskih i srodnih prava propisana su zasebno u glavi XXVII KZ-a u širem opsegu pružajući zaštitu i moralnim pravima autora

**Neovlašten pristup (čl.266.)**

(1) Tko neovlašteno pristupi računalnom sustavu ili računalnim podacima,kaznit će se kaznom zatvora do 2 godine.

(2) Tko kazneno djelo iz stavka 1.ovoga članka počini u odnosu na računalni sustav ili računalne podatke tijela državne vlasti, Ustavnog suda RH ili međunarodne organizacije koje je RH član,tijela jedinica lokalne ili područne samouprave,javne ustanove ili trgovačkog društva od posebnog javnog interesa,kaznit će se kaznom zatvora do 3 godine.

(3) Za pokušaj kaznenog djela iz stavka 1. i 2. ovog članka počinitelj će se kazniti.

(4) Kazneno djelo iz stavka 1. ovog članka progoni se po prijedlogu.

- cilj je ovog djela zaštititi integritet računalnog sustava i podataka od tzv. **hakinga** omogućavajući korisnicima učinkovito upravlajuju, koriste se njegovim radom i nadziru ga

- razlog uvođenja ovog djela je u tome što se pravna zaštita nije mogla osigurati tradicionalnim kaznenim propisima zbog prirode samog pristupa koji najčešće nema fizički karakter, pa je stoga i granicu tog pristupa kao i vrijeme kad je on počinjen daleko teže utvrditi i dokazati

- naš zakon ne pravi razliku je li se računalnom sustavu ili podacima pristupilo daljinski ili neposrednim fizičkim pristupom

- prva država koja je inkriminirala nezakonit pristup tuđim sustavima/podacima je Švedska 1973.g. , njezin primjer slijedile su druge zemlje, ali pristup je bio neujednačen

- Konvencija predviđa rezerve i ograničenja ovog djela( čl.2.) propisujući da stranke mogu uvjetovati izvršenje ovog djela ako je počinjeno povredom sigurnosnih mjera s namjerom pribavljanja računalnih podataka ili nekom drugom nepoštenom namjerom ili u pogledu računalnog sustava koji je spojen s drugim računalnim sustavom

- važeći Kazneni zakon ( za razliku od prethodnog zakona gdje je to uvjetovano postojanjem zaštitnih mjera) nema takvih ograničenja , već kažnjava svaki neovlašteni pristup

- kažnjiv je samo neovlašeni i namjerni pristup, a obuhvaćeni su i oni slučajevi kada se neovlašteno pristupi računalnim podacima pohranjenim na nekom mediju za pohranu podataka

**Ometanje rada računalnog sustava (čl.267.)**

(1) Tko onemogući ili oteža rad ili korištenje računalnog sustava,računalnih podataka ili programa ili računalnu komunikaciju,kaznit će se kaznom zatvora do 3 godine.

(2) Za pokušaj kaznenog djela iz stavka 1. ovog članka počinitelj će se kazniti.

- ometanje rada računalnog sustava jedan je od oblika računalne sabotaže usmjeren na sprječavanje ili otežavanje dostupnosti računalnog sustava , podataka ili programa koji su unutar njega pohranjeni ili usluga koje se putem njega nude

- najčešći cilj takvih radnji je da se ovlaštenim korisnicima onemogući ili oteža korištenje, odnosno komunikacija putem nekog računalnog sustava koji koriste za pristup internetu ili digitalnim sadržajima i uslugama koje se na njmu ili putem njega nude

- prema Konvenciji se ometanje provodi unošenjem,prenošenjem,oštećivanjem, brisanjem, mijenjanjem ili činjenjem neuporabljivima računalnih podataka

- naš KZ ne navodi radnje kojima se čini ovo djelo niti upućuje na to što bi se smatralo činom „ozbiljnog ometanja“ poput nanošenja veće štete prenošenjem malicioznih programa koji usporavaju rad sustava ili slanja velike količine podataka (npr. dDos napadi)

- kvalificirani oblik ovog djela je predviđen u čl.273. kada je djelo počinjeno:

**a)** u odnosu na računalni sustav ili računalne podatke tijela državne vlasti, Ustavnog suda RH i međunarodne organizacije koje je RH član,tijela jedinica lokalne ili područne(regionalne) samouprave, javne ustanove ili trgovačkog društva od posebnog javnog interesa

**b)** prikrivajući stvarni identitet i uzrokujući zabludu o ovlaštenom nositelju identiteta

**c)** sredstvom namijenjenim za izvršenje napada na veći broj računalnih sustava ili kojim je prouzročena znatna šteta (npr. botnetom ili dDos napadom)

- ovo djelo može biti počinjeno samo s namjerom i neovlašteno ( neovlaštenim se **ne** smatra poduzimanje radnji radi provjere sigurnosti ili implementacije mjera sigurnosti uz odobrenje ovlaštenje osobe)

**Oštećenje računalnih podataka (čl.268 )**

(1) Tko neovlašteno u cijelosti ili djelomično ošteti,izmijeni,izbriše,uništi,učini neuporabljivim ili nedostupnim tuđe računalne podatke ili programe,kaznit će se kaznom zatvora do 3 godine.

(2) Za pokušaj kaznenog djela iz stavka 1.ovog članka počinitelj će se kazniti.

- oštećivanje računalnih podataka ili programa jedan je od najtežih oblika računalne sabotaže, pogotovo u informacijskom društvu kojem su temeljni resursi informacije

- razlog uvođenja ovog kaz. djela je nemogućnost postojećih zakonodavstava da odgovore na oštećenje netjesnih stvari kao što su računalni podaci i programi

- cilj ovog djela je pružiti računalnim podacima i programima isti stupanj zaštite kao tjelesnim objektima i zaštititi njihov integritet i dostupnost

- ovim djelom su posebno inkriminirane neovlaštene i namjerne radnje ovlaštenih korisnika ili drugih osoba koje daljinski ili neposredno fizički pristupe sustavu, kao i djelovanja počinitelja koji izrađuju i distribuiraju maliciozne prograne čijom aktivacijom dođe do oštećenja,izmjene,brisanja,uništenja,činjenja neuporabljivim ili nedostupnim tuđih podataka ili programa

- odgovorne su osobe koje to učine s namjerom i neovlašteno

- kaznenu odgovornost ne snose osobe koje su ovlaštene pristupiti podacima i programima , ali ih slučajno ili greškom oštete, unište ili učine neupotrebljivim pri obavljanju svojih poslova

- viša kazna predviđena je u čl.273 ( a), b) i c) isto kao u ranijem primjeru )

**Neovlašteno presretanje računalnih podataka (čl.269 )**

(1) Tko neovlašteno presretne ili snimi nejavni prijenos računalnih podataka,uključujući i elektromagnetsku emisiju računalnog sustava ili drugome učini dostupnim tako pribavljene podatke,kaznit će se kaznom zatvora do 3 godine

(2) Za pokušaj kaznenog djela iz stavka 1. ovog članka počinitelj će se kazniti

(3) Podaci koji su nastali počinjenjem kaznenog djela iz st.1. ovog članka će se uništiti

- jedan od oblika računalne špijunaže čiji je cilj očuvati tajnost komunikacije

- odnosi se na sve oblike elektroničke komunikacije, neovisno o tome odvija li se telefonom, telefaks uređajem, elektroničkom poštom ili prijenosom datoteka

- prema Konvenciji neovlašteno presretanje se odnosi na nejavni prijenos računalnih podataka prema računalnom sustavu, iz njega ili unutar njega, a obuhvaćeno je i presretanje elektromagnetske emisije računalnog sustava jer su uz pomoć odgovarajućih uređaja i program može rekonstruirati sadržaj

- ako nije riječ o podacima koji već uživaju kaznenopravnu zaštitu poput osobnih podataka ili poslovnih , službenih ili drugih tajnih podataka , neovlašteno pribavljanje takvih podataka neće bit objekt zaštite

- kvalificirani oblik djela je predviđen u čl.273. ( a), b) i c) isto kao u ranijem primjeru )

- u odnosu na subjektivnu stranu, ovo djelo može biti učinjeno samo s namjerom i ako je neovlašteno

- ne odnosi se na primjere kada presretanje poduzimaju osobe koje su na to ovlaštene od sudionika komunikacije ili čije ovlaštenje proizlazi iz zakona, kao npr. obavještajne službe radi nacionalne sigurnosti ili redarstvene vlasti kada je riječ o posebnim istražnim radnjama pod uvjetom da je presretanje poduzeto u skladu sa zakonom

**Zloporaba naprava (čl. 272.)**

(1) Tko izradi, nabavi,uveze, proda, posjeduje ili čini drugome dostupne uređaje ili računalne programe ili računalne podatke stvorene ili prilagođene za počinjenje kaznenih djela iz [čl. 266.- 271.[tt](javascript:fold(this,'1');)](javascript:fold(this,'1');) ovoga Zakona s ciljem da ih se uporabi za počinjenje nekog od tih djela, kaznit će se kaznom zatvora do tri godine.

(2) Tko izradi, nabavi,uveze, proda, posjeduje ili čini drugome dostupne računalne lozinke, pristupne šifre ili druge podatke kojima se može pristupiti računalnom sustavu s ciljem da ih se uporabi za počinjenje kaznenih djela iz čl. 266.- [271. ovoga Zakona[tt](javascript:fold(this,'21',['21_1'],[':hr:zakon:kazneni-zakon:include:271-clanak-racunalna-prijevara']);)](javascript:fold(this,'21',['21_1'],[':hr:zakon:kazneni-zakon:include:271-clanak-racunalna-prijevara']);), kaznit će se kaznom zatvora do jedne godine.

**(3)** Počinitelj kaznenog djela iz [stavka 1. ovoga članka [tt](javascript:fold(this,'22');)](javascript:fold(this,'22');) neće se kazniti kaznom strožom od one koja je propisana za kazneno djelo koje je počinitelj imao za cilj.

**(4)** Posebne naprave, programi iz [stavka 1. ovoga članka [tt](javascript:fold(this,'29',['29_1'],[':hr:zakon:kazneni-zakon:include:272-clanak-1-stavak']);)](javascript:fold(this,'29',['29_1'],[':hr:zakon:kazneni-zakon:include:272-clanak-1-stavak']);) će se oduzeti, a podaci iz [stavka 1. i 2. ovoga članka [tt](javascript:fold(this,'30',['30_1'],[':hr:zakon:kazneni-zakon:include:272-clanak-1-stavak']);)](javascript:fold(this,'30',['30_1'],[':hr:zakon:kazneni-zakon:include:272-clanak-1-stavak']);) će se uništiti.

- jedno od temeljnih obilježja kiberkriminala je velika rasprostranjenost i široka dostupnost različitih naprava koje mogu poslužiti ili olakšati počinjenje nekog od kaznenih djela navedenih u glavi XII KZ-a

- pojam naprava široko je definiran i sukladno Konvenciji obuhvaća:

**a)** uređaje, računalne programe i računalne podatke

**b)** lozinke, pristupne šifre ili druge podatke za neovlašten pristup računalnom sustavu

- sve te naprave dostupne u putem različitih internetskih servisa , a upute o tome kako činiti ta djela nalazimo na hakerskim web- stranicama, forumima, tematskim skupinama ali i na legalnim izvorima poput youtube ili drugim videoservisima

- pri odlučivanju može li se neki uređaj ili program smatrati takvom napravom odlučuju dva elementa :

**1)** da je riječ o napravi stvorenoj ili prilagođenoj za činjenje nekog od prethodnih kaznenih djela, što isključuje naprave koje redovito koristimo u radu npr.računala ili skenera

**2)** subjektivni element, tj. namjera da ih se uporabi za počinjenje nekog od prethodno opisanih djela

- ako su oba elementa ispunjena kaznit će se onaj koji izradi, nabavi, proda, posjeduje ili čini druge dostupne takve naprave

- kazniti se može samo netko tko makar pokuša počiniti neko djelo

- u odnosu na Konvenciju , nas KZ je predvidio pojam distribucije takvih naprava

- **distribucija** se odnosi na slanje takvih naprava drugima, dok se **činjenje dostupnim** odnosi na online dostupnost putem internetskih servisa i poveznica koji omogućavaju pristup takvim napravama

- u našem KZ-u zlouporaba naprava ( u odnosu na Konvenciju) ima širi obuhvat , tako se odnosi i na naprave kojim se koristi za počinjenje računalnog krivotvorenja i računalne prijavare

- što se tiče subjektivne strane, ovo djelo može biti počinjeno samo s namjerom da se naprava uporabi za počinjenje kaznenih djela navedena u KZ

- kaznene odgovornosti neće biti ako se radnje izrade,nabave,prodaje,posjedovanja ili činjenja drugima dostupnim ovakve naprave nije u svrhu počinjenja kaznenog djela kada se to čini radi provjere sigurnosti ili zaštite računalnog sustava

**Računalno krivotvorenje ( čl.270 )**

(1) Tko neovlašteno izradi, unese, izmijeni, izbriše ili učini neuporabljivim ili nedostupnim računalne podatke koji imaju vrijednost za pravne odnose, u namjeri da se oni uporabe kao vjerodostojni, ili tko takve podatke uporabi ili nabavi radi uporabe, kaznit će se kaznom zatvora do tri godine.

(2)Za pokušaj kaznenog djela iz [stavka 1. ovoga članka [tt](javascript:fold(this,'1');)](javascript:fold(this,'1');) počinitelj će se kazniti.

(3)Podaci koji su nastali počinjenjem kaznenog djela iz [stavka 1. ovoga članka [tt](javascript:fold(this,'2',['2_1'],[':hr:zakon:kazneni-zakon:include:270-clanak-1-stavak']);)](javascript:fold(this,'2',['2_1'],[':hr:zakon:kazneni-zakon:include:270-clanak-1-stavak']);) će se uništiti.

- razlog uvođenja ovog kaznenog djela je popunjavanje pravnih praznina u odnosu na tradicionalno djelo krivotvorenja koje se odnosi na vizualno čitljive dokumente, odnosno dokumente koje je moguće iščitati bez tehničke pomoći

- ovisno o radnji počinitelja treba razlikovati **tri slučaja :**

**1)** kreiranje krivotvorenoga digitalnog dokumanta ( izrada i unos )

**2)** falsificiranje postojećega originalnog digitalnog dokumenta ( izmjena)

**3)** onemogućavanje korištenja originalnim digitalnim dokumentom

- zaštićeni objekt je računalni podatak koji ima vrijednost za pravne odnose , odnosno njegova vjerodostajnost i funkcionalnost, pa je zbog toga cilj zaštititi cjelobitost, dostupnost i autentičnost podataka,ali samo pod uvjetom da oni imaju vrijednost za pravne odnose,tj. da njihova uporaba ima ili može imati pravne učinke

- u pogledu subjektivnog elementa, počinitelj mora djelovati s namjerom

- Konvencija (za razliku od KZ-a) sadrži i mogućnost rezerve te omogućava strankama da kaznenu odgovornost propišu samo za počinitelje koji postupaju s prijevarnom ili sličnom namjenom

**Računalna prijevara (čl.271.)**

(1) Tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, izmijeni, izbriše, ošteti, učini neuporabljivim ili nedostupnim računalne podatke ili ometa rad računalnog sustava i na taj način prouzroči štetu drugome, kaznit će se kaznom zatvora od šest mjeseci do pet godina.

(2)Ako je kaznenim djelom iz [stavka 1. ovoga članka [tt](javascript:fold(this,'1');)](javascript:fold(this,'1');) pribavljena znatna imovinska korist ili prouzročena znatna šteta, počinitelj će se kazniti kaznom zatvora od jedne do osam godina.

(3)Podaci koji su nastali počinjenjem kaznenog djela iz [stavka 1. i 2. ovoga članka [tt](javascript:fold(this,'2',['2_1'],[':hr:zakon:kazneni-zakon:include:271-clanak-1-stavak']);)](javascript:fold(this,'2',['2_1'],[':hr:zakon:kazneni-zakon:include:271-clanak-1-stavak']);) će se uništiti.

- računalna prijevara obuhvaća najraznovrsnije oblike prijevara u kiberprostoru i danas je jedna od najčešćih zloporaba na internetu

- razlog za uvođenje ovog djela u KZ je popunjavanje pravnih praznina u odnosu na tradicionalno djelo prijavare

- razlika je u objektu napada jer tradicionalna prijevara podrazumijeva prijevaru neke osobe, odnosno njezino dovođenje u zabludu

- budući da se računalna prijevara nejčešće čini putem računalnih sustava i programa taj subjektivni odnos između žrtve i počinitelja nije prisutan, a počinitelj može programski izvesti djelo računalne prijevare prema većem broju potencijalnih žrtava , a da sam nije prisutan niti se u tom času koristi računalom

- ono što ovo djelo razlikuje od kaznenih djela oštećenja podataka ili ometanja rada računalnih sustava nisu radnje počinitelja, nego subjektivni element , tj. njegova namjera da sebi ili drugome pribavi protupravnu imovinsku korist

- dodatni element koji mora biti ispunjen je šteta koja je time prouzročena drugome

**Iskorištavnje djece za pornografiju ( čl.163) i druga djela u vezi s dječjom pornografijom**

(1)

- kaznena djela u vezi s dječjom pornografijom iz Konvencije obuhvaćena su , pa i daleko šire opisna u kaznenom djelu **Iskorištavanja djece za pornografiju**

- naš KZ sankcionira i svjestan pristup dječjoj pornografiji putem informacijsko- komunikacijskih tehnologija, a kako pristup takvim saržajima može bit slučajan ili učinjen preko poveznice koja je upućivala na drugačiji sadržaj , u praksi će biti teško dokazati da je netko to učinio svjesno

- Konvencija Vijeća Europe o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja definira **dječju pornograafiju** znatno uže od Konvencije i našeg KZ-a : „materijal koji vizualno ili na drugi način prikazuje pravo dijete ili realno prikazano nepostojeće dijete ili osobu koja izgleda kao dijete, u pravom ili simuliranom spolno eksplicitnom ponašanju ili koji prikazuje spolne organe djece u spolne svrhe“

- Konvencija Vijeća Europe o zaštiti djece od seksualnog iskorištavanja i seksualnog zlostavljanja definira dječju pornografiju kao „materijal koji vizualno prikazuje dijete koje sudjeluje u stavrnoj ili simuliranoj seksualno eksplicitnoj aktivnosti ili bilo koji prikaz spolnih organa djeteta u primarno seksualne svrhe“

- u našeg KZ-u sankcionirano je upoznavanje djece s pornografijom(čl. 165) koji propisuje kaznu zatvora do tri godine za onog tko posredstvom računalnog ustava , mreže ili medija za pohranu računalnih podataka ili na drugi način učini pristupačnim slike, spise, audio sadržaje i druge predmete pornografskog sadržaja ili mu pokaže pornografsku predstavu

- sve češći oblik nezakonitog ponašanja u virtualnom svijetu je **kibernasilje i kiberuhođenje**:

**a) Kibernasilje-** svaki oblik komunikacije putem inf.-komunik. tehnologija kojim se vrši nasilje i zlostavljanje djece ( zadiranje u privatnost, poticanje grupne mržnje, uhođenje, uznemiravanje itd.)

**-** kazneno zakonodavstvo se ne primjenjuje prema djetetu koje u vrijeme počinjenja djela nije navršilo 14 godina

**b) Kiberuhođenje** – učestalo korištenje elektroničkim komunikacijama , poput internetskih servisa i mobilnih aplikacija, radi uznemiravanja ili zastrašivanja neke osobe (vrijeđenje, slanje prijetećih i uznemiravajućih poruka ili zastrašivanja)

- djelo se progoni po prijedlogu osim ako je počinjeno prema djetetu

**Javno poticanje na nasilje i mržnju ( čl.325.)**

(1) Tko putem tiska, radija, televizije, računalnog sustava ili mreže, na javnom skupu ili na drugi način javno potiče ili javnosti učini dostupnim letke, slike ili druge materijale kojima se poziva na nasilje ili mržnju usmjerenu prema skupini ljudi ili pripadniku skupine zbog njihove rasne, vjerske, nacionalne ili etničke pripadnosti, podrijetla, boje kože, spola, spolnog opredjeljenja, rodnog identiteta, invaliditeta ili kakvih drugih osobina,kaznit će se kaznom zatvora do tri godine.

(2) Tko organizira ili vodi grupu od 3 ili više osoba radi počinjenja djela iz st.1.ovog članka, kaznit će se kaznom zatvora od 6 mjeseci do 5 godina.

(3) Tko sudjeluje u udruženju iz st.1. ovog članka, kaznit će se kaznom zatvora do 1 godine.

(4) Kaznom iz [stavka 1. ovoga članka [tt](javascript:fold(this,'1');)](javascript:fold(this,'1');) kaznit će se tko javno odobrava, poriče ili znatno umanjuje kazneno djelo genocida, zločina agresije, zločina protiv čovječnosti ili ratnog zločina, usmjereno prema skupini ljudi ili pripadniku skupine zbog njihove rasne, vjerske, nacionalne ili etničke pripadnosti, podrijetla ili boje kože, na način koji je prikladan potaknuti nasilje ili mržnju protiv takve skupine ili pripadnika te skupine.

(5) Za pokušaj kaznenog djela iz [stavka 1. i 4. ovoga članka [tt](javascript:fold(this,'2',['2_1'],[':hr:zakon:kazneni-zakon:include:325-clanak-1-stavak']);)](javascript:fold(this,'2',['2_1'],[':hr:zakon:kazneni-zakon:include:325-clanak-1-stavak']);) počinitelj će se kazniti.

- kao bi se lista djela proširila i na druge nemoralne sadržaje 2003.g. donesen je Dodatni protokol uz Konvenciju o kiberkriminalu koji se odnosi na kriminalizaciju djela rasističke i ksenofobične prirode koja su počinjena pomoću računalnih sustava

- Dodatnim protokolom se proširuje lista kaznenih djela iz Konvencije, inkriminira se pomaganje i poticanje te se propisuju mjere koje se moraju poduzeti na nacionalnoj razini

- RH je Dodatni protokol potpisala 2003. i ratificirala 2008. godine kada je donesen Zakon o potvrđivanju Dodatnog protokola uz Konvenciju o kiberkriminalu koji je na snagu stupio 21.6.2008.

- kvalificirani oblik kaznenog djela javnog poticanja na nasilje mržnju predviđena je za onog tko :

**a)** organizira ili vodi grupu od tri ili više osoba radi počinjenja tog djela

**b)** sudjeluje u takvom udruženju

**Nedozvoljenja upotreba autorskog djela ili izvedbe umjetnika izvođača (čl. 285.)**

(1) Tko protivno propisima kojima se uređuju autorsko i srodna prava reproducira, preradi, distribuira, skladišti ili poduzima druge radnje radi distribucije ili priopći javnosti na bilo koji način tuđe autorsko djelo ili dopusti da se to učini i na taj način pribavi imovinsku korist ili prouzroči štetu, kaznit će se kaznom zatvora do tri godine.

(2) Kaznom iz [stavka 1. ovoga članka [tt](javascript:fold(this,'1');)](javascript:fold(this,'1');) kaznit će se tko protivno propisima kojima se uređuje autorsko i srodna prava fiksira tuđu nefiksiranu izvedbu umjetnika izvođača, reproducira, preradi, distribuira, skladišti ili poduzima druge radnje radi distribucije tuđe fiksirane izvedbe umjetnika izvođača ili priopći javnosti na bilo koji način tuđu fiksiranu ili nefiksiranu izvedbu umjetnika izvođača ili dopusti da se to učini i na taj način pribavi znatnu imovinsku korist ili prouzroči znatnu štetu.

(3) Kaznom iz [stavka 1. ovoga članka [tt](javascript:fold(this,'2',['2_1'],[':hr:zakon:kazneni-zakon:include:285-clanak-1-stavak']);)](javascript:fold(this,'2',['2_1'],[':hr:zakon:kazneni-zakon:include:285-clanak-1-stavak']);) kaznit će se tko protivno propisima kojima se uređuju autorsko i srodna prava osujećuje tehničke mjere za zaštitu prava autora i umjetnika izvođača ili ukloni ili preinači podatke o upravljanju tim pravima i na taj način pribavi znatnu imovinsku korist ili prouzroči znatnu štetu.

(4) Za pokušaj kaznenog djela iz [stavka 1., 2. i 3. ovoga članka [tt](javascript:fold(this,'3',['3_1'],[':hr:zakon:kazneni-zakon:include:285-clanak-1-stavak']);)](javascript:fold(this,'3',['3_1'],[':hr:zakon:kazneni-zakon:include:285-clanak-1-stavak']);) počinitelj će se kazniti.

(5) Predmeti koji su bili namijenjeni ili uporabljeni za počinjenje kaznenog djela iz [stavka 1., 2., 3. i 4. ovoga članka [tt](javascript:fold(this,'6',['6_1','6_2','6_3'],[':hr:zakon:kazneni-zakon:include:285-clanak-1-stavak',':hr:zakon:kazneni-zakon:include:285-clanak-2-stavak',':hr:zakon:kazneni-zakon:include:285-clanak-3-stavak']);)](javascript:fold(this,'6',['6_1','6_2','6_3'],[':hr:zakon:kazneni-zakon:include:285-clanak-1-stavak',':hr:zakon:kazneni-zakon:include:285-clanak-2-stavak',':hr:zakon:kazneni-zakon:include:285-clanak-3-stavak']);) će se oduzeti, a predmeti koji su nastali počinjenjem tih kaznenih djela će se uništiti osim ako onaj čije je pravo povrijeđeno zatraži njihovu predaju uz naknadu koja ne može biti viša od troškova njihove proizvodnje. Naknada je prihod državnog proračuna i koristit će se za suzbijanje kaznenih djela protiv intelektualnog vlasništva.

**Povreda drugih autorskom pravu srodnih prava (čl.286.)**

(1) Tko protivno propisima kojima se uređuju autorsko i srodna prava reproducira, distribuira, skladišti ili poduzima druge radnje radi distribucije, ili stavi na raspolaganje javnosti tuđi fonogram ili dopusti da se to učini i na taj način pribavi znatnu imovinsku korist ili prouzroči znatnu štetu, kaznit će se kaznom zatvora do jedne godine.

(2) Kaznom iz [stavka 1. ovoga članka [tt](javascript:fold(this,'1');)](javascript:fold(this,'1');) kaznit će se tko protivno propisima kojima se uređuju autorsko i srodna prava reproducira, distribuira, skladišti ili poduzima druge radnje radi distribucije, ili javno prikaže ili stavi na raspolaganje javnosti tuđi videogram ili dopusti da se to učini i na taj način pribavi znatnu imovinsku korist ili prouzroči znatnu štetu.

(3) Kaznom iz [stavka 1. ovoga članka [tt](javascript:fold(this,'2',['2_1'],[':hr:zakon:kazneni-zakon:include:286-clanak-1-stavak']);)](javascript:fold(this,'2',['2_1'],[':hr:zakon:kazneni-zakon:include:286-clanak-1-stavak']);) kaznit će se tko protivno propisima kojima se uređuju autorsko i srodna prava reemitira tuđe emitiranje, ili javno priopći tuđe emitiranje uz plaćanje ulaznica ili stavi na raspolaganje javnosti tuđe emitiranje ili dopusti da se to učini i na taj način pribavi znatnu imovinsku korist ili prouzroči znatnu štetu.

(4) Kaznom iz [stavka 1. ovoga članka [tt](javascript:fold(this,'3',['3_1'],[':hr:zakon:kazneni-zakon:include:286-clanak-1-stavak']);)](javascript:fold(this,'3',['3_1'],[':hr:zakon:kazneni-zakon:include:286-clanak-1-stavak']);) kaznit će se tko protivno propisima kojima se uređuju autorsko i srodna prava osujećuje tehničke mjere za zaštitu srodnih prava proizvođača fonograma, videograma ili organizacija za radiodifuziju ili ukloni ili preinači podatke o upravljanju tim pravima ili dopusti da se to učini i na taj način pribavi znatnu imovinsku korist ili prouzroči znatnu štetu.

(5) Za pokušaj kaznenog djela iz [stavka 1. do 4. ovoga članka [tt](javascript:fold(this,'4',['4_1'],[':hr:zakon:kazneni-zakon:include:286-clanak-1-stavak']);)](javascript:fold(this,'4',['4_1'],[':hr:zakon:kazneni-zakon:include:286-clanak-1-stavak']);) počinitelj će se kazniti.

(6) Predmeti koji su bili namijenjeni ili uporabljeni za počinjenje kaznenog djela iz [stavka 1., 2., 3. i 4. ovoga članka [tt](javascript:fold(this,'8',['8_1','8_2','8_3','8_4'],[':hr:zakon:kazneni-zakon:include:286-clanak-1-stavak',':hr:zakon:kazneni-zakon:include:286-clanak-2-stavak',':hr:zakon:kazneni-zakon:include:286-clanak-3-stavak',':hr:zakon:kazneni-zakon:include:286-clanak-4-stavak']);)](javascript:fold(this,'8',['8_1','8_2','8_3','8_4'],[':hr:zakon:kazneni-zakon:include:286-clanak-1-stavak',':hr:zakon:kazneni-zakon:include:286-clanak-2-stavak',':hr:zakon:kazneni-zakon:include:286-clanak-3-stavak',':hr:zakon:kazneni-zakon:include:286-clanak-4-stavak']);) će se oduzeti, a predmeti koji su nastali počinjenjem tih kaznenih djela će se uništiti osim ako onaj čije je pravo povrijeđeno zatraži njihovu predaju uz naknadu koja ne može biti viša od troškova njihove proizvodnje. Naknada je prihod državnog proračuna i koristit će se za suzbijanje kaznenih djela protiv intelektualnog vlasništva.

- problem piratstva datira još od poč. 80-ih g. kada se na komercijalnoj osnovi počinje nuditi server

- digitalizacijom i pojavom novih formata ubrzo se prenosi i na područje audio i audiovizualnih sadržaja te književnih djela u digitalnom obliku

- nastojanja da se takve negativne pojave suzbiju, a zakonodavstvo na tom području uskladi putem Konvencije o kibernetičkom kriminalu, nisu dala očekivane rezultate

- Konvencijom je kaznenopravna odgovornost ograničena samo na radnje koje su poduzete s namjerom,u komercijalnim razmjerima i pomoću računalnog sustava,a ne odnosi se na moralna prava

- u našem zakonodavstvu zaštita autorskog prava i srodnih prava pruža se **Zakonom o zaštiti autorskog prava i srodnih prava**, koji sadrži prekršajne odredbe , dok je Kaznenim zakonom sankcionirana Nedozvoljena uporaba autorskog djela ili izvedbe umjetnika izvođača i povreda drugih autorskom pravu srodnih prava

- zbog moguće kolizije kaznenih i prekršajnih odredbi , kaznena odgovornost je ograničena samo na slučajeve namjernog pribavljanja znatne imovinske koristi , odnosno nanošenja znatne imovinske štete,a njihovu visinu određuje Kazneni odjel Vrhovnog suda

- KZ jamči i zaštitu moralnim prava autora te sankcionira i osujećiva tehničke mjere zaštite i uklanja ili preinačava podatke o upravljanju tim pravima pod uvijetom da je time pribavljena znatna imovinska korist ili prouzročena znatna šteta

**Zajedničke odredbe**

- za sva kaznena djela protiv računalnih sustava , podataka i programa , progon se provodi po službenoj dužnosti , osim za kazneno djelo neovlaštenog pristupa za koje se kazneni postupak provodi samo na prijedlog oštećenika

- počinitelji tih kaznenih djela kažnjavaju se samo ako ih počine s namjerom, a kažnjivo je također poticanje na činjenje ili pomaganje u činjenju tih djela

- kod svih djela kažnjiv je i pokušaj, osim za zloporabu naprava

- sukladno Konvenciji i Direktivi za sva djela predviđena je kaznena odgovornost pravnih osoba, odnosno odgovornih osoba u njima, prema odredbama važećeg **Zakona o odgovornosti pravnih osoba za kaznena djela**

- sud počinitelju može izreći sigurnosnu mjeru **Zabrane pristupa internetu** ako postoji opasnost da će zlouporabom interneta ponovno počiniti kazneno djelo

- danas, u vrijeme kada se o pravu na pristup internetu sve više govori kao temeljnom pravu čovjeka, a većina poslova, u većoj ili manjoj mjeri, istiskuje korištenje informacijskom i komunikacijskom tehnologijom, takvom se zabranom osobi najčešće onemogućava zapošljavnje, a time i ugrožava njezina egzistencija

**6.4.3. Kazneno procesne odredbe Konvencije o kibernetičkom kriminalu**

- osim kazneno materijalnih odredbi, Konvencija o kiberkrimalu sadrži i odredbe koje se odnose na kazneno procesne mjere i ovlasti koje se provode radi učinkovitog otkrivanja i kaznenog progona počinitelja kiberkriminala

- **odredbe** o tome sadržane su čl. 15.-21. Konvencije, a odnose se na inplementaciju 6 mjera, a to su:

* + Hitna zaštita pohranjenih računalnih podataka
  + Hitna zaštita i djelomično otkrivanje podataka o prometu
  + Nalog za predaju, odnosno dostavu podataka
  + Pretraga i oduzimanje pohranjenih računalnih podataka
  + Prikupljanje računalnih podataka u realnom vremenu
  + Presretanje podataka o sadržaju

**Hitna zaštita pohranjenih računalnih podataka**

- u slučajima kiberkriminala, podaci nužni za otkrivanje i progon počinitelja najčešće se nalaze u digitalnom obliku,tj. u obliku računalnih podataka

- takvi podaci su u velikoj mjeri podložni promjenama i mogućem uništenju

- u **čl. 16. Konvencije** propisana je mjera hitne zaštite pohranjenih računalnih podataka

- svaka članica dužna je usvojiti zakonske i druge mjere koje su potrebne kako bi njena nadležna tjela mogla naložiti ili na drugi način postići hitnu zaštitu određenih računalnih podataka

- hitna zaštita podataka ostvaruje se tako da nadležno državno tijelo izda osobi koja posjeduje ili kontrolira podatke **nalog** kojem tu osobu obveže da računalne podatke koji su predmet naloga zaštiti i sačuva njihovu cjelovitost na vrijeme koje je nužno, ali najviše 90 dana od dana izdavanja naloga

- Konvencija predviđa i mogućnost da države članice usvoje zakonske i druge mjere koje su potrebne da bi se osobu kojoj je izdan nalog za pohranu podataka obvezalo i da postupke koji su joj naloženi drži u tajnosti

**Hitna zaštita i djelomično otkrivanje podataka o prometu**

- **podaci o prometu** su svi računalni podaci u vezi komunikacija, koji su stvoreni pomoću računalnog sustava koji je dio komunikacijskog lanca, a koji podaci naznačuju podrijetlo komunikacije, njezino odredište, put, vrijeme, datum, veličinu, trajanje ili vrstu te usluge

- i ti podaci podložni su promjenama i uništenju te je potrebno osigurati njihovu zaštitu

- ako u komunikacijskom lancu sudjeluju 3 davatelja usluga kao posrednici,onda je uporaba podataka koji se nalaze kod prvog preduvjet da bi se mogli sačuvati i koristiti podaci kod drugog (i nakon toga trećeg) davatelja komunikacijske usluge

- prema **čl. 17. Konvencije** svaka članica dužna je osigurati mogućnost hitne zaštite podataka o prometu, bez obzira na to koliko je davatelja komunikacijskih usluga uključeno u prijenos komunikacije

- to se ostvaruje na način da države članice stvore pravne mehanizme kojima se može hitno otkriti nadležnom tijelu dovoljnu količinu podataka potrebnu za indentifikaciju svih davatelja komunikacijskih usluga

**Nalog za predaju podataka**

- svaka država članica dužna je usvojiti zakonske i druge mjere potrebne da bi njezina nadležna tijela mogla naložiti osobi koja posjeduje određene računalne podatke da ih preda (odnosi se na sve računalne podatke)

- posebna pravila predviđena su za predaju tzv. **pretplatničkih informacija**

- **nadležna tijela mogu naložiti davatelju komunikacijskih usluga koji se tiču:**

**a)** vrste komunikacijske usluge koja je korištena, poduzetih tehničkih mjera i razdoblja pružanja usluge

**b)** pretplatnikovog identiteta, adrese, broja telefona, informacije za slanje računa

**c)** sve druge informacije o mjestu gdje je komunikacijska oprema instalirana, raspoložive na osnovi pretplatničkog ugovora ili sporazuma

**Pretraga i oduzimanja pohranjenih računalnih podataka**

- clj je ove mjere pronalaženje i prikupljanje dokaza

- Konvencija propisuje da svaka država članica mora usvojiti zakonske i druge mjere potrebne da bi njezina nadležna tijela mogla izvršiti pretragu računalnih podataka te odrediti njihovo oduzimanje ili osiguranje

- potrebno je osigurati da nadležna tijela imaju mogućnost pretraživanja računalnog sustava i njegovih dijelova kao i svih medija koji se nalaze na teritoriju članice

- **oduzimanje, odnosno osiguranje podataka se postiže na način da nadležno tijelo:**

**a)** oduzme ili na sličan način osigura računalo, njegov dio ili medij za pohranu podataka

**b)** napravi ili zadrži kopiju podataka

**c)** sačuva cjelovitost podataka

d) učini podatke nepristupačnim ili ih uklone iz računalnih sustava kojemu je pristupljano

- članice Konvencije moraju osigurati da nadležna tijela mogu naložiti svakoj osobi koja ima saznanja o funkcioniranju računalnog sustava ili o mjerama poduzetim radi zaštite računalnih podataka u njemu da dade informacije koje su razumno nužne

**Prikupljanje prometnih podataka u realnom vremenu**

- cilj je ove mjere identificirati i locirati počinitelja, te otkriti druge supočinitelje i sudionike

- **moguće ju je inplementirati na dva načina:**

**1)** tako da nadležna tijela mogu sama prikupiti ili snimiti dotične podatke

**2)** na način da država osigura da ta nadležna tijela mogu primorati davatelja komunikacijske usluge da u okviru svojih tehničkih mogućnosti prikupi ili snimi potrebne podatke

- i kod ove mjere mora postojati da se davatelja usluge obveže da čuva u tajnosti provođenje ove mjere

**Presretanje podataka o sadržaju**

- cilj je ove mjere presresti i snimiti komunikaciju te analizirati njezin sadržaj neovisno o tome je li riječ o zamjeni datoteka, elektroničkoj pošti, internetskoj telefoniji ili drugom obliku komunikacije

- riječ je najinvazivnijoj mjeri kojom se zadire u privatnost građana, stoga ova mjera zahtijeva vrlo ozbiljna ograničenja i nadzor primjene

**Ravnoteža između postupovnih mjera i očuvanja prava i sloboda građana**

- pisci Konvencije bili su svjesni mogućih zlouporaba zbog prekomjernih ovlasti ako se unaprijed ne odrede granice primjene navedenih mjera

- zbog toga su predvidjeli uvjete i ograničenja kojima se ostvaruje ravnoteža između interesa učinkovitog kaznenog progona i zaštite temeljnih ljudskih prava i sloboda

- izrijekom se zahtijeva primjena načela proporcionalnosti

- očuvanje ljudskih prava podrazumijeva da se primjena mjera i ovlasti može uvjetovati postojanjem ssudskog ili drugog nezavisnog nadzora,provjerom osnova koje opravdavaju primjenu pojedine mjere te ograničavanjem njihova opsega i trajanja

- Konvencija predviđa da se neke od navedenih mjera mogu primjeniti samo kad je riječ o nekim kaznenim djelima, npr. mjera presretanja sadržaja komunikacija može se primjeniti samo u slučaju istrage i progona počinitelja određenih teških kaznenih djela

**6.5. Etiologija hibernetičkog kriminala**

- kao što su brojni i raznoliki pojavni oblici kibernetičkog kriminala, tako su brojni raznoliki oblici i motivi koji u konkretnim situacijama dovode do takvih djela i potiču njegove počinitelje na takve kažnjive radnje

- budući da je svako takvo djelo rezultat djelovanja nekog čovjeka, a čovjek je kao društveno biće nužnu upućen na sredinu u kojoj živi i radi, taka uzroke nemožemo tražiti samo u njemu samom

- potrebno je razlikovati kriminogene učinke koji se nalaze izvan osobe počinitelja (**vanjski, egzogeni, objektivni učinci**) i one koji se nalaze u osobi počinitelja (**unutarnji, endogeni, subjektivni uzroci**)

**6.5.1 Objektivni kriminogeni čimbenici**

- kiberkriminal je opća forma kroz koju se ispoljavaju različite kriminalne aktivnosti kao tradicionalne tako i nove nastale razvojem računalnog kriminala i kiber prostora

- kiberkriminal je kriminalitet suvremenog razvijenog društva, te je u neposrednoj vezi sa stupnjem postignutog društveno ekonomskog razvoja

- kiberkriminal je globalni, transnacionalni kriminalitet kako u pogledu rasprostranjenosti njegova činjenja tako i glede posljedica

- kiberkriminal je neovisan o dobi i znanju počinitelja zbog dostupnosti i lakoće korištenja sofisticiranim alatima i metodama napada

- kiberkriminal odlikuje jedna od najviših stopa rasta popraćena velikim stupnjem neprijavljivanja

- kiberkriminal je posljedica brojnih slabosti, ponajviše ljudskih i tehničkih koje onemogućavaju djelotvornu borbu protiv njega

- kiberkriminal može dovesti do najštetnijih posljedica za pojedinca i društvo u cjelini ugrožavanjem kritične infrasturkture društva

- kiberkriminal je teško suzbiti i zaustaviti

- kiberkriminalu pogoduje sve veća količina podataka s novim zahtjevima za inform. sustave

- kiberkriminal je kriminalitet 21.st. što potvrđuje njegov eksponencijalni rast i veći broj počinitelja takvih kaznenih djela

**6.5.2. Subjektivni kriminogeni čimbenici**

- **Alvin Toffler: Šok budućnosti** -nagovjestio moguće negativne posljedice koje nova tehnologija i ubrzani tempo života nose sa sobom

- upozorio je na pojavu tzv. **bolesti mjene** (nesnalaženje i nepravodobno prilagođavanje sve većeg broja pojedinaca novonastalim promjenama koje uzrokuje razvoj visoke tehnologije)

- dovodi do fizičkih i psihičkih posljedica kod čovjeka:

**a)** preopterećenost informacijama

**b)** stres odlučivanja

- **subjektivni kriminogeni čimbenici:**

**a)** otuđenost

**b)** frustracija

**c)** psihička oboljenja

**d)** motivacija

**e)** stavovi

**f)** shvaćanja

**6.6. Novi trendovi na području kibernetičkog kriminala**

- intentizivni razvoj i povezivanje nacionalnih informacijskih infrastruktura imali su za posljedicu da kibernetički kriminalitet uzima maha i na onim područjima na kojima se već tradicionalno ugrožavaju najvažniji interesi društva, npr. kibernetički terorizam i sve veća sinergija organiziranog i kibernetičkog kriminala

**6.6.1. Sinergije organiziranog i kibernetičkog kriminala**

- tradicionalnu hijerarhijsku, centraliziranu i vertikalnu strukturu sve više zamjenjuje mrežna, decentralizirana i horizontalna organizacija (**prvi trend**)

- **drugi trend** koji ima utjecaj na organizirani kriminal je globalizacija koja pogoduje transnacionalnom organiziranom kriminalu uklanjajući ograničenja u proteku informacija i kretanju ljudi i roba

- **treći trend** se odnosi na nove oblike komunikacije što im omogućava visok stupanj anonimnosti

**- četvrti trend** se odnosi na upotrebu visokih tehnologija za pripremu i počinjenje novih računalnih delikata kao i lakše izvršavanje tradicionalnih

- **peti trend** se odnosi na uspostavu i iskorišavanje crnih kibertržišta i hakera za izradu i ponudu naprava za činjenje kaznenih djela

- **Rob WainWright** izjavio je da je internet postao glavno sredstvo organiziranog kriminala, a koristi se i za krijumčarenje droge i ljudi kao i pranje novca te izvršenja „tradicionalnih“ kaznenih djela i prekršaja

**6.6.2. Drugi trendovi**

**-** predviđanja **tvrtke RSA** u izvještaju **Unutarnji pogled na promjenjivi krajolik prijetnji na području kiberkriminala** navodi slijedeće trendove:

**1. Daljnji rast tržišta kiberkriminala kao usluge**

- proteklih godina ubrzano raste, a vjerojatno će se rast nastaviti

- sve veća konkurencija na tržištu kiberkriminala kao usluge tjera davatelje usluga da se ponašaju kao na legalnom tržištu nudeći mogućnost povrata sredstava ako roba ili usluga ne bude funkcionalna

- sve veća potražnja za alatima ili uslugama vodi većoj ponudi i konkurenciji

- veća konkurencija vodi većoj inovativnosti ponuditelja što rezultira većom kvalitetom napravljenog malwarea i većoj sofisticiranosti usluga koje se na tom tržištu nude

- sve više dolazi do pada cijena pa se mnoge vrste napada ili alata nude iznimno povoljno

***\* crimeware je*** *izraz za softver koji se koristi za činjenje kaznenih djela u kiberprostoru, kao što su krađa osobnih podataka,novca ili vlasničkih informacija,a može se širiti putem virusa, trojanskih konja,crva,spywarea ili adwarea*

**2. Veće korištenje mobilnim telefonima otvara veće područje za napad**

- danas oko polovice odrasle svjetske populacije posjeduje pametni telefon čime oni postaju uređaji za koji su korisnici vezani više nego za računala

- najveći broj napada izvodi se na mobitelima koji upotrebljavaju operativni sustav android jer je njegov tržišni udio oko 79%, ali razlog tome nije samo tržišni udio nego i to što je riječ o otvorenom sustavu

**3. Razvoj novih taktika napada**

- bankovni botnetovi postaju sve otporniji na njihovo ukidanje, a cilj napada se sve više seli s fizičkih osoba na sektor trgovine i financijske institucije

- očekuju se napadi velikih razmjera na maloprodaju i bankarske sustave zato što kriminalci traže učinkovitije i profitabilnije vrste napada

**4.Rast ciljanih i naprednih prijetnji**

- **spear-phishing** je ciljana prijevara e-mail poštom počinjena s jedinom namjerom dobivanja neovlaštenog pristupa osjetljivim podacima

- za razliku od phishinga, koji je usmjeren na široki krug potencijalnih žrtava, spear-phishing je usmjeren na određenu grupu ili organizaciju

- namjera je da se ukrade intelektualno vlasništvo, financijski podaci, poslovne ili vojne tajne

- očit je sve veći prijelaz na tzv. **Watering-hole napade** pri kojima kriminalac kompromitira organizaciju koja je od poslovnog ili drugog interneta za primarnu metu tj. zaposlenike tvrtke koje želi napasti

- **trend mikro sigurnosna predviđanja za 2015:**

**1)** sve više kiberkriminalaca će se koristiti darknetovima i ekskluzivnim pristupom forumima za razmjenu i prodaju Crimewarea

**2)** povećana kiber aktivnost će dovesti do boljih hakerskih alata i pokušaja napada

**3)** ciljani napadi će postati prevladavajući oblik kiberkriminala

**4)** novi načini mobilnih plaćanja će dovesti do novih prijetnji

**5)** Exploit kits će najprije ciljati operativni sustav Android na mobitelima

**6)** biti će više pokušaja iskorištavanja ranjivosti programa otvorenog koda

**7)** tehnološke različitosti će spasoto IoE/IoT uređaje od masovnih napada,ali ne i podatke

**8)** pojavit će se ozbiljne prijetnje motivirane zloporabama online bankarstva i dr. financijskih usluga

- novi poslovni model kriminala kao usluge sve više postaje glavni čimbenik koji komercijalnom ponudom alata i usluga pogoduje činjenju svih oblika kiberkriminala

-ključnu ulogu na tom crnom kibertržištu sve više ima organizirani kriminal

- žrtve su sve manje pojedinci, a sve više tvrtke i sektori na kojima se može ostvariti veći profit

- budući da je rijeć o globalnom problemu jedini način da se to spriječi je zajednička međunarodna aktivnost i suradnja specijaliziranih jedinica policije i privatnog sektora uz velika ulaganja onih zemalja koje su najviše ugrožene

**7. Cjelina: VISOKE TEHNOLOGIJE I INTELEKTUALNO VLASNIŠTVO**

**7.1. Uvod**

- **pojam intelektualnog vlasništva** odnosi se na nematerijalna dobra (proizvodi ljudske kreativnosti, umnog rada i stvaralaštva poput izuma,književnih i umjetničkih djela,dizajna proizvoda te simbola i nazivlja korištenog u pravnom prometu)

- **pravo intelektualnog vlasništva je** pravna disciplina koja izučava pravne institute razvijene radi zaštite intelek. vlasništva,tj. poticanja znanstvenog, tehničkog i umjetničkog napretka

- u osnovi svih prava intel.vlasn. stoji **društveni ugovor**

- put do prihvaćenog sustava prava intelek. vlasn. trajao je skoro 500 godina ( od prvih patentnih pisama engleskih vladara i zakona koje je izglasala Narodna skupština u Parizu 1791.g., pa sve do WIPO-vih internetskih ugovora iz 1995.g.)

- u osnovi prava intelektualnog vlasništva je namjera da se piscima, slikarima, izumiteljima i drugim kreativnim autorima dodjeli vremenski ograničen monopol ekonomskog iskorištavanja vlastitog djela, a to daje autoru pravo da ponudi svoj rad na tržištu,stavi ga u gospodarski prostor i da živi od svog rada

- nakon isteka **roka zaštite** ( 70 g. nakon smrti autora ili 20 g. nakon 1.registracije patenta) autorova djela prelaze u **public domain** (javno vlasništvo) i slobodna su za uporabu i korištenje bez naknade

- moderni sustav intel. vlasn. je temelje dobio krajem 19.st. u obliku **3 velike međunarodne konvencije:**

**1)** Pariška konferencija za zaštitu industrijskog vlasništva (1883.g.)

**2)** Bernska konferencija za zaštitu književnih i umjetničkih djela (1886.g.)

**3)** Madridski sporazum u pogledu međunarodne registracije znakova (1891.g.)

- prava intel. vlasn. uređuju načine stjecanja intel.vlasn. i načine zaštite njegova neovlaštenog korištenja

- tradicionalno, **pravo intelekt. vlasn. dijelimo u 2 grupe:**

**1) autorsko pravo i njemu srodna prava** – obilježava ih dug jednokratan rok trajanja zaštite te nepostojanje posebno propisanog postupka registracije (npr. prava proizvođača fonograma, prava umjetnika izvođača, prava organizacija za radiodifuziju, prava filmskih producenata, nakladnika na izdanjima i prizvođača baza podataka na bazama podataka)

**2) prava industrijskog vlasništva** – prava kojima se izumitelji, proizvođači i drugi nositelji prava štite od neovlaštene konkurencije koja bi bez naknade iskorištavala rezultate njihova istraživanja, razvoja i promocije te ga karakterizita određeni propisani postupak registracije (npr. patent, žig, industrijski dizajn, oznake zemljopisnog podrijetla, oznake izvornosti,itd.)

- prava intel.vlasn. su usko povezana s informacijskim tehnologijama

- daljnji razvoj intel.vlasn. će ovisiti o međuodnosu prava intel.vlasn. s pravom tržišnog natjecanja,pravom zaštite potrošača, pravom na zaštitu privatnosti,tj. zaštitu osobnih podat.

**7.2. Pravna zaštita računalnih programa**

**7.2.1. Općenito**

- razvoj računalnih programa je kapitalno i intelektualno zahtjevna djelatnost

- kompetentni računalni programeri su visoko specijalizirana i tražena radna snaga

- računalne programe je potrebno adekvatno regulirati kako bi se zaštitilo investitore, razvijatelje (developere, programere) i korisnike

- sred. 70-ih je **WIPO** **(World Intelectual Property Organization)** raspravljao o odabiru odgovarajuće zaštite računalnih programa, a razmatrani modeli zaštite su podrazumijevali primjenu odredaba autorskog prava, patentnopravnu zaštitu, zaštitu putem poslovne tajne i općih pravila obveznog prava te zaštitu putem sui generis prava (nije postignut konsenzus)

- kraj 70-ih i poč. 80-ih 20.st. označava prekretnicu u razmatranju odabira pravne regulacije računalnih programa (izum mikroprocesora, širenje inform.tehnologije izvan vojnih i akademskih krugova te revolucija kućnih i osobnih računala)

**7.2.2. Ključni pojmovi**

- **softver je** programska osnovica informacijskog sustava u kontrastu prema **hardveru** – materijalnoj,tj.fizičkoj osnovici

- iako se softver koristi kao istoznačnica pojmu računalni program, on nekad označava i dodatne sadržaje – datoteke s dodatnim katalogom instrukcija (tzv.library datoteke) te uputstva i dokumentaciju koja komentira rad i mogućnosti računalnog programa

- **računalni program** (prema Direktivi 2009/24/EZ Eurospkog parlamenta o pravnoj zaštiti računalnih programa) je program u bilo kojem obliku koji uključuje programe koji su ugrađeni u hardver te pripremne materijale koji su poslužili u razvoju računalnog programa pod uvjetom da je priroda pripremnih materijala takva da mogu poslužiti za izradu računalnog programa

- **računalni program** (prema KZ) je skup računalnih podataka koji su u stanju prouzročiti da računalni sustav izvršiodređenu funkciju

- **pojam softverske industrije** obuhvaća ukupnost gospodarske aktivnosti zasnovane na razvoju i komercijalnom iskorištavanju softvera ( tu spadaju multinacionalne kompanije poput Googlea, Microsofta, Facebooka te razne manje i srednje kompanije)

- softverske kompanije često počinju kao **tzv. startup kompanije** pokrenute s minimumom sredstava i u spartanskim uvijetima, a s godinama mogu izrasti u industrijskog diva koji zapošljava na desetke tisuća programera,dizajnera i inženjera

***\* startup kompanija je*** *poduzeće formalno osnovano kao trgovačko društvo ili ortakluk sa svrhom istraživanja potreba tržišta i razvoja održivog poslovnog modela koji nudi proivod ili uslugu tržištu*

- priroda tržišta i distribucije softvera je globalna, riječ je o **direktnoj elektroničkoj trgovini**

- postoje mnoge definicije računalnih programa,a neke od njih se odnose na funkciju i namjenu računalnog programa,neke na komercijalnu primjenu

- **najednostavnija definicija računalnog programa** bila bi da je riječ o skupu naredbi namijenjenih izvršenju određenog zadatka od strane računala

- računalni program se može sastojati od 1 ili niza naredbi unešenih u datoteku u obliku strojnog jezika ili pisanih u nekom od tzv. viših programskih jezika (npr. inačice BASIC jezika, C, Pascal, Ruby, PHP – više ih je od 200)

- **računalni program je korisnicima dostupan u 2 oblika:**

**1)** kao **izvršna datoteka** – oblik računalnog programa koje računalo može izvršiti

**2)** kao **izvorni kod programa** – skup programiranih naredbi unesenih upotrebom nekog programskog jezika u obliku teksta koje programer može razumijeti i interpretirati

- **kompilacija** je postupak preoblikovanja programeru i korisniku razumljivog izvornog koda u izvršni kod koji je razumljiv samo računalu

- **dekompilacija** je povrat izvornog koda iz izvršnog koda

- **digitalno ili softversko piratstvo** je neovlaštena distribucija i reprodukcija,tj. stavljanje na raspolaganje javnosti putem interneta zaštićenih digitalnih sadržaja,tj. računalnih programa

- neovlaštena distribucija je uređena KZ-om i u prekršajnim odredbama ZAPSP-a

**7.2.3. Razvoj pravne zaštite računalnih programa**

- prvi zakon, koji je eksplicitno uredio pravni status računalnih programa kao autorskog djela, donesen je 1980.g. u SAD-u u okviru reforme Zakona o autorskom pravu

- autorskopravna zaštita počinje samim činom nastanka djela i traje 70 g. nakon smrti autora te djeluje prema svim fizičkim i pravnim osobama

- Silicijska dolina je postala svjetski centar razvoja informacijskih tehnologija

- američki primjer su prihvatila europska i azijska zakonodavstva tijekom 80-ih i 90-ih g.

- američki zakonodavac nije isključio mogućnost drugih oblika zaštite (npr.patentna zaštita)

- 1975.g. su europska nacionalna zakonodavstva usvajanjem **Europske patentne konvencije** isključila računalne programe od patentne zaštite

**7.2.4. Od Bernske konvencije do WTO TRIPS-a**

- na međunarodnoj razini, sustav autorskog i srodnih prava počiva na **Bernskoj konvenciji** iz 1886.g. koja predstavlja platformu regulacije sadržaja i ostvarivanja autorskog prava i temelj suvremenog sustava intel.vlasništva, no ne sadrži odredbe o računalnim programima

- 1. multilateralni sporazum koji regulira računalne programe kao autorska djela je **TRIPS** – The Agreement on Trade-Related Aspects of Intellectual Property Rights ili Sporazum o trgovinskim aspektima prava intelektualnog vlasništva pripremljen u okviru WTO (1994.g.)

- **WTO** se bavi ukidanjem prepreka slobodnoj trgovini među zemljama članicama,tj. radi na uklanjanju financijskih i administrativnih zapreka poput carina i dr. naknada i stvaranja jedinstvenog trgovinskog prostora među članicama (više od 150 članica)

- WTO ima i ulogu rada na široj zaštiti intelektualnog vlasništva

- TRIPS je stvoren kao okvir primjene WTO pravila na pitanja gospodarskog iskorištavanja i trgovine na području intelekt.vlasništva

- čl.10. TRIPS-a definira računalne programe kao autorska književna djela zaštićena prema odredbama Bernske konvencije

**a) Utjecaj TRIPS-a na kasniju međunarodnu legislativu**

- osim zaštite računalnih programa, TRIPS je uveo i novu kategoriju intelektualnog vlasništva,a to je zaštita topografija poluvodičkih integriranih sklopova,tj. rasporeda poluvodičkih elemenata na tiskanim pločama koje su osnova elektroničkih uređaja

**b) Računalni programi u ugovorima Svjetske organizacije za intelektualno vlasništvo**

- Svjetska organizacija za intelektualno vlasništvo sred. 90-ih 20.st. usvaja tzv. WIPO-ve internetske ugovore (Ugovor o autorskom pravu Svjetske organizacije za intel.vlasn i Ugovor o izvedbama i fonogramima Svjetske organizacije za intel.vlasn. iz 1996.g.)

- čl.4. Ugovora o autorskom pravu definira računalne programe kao autorska djela

**7.2.5. Zakonodavstvo Europske Unije**

- tijela Unije od sred. 80-ih 20.st. intezivno proučavaju utjecaj informacijske tehnologije na intelekt.vlasn. s drugim granama i kategorijama prava, pogotovo pravo tržišnog natjecanja, pravom zaštite potrošača te pravnim okvirom zaštite osobnih podataka

- određen broj država članica pripada common law sustavu koji definira copyright kao primarno imovinsko pravo ( **right to copy** – Statute of Anne, 1708.g.)

- većina članica EU pripada kontinentalnom europskom pravnom krugu i svoje autorskopravno zakonodavstvo bazira na francuskom **droit d'auteur modelu** koji karakterizira dualizam imovinskih i moralnih prava

- hrvatski pravni sustav određuje da **autorsko pravo sadrži:**

**a) moralna prava autora**

**b) imovinska prava autora**

**c) druga prava autora**

- 1998. g.- **Copyright and the Challenge of Technology** ( prvi službeni dokument kojim je Europska komisija razmatrala utjecaj inform.tehnologija na europski pravni okvir autorskog prava objavljen kao neformalni **green paper**)

- **10 direktiva** *(\*u knjizi piše 9, a navedeno ih je 10)* koje uz TRIPS, Bernsku konvenciju te WIPO-ve ugovore čini okvir europskog autorskog prava:

**1)** Direktiva o računalnim programima (Direktiva 2009/24/EZ Europskog parlamenta i Vijeća od 23.4.2009. o pravnoj zaštiti računalnih programa)

**2)** Direktiva o pravu posudbe ( Direktiva 2006/115/EZ Europskog parlamenta i Vijeća od 12.12.2006. o pravu iznajmljivanja i pravu posudbe te o određenom autorskom i srodnim pravima u području intel.vlasn.)

**3)** Direktiva o pravima na satelitsko i kabelsko emitiranje i reemitiranje ( Direktiva 93/83/EZ Europskog parlamenta i Vijeća od 27.9.1993. o koordinaciji određenih pravila s obzirom na autorsko i srodna prava koji se odnose na satelitsko i kabelsko emitiranje i reemitiranje)

**4)** Direktiva o bazama podataka ( Direktiva 96/9/EZ Europskog parlamenta i Vijeća od 11.3.1996. o pravnoj zaštiti baza podataka)

**5)** Direktiva o elektroničkoj trgovini (Direktiva 2000/31/EZ Europskog parlamenta i Vijeća od 8.6.2000. o pravnim aspektima usluga inform.društva na unutarnjem tržištu)

**6)** Direktiva o djelima siročadi ( Direktiva 2012/28/EU Europskog parlamenta i Vijeća od 25.10.2012. o određenim dozvoljenim korištenjima djela siročadi)

**7)** Direktiva o informacijskom društvu (Direktiva 2001/29/EZ Europskog parlamenta i Vijeća od 22.5.2001. o usklađivanju određenih aspekata autorskog i srodnih prava u inf.društvu)

**8)** Direktiva o pravu slijeđenja (Direktiva 2001/84/EZ Europskog parlamenta i Vijeća od 27.9.2001. o pravu slijeđenja u korist autora izvornikka umjetničkog djela)

**9)** Direktiva o provedbi zaštite ( Direktiva 2004/48/EZ Europskog parlamenta i Vijeća od 29.4.2004. o provedbi zaštite intel.vlasn.)

**10)** Direktiva o trajanju zaštite (Direktiva 2006/116/EZ Europskog parlamenta i Vijeća od 12.12.2006. o trajanju zaštite autorskog prava i određenih srodnih prava)

**7.2.6. Računalni programi u zakonodavstvu RH**

- hrvatski pravni sustav računalni program smatra autorskim djelom

- ZAPSP uređuje autorsko pravo kao pravo autora na djelima iz književnog, znanstvenog i umjetničkog područja te srodna prava poput prava umjetnika izvođača na njihovim izvedbama, prava proizvođača fonograma na njihovim fonogramima, prava filmskih producenata (proizvođača videograma) na njihovim videogramima, prava organizacija za radiodifuziju na njihovim emitiranjima, prava nakladnika na njihovim izdanjima, prava proizvođača baza podataka na njihovim bazama podataka

- ZAPSP uređuje i ostvarivanje autorskog prava i srodnih prava, kako individualno ( od strane autora ili drugog nositelja prava,npr.nakladnika) tako i kolektivno (od strane tijela za kolektivno ostvarivanje prava kojima autori ustupaju ostvarivanje svojih prava zbog učinkovitosti i pravne sigurnosti te lakše zaštite od povreda)

**a) Računalni program kao autorsko djelo**

- **autorsko djelo je** originalna intelektualna tvorevina iz književnoga, znanstvenog i umjetničkog područja koja ima individualni karakter, bez obzira na način i oblik izražavanja, vrstu, vrijednost ili namjenu

- računalni program je zaštićen kao jezično djelo ako ispunjava **uvjet izvornosti** (računalni program je izvoran ako je vlastita intelektualna tvorevina svog,odnosno svojih autora)

- **pojam računalni program** obuhvaća izražaj računalnog programa u bilo kojem obliku uključujući i pripremni dizajnerski materijal, a ideje i načela na kojima se zasniva bilo koji element računalnog programa, uključujući i ona na kojima se zasnivaju njegova sučelja, nisu zaštićena autorskim pravom 🡪 autorsko pravo ne štiti ideje,već njihovo konkretno oživotvorenje u formi autorskog djela

- autor djela je fizička osoba koja je autorsko djelo stvorila te mu pripada autorsko pravo na njegovu autorskom djelu činom samog stvaranja autorskog djela

- **sadržaj autorskog prava:**

**1) moralna prava autora** – štite osobne i duhovne veze autora s njegovim djelom

**2) imovinska prava autora** – štite autorove imovinske interese u pogledu njegova djela

**3) druga prava autora** – štite ostale interese autora

- **moralna prava autora:**

**a) pravo prve objave** - pravo autora da odredi hoće li, kada, gdje, kako i pod kojim uvjetima njegovo autorsko djelo biti prvi put objavljeno

**b) pravo na priznanje autorstva** – autorovo pravo biti priznat i označen kao autor djela

- osoba koja javno koristi autorsko djelo dužna je pri svakom korištenju naznačiti autora, osim ako autor u pisanom obliku izjavi da ne želi biti naveden ili ako način pojedinoga javnog korištenja autorskog djela onemogućava navođenje autora

**c) pravo na poštivanje autorskog djela i čast ili ugled autora** - autor ima pravo usprotiviti se deformiranju, sakaćenju i sličnoj izmjeni svojega autorskog djela, te uništenju kao i svakom korištenju autorskog djela na način koji ugrožava njegovu čast ili ugled

**d) pravo pokajanja** - pravo autora da opozove pravo na iskorištavanje njegovoga autorskog djela i njegovo daljnje korištenje, uz popravljanje štete korisniku toga prava, ako bi daljnje korištenje štetilo njegovoj časti ili ugledu

- uz bok moralnim stoje i imovinska prava autora

- autor ima isključivo pravo raditi sa svojim autorskim djelom što ga je volja dok god je to u skladu sa zakonom

- **imovinska prava autora su:**

**a) pravo reproduciranja** - isključivo pravo izrade autorskog djela u jednom ili više primjeraka, u cijelosti ili u dijelovima, izravno ili neizravno, privremeno ili trajno, bilo kojim sredstvima i u bilo kojem obliku

- pravo reproduciranja uključuje i fiksiranje kojim se označava utvrđivanje autorskog djela na materijalnu ili drugu odgovarajuću podlogu

- u kontekstu računalnih programa to podrazumijeva zapisivanje računalnog programa na unutarnju ili vanjsku memoriju za pohranu podataka (tvrdi ili solid state disk,optički medij, flash memoriju ili kakav drugi oblik fizičke memorije lokalno ili na mreži)

**b) pravo distribucije** - isključivo pravo stavljanja u promet izvornika ili primjeraka autorskog djela prodajom ili na koji drugi način te njihova nuđenja javnosti u tu svrhu

- iznajmljivanje označava davanje na korištenje izvornika ili primjeraka djela u ograničenom razdoblju radi ostvarivanja izravne ili neizravne imovinske ili komercijalne koristi

**c) pravo priopćavanja autorskog djela javnosti** - autor ima isključivo pravo priopćavanja autorskog djela javnosti,a to pravo obuhvaća:

**1)** pravo javnog izvođenja

**2)** pravo javnog prikazivanja scenskih djela

**3)** pravo javnog prenošenja

**4)** pravo javnog priopćavanja fiksiranog djela

**5)** pravo javnog prikazivanja

**6)** pravo radiodifuzijskog emitiranja

**7)** pravo radiodifuzijskog reemitiranja

**8)** pravo javnog priopćavanja radiodifuzijskog emitiranja

**9)** pravo stavljanja na raspolaganje javnosti – osobito važno za autorska djela u digitalnom obliku (isključivo pravo da se autorsko djelo priopći javnosti,bežično ili putem žica, na način koji pripadnicimajavnosti omogućava pristup autorskom djelu s mjesta i u vrijeme koje sami odaberu )

**d) pravo prerade** - isključivo pravo na prevođenje, prilagođavanje, glazbenu obradu ili koju drugu preinaku autorskog djela

- autor je slobodan dopustiti (licencirati) drugima da dospodarski iskorištavaju njegovo djelo uz njega ili nekog trećeg (**neisključiva licencija**) ili umjesto njega ili bilo koga drugoga (**isključiva licencija**)

- jedina ograničenja prepoznaje i regulira ZAPSP kao **vremenska i sadržajna ograničenja autorskog prava**

- **rok trajanja zaštite** je životni vijek autora i 70 godina nakon njegove smrti

- **sadržajna ograničenja autorskog prava** predstavljaju zakonom i međunarodnim konvencijama određene slučajeve poput privremene radnje reproduciranja autorskog djela, reproduciranja autorskog djela za privatno i drugo vlastito korištenje, izradu efemernih snimki, ograničenja u korist pojedinih ustanova koje imaju određene ovlasti koje se odnose na čuvanje i osiguranje djela bez ostvarivanja komercijalne koristi

**b) Poseban položaj računalnog programa u odnosu na ostale kategorije autorskih djela**

- status računalnih programa je dijelom iznimka od općih pravila i u 8.poglavlju ZAPSP-a su donesene posebne odredbe za računalne programe

- čl.109. ZAPSP-a definira prava autora na računalnom programu

- **autor ima isključivo pravo odobriti:**

**1)** trajno ili privremeno reproduciranje računalnog programa bilo kojim sredstvom i u bilo kojem obliku, djelomično ili u cijelosti, to uključuje i učitavanje, prikazivanje, izvođenje, prenošenje ili pohranu računalnog programa za koje je potrebno takvo reproduciranje

**2)** prijevod, prilagodbu, obradu i bilo koju drugu izmjenu računalnog programa te reproduciranje rezultata tih izmjena, s time da prava osobe koja je izmijenila program ostaju nedirnuta

**3)** distribuciju izvornika ili primjeraka računalnog programa, u bilo kojem obliku, kao i njihovo iznajmljivanje

- te posebne odredbe se odnose i na iznimke u pogledu imovinskih,ali i nekih moralnih prava

- ako je računalni program stvorio zaposlenik u izvršavanju svojih obveza ili slijedeći upute poslodavca, poslodavac je isključivo ovlašten izvršavati sva imovinska prava na tako stvorenom programu, ako ugovorom nije drugačije određeno

- na računalni program se ne primijenjuju odredbe o pravu pokajanja,ograničenju autorskog prava u pogledu reprodukcije autorskog djela za privatno i drugo vlastito korištenje bez izravne ili neizravne komercijalne svrhe te ostavrivanje prava na naknadu za reproduciranje autorskog djela za privatno ili drugo vlastito korištenje

**c) Dekompiliranje**

- autor odlučuje hoće li uz izvršni oblik programa distribuirati i njegov izvorni kod

- komercijalni računalni programi dolaze isključivo u izvršnom obliku, a prateći licencijski ugovori od korisnika zahtijevaju da se suzdrže od radnji koje mogu dovesti do povrede autorovog isključivog prava na prilagodbu,obradu i drugu izmjenu

- ZAPSP predviđa iznimku autorovog isključivog prava da odobri izmijenu ili prilagodbu programa u pogledu dekompilacije,pod uvijetom da su zadovoljeni određeni uvijeti:

1) da te radnje izvodi osoba koja ima odobrenje za korištenje ili druga osoba koja ima pravo koristiti primjerak programa, ili osoba koja je u njihovo ime ovlaštena to učiniti

2) da informacije potrebne za postizanje interoperabilnosti prethodno nisu bile odmah dostupne prethodno navedenim osobama

3) da su te radnje ograničene samo na one dijelove izvornog programa koji su potrebni za postizanje interoperabilnosti

- dekompilacija može omogućiti stručnjacima neovisnu procjenu o pravoj svrsi računalnog programa koji može posjedovati i razne karakteristike malicioznih programa, poput backdoorova i dr. metoda ostvarivanja neovlaštenog pristupa korisnikovom računalu, praćenja korisnikove aktivnosti na računalu i internetu, praćenja korisnikove komunikacije,..

**d) Posebne mjere zaštite**

- ponuda i distribucija digitalnih sadržaja,pa tako i računalnih programa je temeljni aspekt elektroničke trgovine

- digitalnu distribuciju prate brojne prednosti (trenutačna dostupnost i naplata, niski troškovi umnožavanja i distribucije),ali i mane (digitalno piratstvo, vezanost uz neku konkretnu uslugu i mogućnost da propašću usluge korisnik ostane bez licenciranog sadržaja)

- 80-ih g. se javljaju prve **tehnologije digitalnog upravljanja pravima** (DRM- Digital Rights Managment) kao zaštita od neovlaštene distribucije i reprodukcije digitalnih sadržaja

- najčešće je riječ o sveobuhvatnim rješenjima,mjerama i sredstvima ugrađenih u tehničku ili programsku osnovicu računala,igračih konzola, mobitela i sl.uređaja

- u širem smislu, DRM tehnologije osim tehničkih mjera zaštite(poput npr.enkripcije) mogu obuhvatiti i sustave i rješenja koja služe identifikaciji autora,autorskog djela ili predmeta srodnog prava,uvjeta korištenja i sl. (npr.digitalni vodeni biljeg)

- **upotreba DRM tehnologija ima:**

**a) pravne učinke** (očituju se na području razvoja regulative koja zabranjuje osujećivanje tehničkih mjera zaštite kao one koja jamči zaštitu privatnosti korisnika od mogućih negativnih učinaka takvih tehnologija)

**b) ekonomske ili gospodarske učinke** (očituju se u koristima koje nositelji autorskog prava i drugi poslovni subjekti,pa i društvo, imaju od razvoja i distribucije proizvoda i usluga koje se koriste DRM tehnologijom ili je pak razvijaju

**c) društvene učinke** (tu ubrajamo nastanak političkih pokreta sa svrhom izmjene pravnog položaja digitalnih sadržaja i njihova korištenja,tj. položaja nositelja prava na takvim sadržajima,a u tome su posebno aktivne tzv. Piratske stranke i Free Software pokret čiji je osnovni motiv borbe opasnost koju takve tehnologije mogu predstavljati za privatnost korisnika te sigurnost i integritet podataka u njihovim inform. sustavima)

- odredbe u pogledu zabrane zaobilaženja tehničkih mjera zaštite od neovlaštene reprodukcije i distribucije u hrv.pravnom okviru se nalaze u čl.112.,.175.,176. i 189.st.17. i st.18. ZAPSP-a te u čl.285. st.3. KZ RH

-o povredi prava autora se radi ako počinitelj bilo kojom radnjom distribucije ili posjedovanjem u komercijalne svrhe bilo kojeg sredstva čija je jedina namjena olakšati neovlašteno uklanjanje tehničkog uređaja koji služi za zaštitu računalnog programa ili osujetiti rad toga uređaja

- pod sredstvom se smatra tehnička zaštitna mjera u obliku posebnog softvera (npr. sustav provjere identiteta i prava kakav je ugrađen u operativne sustave pametnih telefona,a koji ne dopušta upotrebu računalnih progra,a koji nisu distribuirani preko službenog distribucijskog kanala,tj. preuzeti iz autoriziranog dućana)

- čl. 176. ZAPSP-a - **podaci o upravljanju pravima** su podaci navedeni od strane nositelja prava kojima se identificira autorsko djelo,tj. predmet zaštite srodnog prava, nositelj prava, uvjeti uporabe odnosno korištenja djela, kao i brojke ili kodovi koji predstavljaju takve podatke ako su navedeni na primjerku autorskog djela ili predmeta srodnog prava iz ovoga Zakona ili se pojavljuju u svezi s njihovim priopćavanjem javnosti

- povredu autorskog prava i srodnih prava čini i osoba koja zna da bez ovlaštenja: uklanja ili preinačuje podatke o upravljanju pravima u elektroničkom obliku, proizvodi, distribuira, uvozi radi stavljanja na tržište, emitira, priopćava javnosti ili stavlja na raspolaganje javnosti autorska djela i predmete srodnih prava s kojih su podaci o upravljanju pravima u elektroničkom obliku uklonjeni ili preinačeni bez ovlaštenja nositelja tog prava ako zna ili mora znati da time uzrokuje, omogućava, olakšava ili prikriva povredu prava iz ovoga Zakona s obzirom i na to da je njezina primjena zamisliva i u slučaju tako distribuiranih rač.programa

- KZ određuje kaznu zatvora od 1 do 3 godine za počinitelja koji protivno propisima kojima se uređuju autorsko i srodna prava osujećuje tehničke mjere za zaštitu prava autora i umjetnika izvođača ili ukloni ili preinači podatke o upravljanju tim pravima i tako pribavi imovinsku korist ili prouzroči znatnu štetu,a djelo je kažnjivo i u pokušaju

**e) Kaznene i prekršajne odredbe o povredi prava autora računalnog programa**

- prava autora su zaštićena odredbama Glave XXVII. KZ-a – Kaznena djela protiv intelektualnog vlasništva, a posebno čl.284. Povreda osobnih prava autora ili umjetnika izvođača te čl.285. Nedozvoljena upotreba autorskog djela ili izvedbe umjetnika izvođača

- ZAPSP u čl.189. predviđa prekršajne sankcije za povrede autorskog i srodnih prava, pa tako i za računalne programe

**7.2.7. Slobodni softver i softver otvorenog koda**

- **razvoj softvera** bilo od strane programera pojedinca ili od skupine programera je postupak u kojem autori dodaju i mijenjaju djelo do trenutka objave gotove inačice

- kada je autor programer pojedinac ili kada se softver razvija u okviru komercijalne djelatnosti nekog trgovačkog društva, pitanje autorstva i upravljanja autorskim pravom na softveru kao autorskom djelu najčešće je regulirano ugovorima i postojećim autorskopravnim okvirom

- hrvatski zakon određuje da ako je računalni program stvorio zaposlenik u izvršavanju svojih obveza ili slijedeću upute poslodavca, poslodavac je isključivo ovlašten izvršavati sva imovinska prava na tako stvorenom programu,ako ugovorom nije drugačije određeno

- suvremeni računalni programi se mogu sastojati od milijuna linija koda i sve su rjeđe plod rada samostalnog pojedinca

- svi autori ne trebaju dijeliti isti stav o konačnom izgledu programa, njegovoj upotrebi ili komercijalnosti

- karakter softvera kao autorskog djela se razlikuje od ostalih autorskih djela

- broj participirajućih autora koji mogu razvijati neki softver nije ograničen fizičkom prisutnošću niti potrebom nalaženja i usuglašavanja stavova

- servisi SourceForge ili Freshmeat te Linux su primjeri okupljališta koja broje tisuće softverskih projekata i desetke tisuća programera

- autori razvijaju vlastite inačice projekta, projekti se cijepaju i razdvajaju u međusobno neovisne projekte i konačne programe koji dijele osnove računalnog koda na kojima su započeli svoj razvoj 🡪 karakteristika softverske industrije

- računalni hardver i pametni elementi industrijskih strojeva, automobila, zrakoplova itd. se često koriste **ugrađenim** (**embedded** – računalni program pohranjen direktno u čipovima koji kontroliraju rad uređaja) **softverom** kojeg su razvijali više desetina ili stotina programera koji su surađivali na daljinu, često bez formalnopravnog okvira, u okviru nekog neformalnog projekta ili iz hobija ili želje da doprinesu rješenju nekog tehničkog problema 🡪 nije praktično i ekonomično

**a) Slobodni softver i GNU javna licencija (GNU Public Licence, GPL)**

- **GNU javna licencija** je najpopularniji i najčešće korišteni tipizirani licencijski ugovor na području upravljanja pravima na računalnim programima 🡪 njegov autor je **Richard M. Stallman** koji je sa suradnicima okupljenima u Free Software Foundation poč. 80-ih g. osmislio **GPL** kako bi razvio alternativni oblik zaštite i distribucije računalnih programa

- **tzv. bulletin board** sustavi su omogućili korisnicima korištenje servisom poput e-pošte i prije nego što je internet izašao iz vojne i striktno akademske sfere i postao komercijalno dostupan

- Stalmann je 1985.g. napisao **prvu inačicu GNU javne licencije**,tj. ugovora o licenciranju softvera kojim se autori softvera odriču imovinskih prava na softveru, istovremeno se obvezujući zajedno distribuirati izvršni i izvorni kos programa (kako bi korisnici mogli prilagoditi softver svojim potrebama) te tekst same GNU licencije (kako bi korisnici u svakom trenutku znali što smiju,a što ne s predmetnim softverskim paketima)

- razvoj novih tehnologija i poslovnih modela iskorištavanja softvera (npr. SaaS – software as a service), ali i regulatorni napredak (TRIPS,WIPO ugovori, direktive EU) potakli su nastanak treće inačice ovog licencijskog ugovora (2007.g. je predstavljena javnosti)

**Osnovne značajke**

- **GPL ugovor (licencija) je** autorskopravni licencijski ugovor kojim se korisnici i/ili osobe koje će u budućnosti razvijati licencirani softver obvezuju koristiti se i raspolagati predmetom licencije pod određenim uvijetima koji su prezentirani u odredbama ugovora kao određene „slobode“

- **termin slobode** se koristi kako bi se naglasio fokus GPL ugovora na zaštiti korisnika u odnosu na tradicionalni, **tzv. proprietary**, tj. standardni autorskopravni licencijski model

- **GPL licencija se temelji na 4 slobode** (koje svaki korisnik mora uživati da bi se taj softver mogao nazvati slobodnim) **:**

**1)** sloboda korištenja softverom u bilo koju svrhu

**2)** sloboda mijenjanja i prilagođavanja softvera korisničkoj želji i potrebi

**3)** sloboda daljnje distribucije softver bez naknade

**4)** sloboda korisnika da dalje distribuira izmijenjene inačice softvera

- iz korisničke perspektive, riječ je o širokom ovlaštenju koji nositelj prava pruža korisniku u pogledu upotrebe djela, ali iz perspektive nositelja prava riječ je o znatnim ograničenjima potencijalne komercijalne primjene

- softver objavljen pod GPL licencijom podrazumijeva za autora znatna ograničenja u pogledu komercijalnog iskorištavanja djela

- autor se pristankom na distribuciju pod GNU javnom licencijom odriče svih imovinskih prava, dajući svoje djelo svima zainteresiranima na besplatno korištenje, prilagodbu i daljnju distribuciju

- uvjet pod kojim je to djelo dostupno korisnicima je da i oni moraju, u slučaju daljnje distribucije, garantirati drugim korisnicima istu razinu prava na djelu

- GPL licencija onemogućuje klasično komercijalno licenciranje softvera, što znači da autori programa objavljenog pod GNU licencijom ne mogu tražiti financijsku naknadu za licenciranje zaštićenog programa od korisnika

- **zagovaratelji modela otvorenog softvera** (čije stavove je preuzela i Open Source zajednica) smatraju kako tzv. zatvoreni,tj. komercijalni softver (softver zatvorenog, nedostupnog izvornog koda) predstavlja opasnost za korisnička osobna prava i za inovaciju ( onemogućava i otežava interoperabilnost)

- **proponenti softvera otvorenog** koda smatraju kako pristup otvorenom izvršnom kodu aplikacije garantira uvid u sve funkcionalnosti računalnog programa, bez straha da će izvršna inačica posjedovati namjerne ili slučajne bugove,tj. greške ili backdoorove, odnosno mogućnost daljinskog pristupa i nadgledanja korisnikovog računala i njegovih navika

- poslovni modeli koje zagovaraju uključuje besplatnu distribuciju softvera, dok bi se prihod ostvarivao pružanjem usluga prilagodbe softvera naručitelju (**tzv. individualni softver** koji je namijenjen širokoj distribucij neograničenom broju potencijalnih klijenata bez posebne prilagodbe svakom korisniku), edukacijom korisnika ili zaradom od oglašavanja

- besplatna distribucija omogućava medijsku prisutnost i eskpoziciju

- pristanak nositelja prava na ograničenja,tj. slobode određuje sudbinu djela do isteka statutarnog vremenskog roka autorskopravne zaštite

**GNU licencija u sudskoj praksi**

- hrvatski sudovi se još nisu susreli sa autorskopravnim slučajem,a svjetski jesu

- 1 od prvih zabilježenih slučajeva u kojima je sud razmatrao GNU licencijski ugovor bio je slučaj švedske tvrtke MyDQL AB protiv američkih tvrki Progress i NuSphere oko prava korištenja MySQL softvera izdanog pod uvijetima GNU javne licencije u komercijalnom softveru iz 2002.g. 🡪 sud zaključio da ne postiji pravni razlog zašto raspolaganje pravima na softveru u okviru GNU licencije ne bi bilo pravno valjano

- najpoznatiji slučaj je SCO v. Linux iz 2003.g. (*pročitati slučaj na 256.str.)*

- 2008.g. je Free Software Foundation tužila Cisco Systems Inc. (*pročitati slučaj na 257.str.)*

- u europskoj pravnoj praksi, valjanost GNU licencije potvrđena je odlukom njemačkog suda u slučaju Welte vs. Sitecom Deutschland Gmbh 2004.g. 🡪 Njemački okružni sud je utvrdio kako je njemačka tvrtka distribuirala softver izdan pod GNU licencijom,konkretno firewall pod nazivom iptabels/netfilter, suprotno odredbama tog ugovora

- 2006.g. – slučaj protiv tvrtke D- Link (opet pobjeda GNU licencije)

- u francuskoj pravnoj praksi, slučaj EDU4 v. AFPA je pokazao kako europski sudovi prihvaćaju odredbe GNU licencije kao valjano raspolaganje pravima korištenja zaštićenim softverom

- djelovanje GNU licencije je bilo podvrgnuto i ispitivanju s aspekta zaštite tržišnog natjecanja 🡪 slučaj Wallace v. Free Software Foundation ( *pročitati slučaj na 257.str.)*

**b) Drugi poznatiji primjeri formularnih softverskih licencijskih ugovora**

- **Apache licencijski ugovor** je razvila Apache Software Foundation, a to je jedan od češće korištenih formularnih ugovora zadnjih godina

- Apache ugovor pripada u kategoriju manje obvezujućih licencijskih ugovora budući da od korisnika i programera, koji pridonose daljnjem razvoju koda, ne traži da inačice programa budu dalje licencirane isključivo pod istim uvijetima

- programer može preuzeti izvorni kod objavljen pod uviejtima Apache licencije, dalje ga razvijati i kasniju unaprijeđenu inačicu licencirati kako god želi, uključujući i uobičajeni autorskopravni ugovor uz pridržaj svih prava

- **licencijski ugovori BSD i MIT** su razvila američka sveučilišta 🡪 ni oni ne brane naknadne izmjene pravnog režima upravljanja pravima na derivatnim djelima te dopuštaju povezivanje softvera dostupnog,tj. licenciranog pod njihovim uvjetima sa softverom kojim upravljaju odredbe drugih formularnih licencijskih ugovora (ti ugovori mogu biti znatno restriktivniji ili mogu biti i klasični autorskopravni ugovor

**c) Slobodni softver i intelektualno vlasništvo**

- u opoziciji prema tzv. vlasničkom softveru (softver koji nositelji prava licenciraju slično ostalim kategorijama autorskih djela), slobodni softver je znao biti nepoželjna pojava

- **slobodni softver nije isto što i softver otvorenog koda!!!**

- **termin open source** obuhvaća različite tipizirane licencijske ugovore koji zahtijevaju zajedničku distribuciju izvršnih datoteka i datoteka koje sadrže izvršni kod softvera 🡪 ti ugovori se međusobno razlikuju (površinski-Apache,MIT,BSD ili fundamentlno-GNU)

- **Leveque i Meniere** – većina open source ugovora uredno funkcionira u okvirima pozitivnog autorskopravnog zakonodavstva (proučavaju open source u kontrastu prema softverskim patentima)

- uzroci odbojnosti prema takvom modelu upravljanja pravima na softveru leže u okolnosti u kojoj programeri stvaraju milijune linija programskog koda bez financijske naknade što stvara određene tržišne efekte

- drugi uzrok je vezan uz opasnost upotrebe tako licenciranog softvera za krajnjeg korisnika

- pitanje odgovornosti proizvođača softvera za njegov rad ostaje glavni uzrok zbog čega će vlasnički softver i dalje dominirati poslovnom upotrebom, dok će free software i open source biti popularniji na privatnim računalima, u znanstvenim i istraživačkim institucijama i startup tvrtkama

- slobodan softver predstavlja konkurenciju komercijalnom softveru u pogledu funkcionalnosti i pouzdanosti koji posredno unapređuje i vlasnički(proprietary) softver

- ovi ugovori nude softverskim programerima realnu alternativu tradicionalnim licencijskim ugovorima i novi poslovni model koji stavlja naglasak na promociju pojedinca, medijsku ekspoziciju i izgradnju osobnog brenda (što je zajednička karakteristika svim kategorijama autorskog stvaralaštva)

**d) Creative Commons licencijski ugovori**

- **CC** su skup licencijskih ugovorima o uvijetima raspolaganja zaštićenim autorskim djelima

- CC ugovori pružaju standardizirani okvir odabira primjene određenih autorskopravnih ovlaštenja pri korištenju zaštićenim autorskim djelom i oni ne zamjenjuju klasični autorskopravni okvir zaštite autorskih djela, već omogućuju brzo i jednostavno raspolaganje ovlaštenjima 🡪 **osnovna svrha** im je brže i lakše iskorištavanje zaštićenih djela u digitalnom okruženju

- neprofitnu udrugu koja stoji iza CC ugovora su pokrenuli **James Boyle, Michael Carroll i Lawrence Lessing** 🡪 zamislili su CC kao skup unaprijed formuliranih, tipiziranih licencijskih ugovora koji omogućavaju autorima da sami izaberu koja će prava pridržati, a koja će prepustiti korisnicima djela

- za većinu djela dostupnih na internetu je teško utvrditi autora ili nositelja prava od kojeg trebamo tražiti dozvolu ako želimo upotrijebiti njegovo djelo

- autor ili nositelj prava nas imovinskim iskorištavanjem nekog sadržaja može postaviti uvjete pod kojima će pristati ba upotrebu svog autorskog djela,a da bi se djelom legalno koristilo potrebno je sklopiti licencijski ugovor specificirajući naknadu,opseg korištenja i dr. okolnosti 🡪 to stvara napor i nije oportunitet u današnjem svijetu

- potrebna je brza mogućnost provjere pravnog statusa zaštićenog sadržaja,tj.pravni mehanizam koji može dati odgovor na pitanje pod kojim uvjetima se može koristiti nekim digitalnim sadržajem

- CC je skup licencijskih ugovora dizajniran kako bi potencijalnim korisnicima zaštićenog sadržaja omogućio da brzom provjerom dobiju informaciju pod kojim je uvjetima zaštićeno djelo dostupno za korištenje

- za razliku od GNU licencije, autori CC ugovora naglašavaju kako su sadržaj pojmova,ovlaštenja i određenja objekata i subjekata zaštite koji se u licencijama spominju definirani u skladu s pojmovima u Bernskoj i Rimskoj konvenciji,WIPO-vom Ugovoru o autorskom pravu i Ugovoru o izvedbama i fonogramima te Univerzalnoj konvenciji o autorskom pravu

- CC sustav poznaje 6 formularnih licencijskih ugovora koji su nazvani u skladu s njihovim najvažnijim elementima (CC BY, CC BY-ND, CC BY-NC, CC BY-SA, CC BY-NC-ND, CC BY-NC-SA)

- svih tih 6 licencijskih ugovora sadrže oznaku **BY**, tj. **„Attribution“** – obvezu označavanja autora djela),a razlike proizlaze iz upotrebe kombinacije NoDerivs, NonCommercial i ShareAlike elemenata kojima se uređuju neka od specifičnih ovlaštenja stjecanja licencije u pogledu:

**a)** slobode izrade prerada (derivativnih,izvedenih djela)

**b)** komercijalne upotrebe licenciranih(i/ili izvedenih) djela

**c)** obveze autora derivativnih djela da ih učine dostupnima pod uvjetima pod kojima je dostupno originalno djelo itd.

**7.3. Pravna zaštita baza podataka**

- prema ZAPSP-u **baza podataka je** zbirka samostalnih djela, podataka ili druge građe u bilo kojem obliku, koji su uređeni po određenom sustavu ili metodi i pojedinačno dostupni elektroničkim ili drugim sredstvima, pri čemu bilo postizanje, bilo verifikacija, bilo predstavljanje njezina sadržaja zahtijeva kvalitativno i/ili kvantitativno znatno ulaganje koje se primjerice sastoji u sredstvima, utrošenom vremenu i uloženom trudu

- **proizvođač baze podataka** je pravna ili fizička osoba koja je poduzela inicijativu i rizik ulaganja

- **zaštita baze podataka** je nezavisna od njezine zaštite autorskim pravom ili bilo kojim drugim pravom, pravom proizvođača baze podataka se može slobodno raspolagati

- pravo proizvođača baze podataka ne utječe ni na koji način na autorsko pravo, pravo umjetnika izvođača, pravo proizvođača fonograma, pravo filmskog producenta i pravo organizacija za radiodifuziju

- **predmet zaštite prava proizvođača baza podataka obuhvaća:**

**1)** cjelokupan sadržaj baze podataka

**2)** svaki kvalitativno i/ili kvantitativno znatni dio sadržaja baze podataka

**3)** kvalitativno i/ili kvantitativno neznatne dijelove sadržaja baze podataka kad se ti dijelovi koriste ponavljano i sustavno, pa je to u suprotnosti s redovitim korištenjem baze podataka ili ako neopravdano štete zakonitim interesima proizvođača baze podataka

- **proizvođač baze podataka ima isključivo pravo izvršiti ili odobriti:**

**1)** reproduciranje svoje baze podataka

**2)** distribuiranje primjeraka svoje baze podataka uključujući iznajmljivanje i isključujući javnu posudbu

**3)** stavljanje na raspolaganje javnosti svoje baze podataka

**4)** drugog oblika priopćavanja javnosti svoje baze podataka

- prava proizvođača baze podataka traju **15 godina** od završetka izrade baze podataka, tj. ako je u tom razdoblju baza podataka zakonito objavljena, prava traju 15 godina od takve prve objave

- svaka kvalitativna ili kvantitativna znatna izmjena dijela sadržaja baze podataka, koja je znatno novo ulaganje u kvalitetu ili kvantitetu sadržaja baze podataka, rezultira novim rokom zaštite (znatna izmjena uključuje i postupno dopunjavanje, brisanje i mijenjanje baze)

- i ZAPSP zadržava neka **ograničenja prava proizvođača baze podataka** 🡪 ovlašteni korisnik objavljene baze podataka može se bez odobrenja njezina proizvođača koristiti znatnim dijelovima baze ako je korištenje namijenjeno nastavi i znanstvenom istraživanju uz obvezno navođenje izvora i u mjeri opravdanoj nekomercijalnom svrhom

- ovlašteni korisnik objavljene baze podataka ne može biti spriječen u korištenju neznatnih dijelova njezina sadržaja za bilo kakvu namjenu, ali kad je ovlašteni korisnik ovlašten samo u pogledu dijela baze podataka, ova se odredba primjenjuje samo na taj dio

- ovlašteni korisnik baze podataka stavljene na raspolaganje javnosti ne smije obavljati radnje koje su u suprotnosti s uobičajenim korištenjem te baze ili koje u nerazumnoj mjeri nanose štetu zakonitim interesima njezina proizvođača.

- ovlašteni korisnik baze podataka stavljene na raspolaganje javnosti ne smije nanijeti štetu nositelju autorskog ili srodnog prava u pogledu autorskog djela ili predmeta zaštite koji su sadržani u bazi podataka (npr.učiniti pristup bazi slobodan neovlaštenim korisnicima..)

- o pravu proizvođača se često govori kao o sui generis pravu (ali su različiti)

**7.3.1. Science Commons**

- 2003.g. je na području pravne zaštite baza podataka pokrenut program Science Commons

- ideja tog projekta je bila učiniti dostupnim petabajte podataka nastalih u laboratorijima diljem svijeta (rezultate raznih istraživanja) pohranjenih u privatne baze podataka koje su često nedostupne znanstvenoj i stručnoj javnosti,ne uvijek iz isključivo komercijalnih interesa

**7.4. Pravna zaštita žigova u digitalnom okruženju**

**7.4.1. Općenito**

- **žigovi su** znakovi koji se koriste na tržištu sa svrhom razlikovanja proizvoda ili usluga različitih poduzetnika (Apple – žigovi iPhone, iPad, MacBook, Microsoft – žig Windows, Office 🡪 to su žigovi sadržani u riječima,tj. tekstu, a postoje i grafičke verzije žigova)

- ponekad se za naziv žig koristi brand,ali to nije isto

- znak koji se štiti kao žig može biti iskazan u raznim formama

- svaki žig mora imati **svojstvo razlikovnosti** (naziva se i razlikovni karakter, distinktivnost ili distinktivni karakter)

- svojstvo razlikovnosti je conditio sine qua non postojanja žiga,a znak koji nema ovo svojstvo nije i ne može biti žig

- svojstvo razlikovnosti znači da je znak podoban da bi služio kao sredstvo za razlikovanje proizvoda ili usluga jednog poduzetnika od onih drugih poduzetnika

- **žigovi nastaju na 2 načina:**

**1)** registracijom - Europa

**2)** uporabom određenog znaka u pravnom prometu – SAD

- nositelj žiga ima određena subjektivna prava koja su apsolutna (djeluju erga omnes)

- **Zakon o žigu**

- registrirani žig nositelju daje isključiva prava koja proizlaze iz toga žiga

- nositelj žiga ima pravo spriječiti sve treće strane da bez njegova odobrenja u trgovačkom prometu rabe:

**1.** svaki znak koji je istovjetan s njegovim žigom u odnosu na proizvode ili usluge koje su istovjetne s onima za koje je žig registriran

**2.** svaki znak kad, zbog istovjetnosti s njegovim žigom ili sličnosti njegovu žigu i istovjetnosti ili sličnosti proizvodima ili uslugama obuhvaćenima tim žigom i tim znakom, postoji vjerojatnost dovođenja javnosti u zabludu, što uključuje vjerojatnost dovođenja u svezu toga znaka i žiga

**3.** svaki znak koji je istovjetan s njegovim žigom ili sličan njegovu žigu u odnosu na proizvode ili usluge koji nisu slični onima za koje je žig registriran, kad taj žig ima ugled u Republici Hrvatskoj i kad uporaba toga znaka bez opravdanoga razloga nepošteno iskorištava razlikovni karakter ili ugled žiga ili im šteti

**7.4.2. Povrede žigova u digitalnom okruženju**

- do povreda dolazi u slučajevima neovlaštenog korištenja žigova od strane trećih osoba

- od 2.pol. 90-ih g. do danas, nositelji žigova su se suočili s nekoliko specifičnih povreda svojih interesa (prvo se javlja cybersquatting)

**a) Registracije i korištenja naziva domena u zloj vjeri**

**Cybersquatting**

- označava neovlaštene registracije žigova unutar naziva internetskih domena

- 1 je od najčešćih slučajeva zlonamjernih manipulaccija nazivima domena

- riječ je o slučajevima u kojima neka osoba registrira domenu sa svrhom da je poslije preproda te tako ostvari profit 🡪 nije zabranjeno dok god se ne vrijeđa nečije pravo na osobno ime,žig ili neki drugi zaštićeni naziv,tj.znak

**Typosquatting**

- slučaj u kojem se registrira ime domene koje sadrži neki zaštićeni naziv ili ime namjerno napisano s greškom,najčešće onom koju korisnici inerneta nesvjesno ili iz neznanja znaju napraviti pri tipkanju (npr. ayhoo.com umjesto yahoo.com)

- i ovdje osoba pokušava profitirati iskorištavajući zaštićeni naziv da bi privukla korisnike interneta na svoje web-odredište

**Ometanje poslovanja konkurenata na tržištu**

- cilj takve registracije je da se nanese šteta konkurentu na tržištu ili da se ostvari korist iskorištavanjem njegovih zaštićenih imena ili znakova

- šteta se najčešće nanosi tako da se zauzme ime domene koje sadrži konkurentovu tvrtku, žig ili neki dr.znak i na taj način ga se spriječi u korištenju odgovarajućim imenom domene

- moguće je i da se promet po imenu domene preusmjeri na neko treće web-odredište čiji sadržaj šteti konkurentovoj reputaciji na tržištu

- moguće je ostvarivanje vlastite koristi (osim štete na strani konkurenta) 🡪 čini se tako da se promet po imenu domene koje sadrži konkurentove zaštićene znakove ili imena preusmjeri na vlastito web-odredište i tako privuče potrošače (primjer: amazon.com je tužio grčko trgovačko društvo koje je registriralo naziv domene kao amazon.gr)

**Iskorištavanje tuđe tržišne reputacije**

- registrira se ime domene koja sadrži tvrtku ili žig koji su dobro poznati tržištu kako bi se na web-odredišta privukle osobe koje pretražuju internet u potrazi za proizvodima ili uslugama povezanim s tom tvrtkom,odnosno žigom)

- ta osoba ostvaruje određenu korist i ometa legitimnog korisnika imena domene

**b) Manipulacije prirodnim rezultatima pretraživanja interneta**

- važnost postizanja dobrog ranga u rezultatima pretraživanja je motivirala osobe koje upravljaju web-odredištima da na razne načine pokušavaju usmjeriti korisnike interneta na svoja odredišta, a neki od tih pokušaja su se temeljili na uporabi tuđeg žiga

- do sad se javilo nekoliko tipova manipulacija prirodnim rezultatima pretraživanja uporabom tuđih žigova,a te manipulacije se mogu klasificirati u **3 kategorije** (**s obzirom na način na koji se žigovi neovlašteno koriste**):

**1)** unošenje žigova u meta-tagove web stranica

**2)** njihovo skrivanje u sadržaju web-stranica (keyword stuffing)

**3)** uporaba unutar tzv.farmi linkova (link farming)

- **meta-tagovi** su dio HTML dokumenta u kojima se taj dokument opisuje,a temeljna svrha im je omogućavanje efikasnijeg pretraživanja i klasificiranja tog dokumenta

- do problema je dolazilo kad bi netko u meta-tagove na svom web odredištu stavio pojmove koji su odgovarali tuđem žigu (radnje među konkurentima na tržištu)

*Primjer! Ako poduzetnik A u meta- tagove svog web odredišta postavi pojmove XYZ, koji odgovaraju žigu njegova konkurenta B,onda postoji vjerovatnost da će web-odredište poduzetnika A biti prikazano u rezultatima pretraživanja u slučajevima kada korisnik interneta vrši pretragu na temelju ključne riječi XYZ.*

- može se javiti i **skrivanje pojmova koji odgovaraju žigovima u sadržaj web-stranice**, a u ovom slučaju se pojmovi koji odgovaraju žigovima ne nalaze u dijelu HTML dokumenta, nego u dijelu koji je vidljiv

- da se takva uporaba žiga sakrije postoje razne metode,a jedna je da se tekst postavi u istoj boji u kojoj je pozadina

-uporaba **tzv. farmi linkova** se temelji na činejnici da internetski pretraživači uzimaju u obzir broj linkova koji na određeno web odredište vode s drugih odredišta 🡪 u rezultatima pretraživanja se postavlja veća količina linkova koji upućuju na odredište (postoje posrednici koji izgrađuju tzv. farme linkova kojima se plaća za uslugu)

- ako se ti linkovi sastoje od tuđeg žiga,onda pretraživač odredištu A može dati veći rang u slučajevima kada korisnik interneta vrši pretragu na temelju ključne riječi koja odgovara žigu

- meta-tagovi proizlaze iz Google-a i Bing-a

**c) Manipulacija žigovima u kontekstu internetskog oglašavanja**

- bilo koja osoba može iskoristiti tuđi žig tako da prikaže korisnicima interneta oglase koji ih vode na web odredišta koja nisu povezana s nositeljem tog žiga

- Google gotovo u potpunosti svoje usluge komercijalizira na temelju oglašavanja,a njegov sustav oglašavanja se zove **AdWords**

- AdWords funkcionira jednostavno 🡪 samo se treba prijaviti na Googleov elektronički sustav za oglašivače,definirati elemente oglasa i cijenu za prikazivanje te platiti naknadu

- AdWords omogućava oglašivačima da marketinšku poruku upute preciznije

- najvažniji kriterij na temelju kojeg se definira kontekst unutar kojeg će se oglas prikazivati su ključne riječi koje su mu pridružene

- putem AdWordsa se može ugovoriti oglašavanje na Googleovom pretraživaču,dr. internetskim pretraživačima koji koriste Googleovu tehnologiju i web odredištima trećih osoba koje participiraju u Googleovom programu AdSense

- **AdWords oglas se sastoje od 3 ključna elementa:**

**1)** ključne riječi na temelju kojih se prikazuju

**2)** sadržaj oglasa

**3)** URL-a na koji se korisnik interneta, koji klikne na oglas,usmjerava

- definiranje cijene – oglašivači moraju navesti najvišu „cijenu po kliku“, što je maksimalan iznos koji su spremni platiti za svaki klik na oglas

- postoje situacije u kojima oglašivači odaberu iste ključne riječi za oglase, pa pretraživač prikazuje oglase prema formuli koja uzima u obzir maksimalnu cijenu po kliku, ali i broj koliko puta su korisnici prethodno kliknuli na oglas (popularniji oglas se više prikazuje)

- do problema dolazi kada neki oglašivač za ključnu riječ u oglašavanju odabere riječ koja odgovara tuđem žigu

**7.4.3. Posebno o sporovima o nazivima domena**

- 1999.g. donesen sustav pravnih pravila Uniform Domain Name Dispute Resolution Policy

**Općenito**

- **Uniform Domain Name Dispute Resolution Policy se koristi u** **2 značenja:**

**1)** označava specifičan mehanizam za rješavanje sporova o nazivima internetskih domena

**2)** naziv je jednog od **2 pravna izvora** koji uređuju taj mehanizam:

**a)** Uniform Domain Name Dispute Resolution Policy (*dalje u tekstu UDRP pravila*)

**b)** Rules of Uniform Domain Name Dispute Resolution Policy (*dalje UDRP pravila postupka*)

- UDRP pravila su temeljni izvor materijalnog prava za rješavanje sporova o nazivima internetskih domena, koji su posljedica žigova, u domenskom prostoru generičkih vršnih domena

- procesni aspekti UDRP-a (mehanizam za rješavanje sporova) su uređeni UDRP pravilima postupka

- UDRP se može voditi u krilu nekoliko ovlaštenih ustanova koje imaju vlastita pravila kojima uređuju aspekte UDRP postupka koji se pred njim vode,a koji nisu regulirani UDRP pravilima i pravilima postupka

- procesna pravila nekih UDRP ustanova podređena su UDRP pravilima i pravilima postupka

**Postupak po UDRP-u**

- UDRP postupak se vodi između korisnika spornog naziva domene (**respondent**, **korisnik domene** ) i osobe koja smatra da je registracijom i uporabom spornog naziva domene povrijeđeno njezino pravo iz žiga (**complainant**, **podnositelj zahtjeva**)

- UDRP postupci se organiziraju u krilu organizacija koje ICANN ovlasti za obavljanje tih poslova – **UDRP ustanove**

- **trenutačno ovlaštene UDRP ustanove:**

**a)** Centar za arbitražu i mirenje pri Svjetskoj organizaciji za intelektualno vlasništvo (WIPO centar)

**b)** National Arbitration Forum iz SAD-a (NAF)

**c)** Asia Domain Name Dispute Resolution Centre (ADNDRC)

**d)** Czech Arbitration Court (CAC)

**e)** Arab Center for Domain Name Dispute Resolution (ACDNDR)

- to su sui generis tijela kojima je povjerena nadležnost za vođenje UDRP postupka, a bave se i drugim poslovima rješavanja sporova (arbitraža i mirenje – WIPO, NAF, CAC)

- te ustanove imaju javno objavljenu listu s određenim brojem stručnjaka koji rješavaju spor 🡪 ti stručnjaci se zovu **panelisti**

- UDRP postupak se može voditi pred panelistom pojedincem ili pred vijećem od 3 člana (odlučuje većinom glasova)

- u pravilu, u sporu odlučuje panelist pojedinac kojeg imenuje UDRP ustanova, a vijeće se imenuje ako to zatraži stranka(osoba koja pokreće postupak to traži u UDRP zahtjevu,a korisnik domene u odgovoru na zahtjev)

- proces sastavljanja vijeća počinje tako da svaka stranka sastavi popis od 3 panelista,a ustanova s popisa svake stranke odabire po 1 panelista,a ko ustanova nije u mogućnosti odabrati nekog s liste, odabire ih sama

- trećeg panelista se imenuje tako da UDRP ustanova predloži strankama 5 potencijalnim panelista sa svoje liste i stranke onda izražavaju svoje preferencije,a nakon toga ustanova imenuje 1 od petorice za predsjednika vijeća pri čemu uzima u obzir preferencije stranaka

- panelisti moraju biti nezavisni i nepristrani i on mora iznijeti sve okolnosti ako utvrdi da može doći u pitanje njegiva nepristranost i nezavisnost

- UDRP ustanovi je prepuštena diskrecijska ocjena o tome jesu li iznesene okolnosti opravdane za izuzeće panelista

- pravila postupka ne predviđaju pravo stranaka da zahtijevaju izuzeće panelista,ali bilo je slučajeva

- postupak koji se vodi na temelju UDRP-a je formaliziran te ne daje velike slobode 🡪 sva komunikacija je pismena i odvija se isključivo razmjenom preko elektroničkih sustava za upravljanje postupcima

- UDRP pravila isključuju mogućnost neposrednog saslušanja stranaka uz iznimku ako panelist smatra da je saslušanje potrebno radi rješavanja u premetu

- sadržaj UDRP zahtjeva,opseg podneska i pravna zaštita su ograničeni i uređeni pravilima (određen točno određen obrazac i maksimalan opseg podnesaka)

- u pogledu pravne zaštite, podnositelj zahtjeva je ovlašten tražiti da se pravo korištenja spornim nazivom domene prenese na njega ili da se registracija naziva domene poništi

- kad se registracija domene samo poništi,ista domena postaje slobodna za registraciju te je može ponovno registrirati bilo koja treća osoba (preuzimanjem domene podnositelji zahtjeva se osiguravaju od takve mogućnosti)

- nakon što primi UDRP zahtjev, UDRP ustanova ispituje udovoljava li propisanim formalnim zahtjevima,a u slučaju da postoje nedostaci, ustanova o njima obavještava podnositelja zahtjeva koji ih je dužan otkloniti u roku od 5 dana (ako se prekorači rok, zahtjev se smatra povučenim,ali se može ponovo pokrenuti)

- postupak počinje teći onog dana kada UDRP ustanova dostavi podneseni zahtjev korisniku domene, a **zahtjev se smatra valjano dostavljenim:**

**1)** kada ustanova dobije potvrdu da ga je korisnik stvarno primio

**2)** kada UDRP ustanova poduzme sve pravilima postupka propisane radnje,ispunjenje kojih dovodi do pravne pretpostavke da je dostava uredno izvršena (zahtjeva se da zahtjev bude poslan na sve poštanske adrese koje postoje u registru domena kao i na određene e-adrese za koje se pretpostavlja da ih korisnik domene rabi)

- pokretanje bilo koje od ove 2 okolnosti dovodi do pokretanja roka od 20 dana za dostavljanje odgovora na zahtjev

- postupak po UDRP-u završava donošenjem odluke kojom se zahtjev odbija ili usvaja

- u slučaju usvajanja tužbenoh zahtjeva, naziv domene se prenosi podnositelju zahtjeva ili se poništava registracija naziva domene ( iznimno, panel je dužan donijeti odluku i dostaviti je UDRP ustanovi u roku od 14 dana od dana imenovanja)

- nakon donošenja odluke od strane panela,UDRP ustanova je dužna u roku od 3 dana proslijediti odluku voditelju registracije,strankama i ICANN-u

- ako je određena promjena u statusu naziva domene, voditelj registracije mora prenijeti domenu na podnositelja zahtjeva ili ju izbrisati iz registra nakon proteka 10 dana od njezinog donošenja

- pravilo o troškovima – naknadu za vođenje postupka snosi podnositelj zahtjeva bez obzira na ishod,a iznos naknade varira ovisno o ustanovi i o broju naziva domena o kojima se odlučuje (između 1000 i 1500 $, iznosi skuplji ako sudjeluje vijeće u sporu – ako korisnik domene traži vijeće, dijeli troškove s podnositeljem zahtjeva)

**Materijalnopravne odredbe UDRP pravila**

- **UDRP sadrži** materijalnopravne odredbe (u čl. 4/a UDRP pravila), pravila postupka te neka dodatna pravila regulacije internetskog domenskog prostora

- **osoba koja pokrene UDRP postupak mora dokazati da je:**

**1)** naziv domene istovjetan ili zbunjujuće sličan robnom ili uslužnom žigu na koji ima pravo

**2)** da korisnik naziva domene nema pravo ili legitimni interes u pogledu tog naziva domene

**3)** da je naziv domene registriran i koristi se u zloj vjeri

- podnositelj zahtjeva u UDRP postupku mora dokazati ta 3 uvjeta,tj. zahtjev će biti usvojen samo ako se dokaže da su sva 3 uvjeta ispunjena

- u praksi se razvila specifičnost postojanja prava ili legitimnog interesa korisnika domene

**Odnos naziva domene i žiga**

- **podnositelj zahtjeva mora dokazati:**

**1)** da on ima prava iz žiga

**2)** da je naziv sporne domene istovjetan ili zbunjujuće sličan tom žigu

- UDRP pravila štite sve žigove bez obzira na način stjecanja

- **žigovno pravo funkcionira na načelu teritorijalnosti** koje nema značajnu ulogu u sporovima koji se rješavaju primjenom UDRP-a

- UDRP pravila se primijenjuju u prostoru gener.vrš.domena bez obzira gdje je žig registriran

- nakon što se utvrdi da podnositelj zahtjeva u postupku ima pravo iz žiga, potreno je ispitati odgovara li naziv domene tom žigu u smislu da mu je **istovjetan ili zbunjujuće sličan**

- istovjetnost bi zahtijevala veći stupanj preklapanja između naziva domene i žiga, nego u slučajevima zbunjujuće sličnosti

- UDRP paneli nemaju razloga analizirati radi li se o istovjetnosti ili zbunjujućoj sličnosti 🡪 oba elementa su jedinstveni standard

**Pravo i/ili legitimni interes korisnika domene**

- ako se utvrdi da osoba koja je pokrenula UDRP postupak ima prava iz žiga, pristupa se rješavanju pitanja postojanja prava ili legitimnog interesa na strani korisnika domene 🡪 ako korisnik domene ima pravo ili legitimni interes na korištenje tom domenom, ona mu ne može biti oduzeta u UDRP postupku

- korisnik domene bi imao pravo na korištenje domenom ako bi domena odgovarala njegovu osobnom imenu/imenu tvrtke/žigu/nekom sličnom nazivu u pogledu kojeg korisnik ima subjektivna prava, ali ako nema pravo,moguće je da postoji legitimni interes za korištenje

- određeno korištenje domenom se smatra legitimnim ako ga prihvati tijelo koje odlučuje u UDRP postupku

- odlučivanje UDRP panela nije u potpunosti slobodno jer UDRP pravila imaju smjernice prema kojima se prosuđuje pitanje prava ili legitimnog interesa

- **korisnik domene ima pravo ili legitimni odnos ako se:**

**1)** prije naznake spora koristio ili se spremao koristiti spornim nazivom domene u vezi s bona fide ponudom proizvoda ili usluga

**2)** ako je bio općepoznat po nazivu domene čak i ako nije stekao prava iz žiga

**3)** koristi nazivom domene u legitimne nekomercijalne svrhe ili kao fair use bz namjere da stekne dobit zbunjujućim preusmjeravanjem potrošača ili nanošenjem štete ugledu žiga

- te 3 okolnosti su samo primjeri (mogu se isticati i druge okolnosti)

- na podnositelju zahtjeva je teret dokazivanja svih okolnosti iz čl.4/a , a to uključuje i činjenicu da korisnik domene u pogledu nje nema pravo ni legitimni interes

- od podnositelja zahtjeva se traži da pokaže prima facie da korisnik domene nema pravo ni legitimni interes u pogledu spornog naziva domene 🡪 ako podnositelj uspije u tome, teret dokazivanja se prebacuje na korisnika domene

- od podnositelja zahtjeva se traži da dokaže negativnu činjenicu – da korisnik nema pravo ili legitimni interes (mogućnost iznošenja činjenica je ograničena)

- u UDRP predmetima stranke mogu biti udaljene te podnositelj zahtjeva često neće znati tko je korisnik naziva domene ni njegove motive za registraciju i uporabu te domene, korisnik domene zna činjenice relevantne za rješavanje pitanja

**Registracija i korištenje nazivom domene u zloj vjeri**

- treći uvijet iz materijalnog dijela UDRP pravila je da je korisnik domenu registrirao i koristi se njom u zloj vjeri

- **potrebno je da zla vjera postoji:**

**1)** u trenutku registracije naziva domene

**2)** tijekom njegova korištenja

- UDRP pravila navode nekoliko okolnosti u kojima se smatra da je zla vjera dokazana, a to će biti slučaj ako panel utvrdi da postoje okolnosti koje indiciraju da je ona registrirana:

**1)** sa svrhom da se proda,iznajmi ili na drugi način prenese podnositelju zahtjeva ili njegovom konkurentu za vrijednost koja prelazi troškove koje je imao njezin korisnik

**2)** sa svrhom da se spriječi nositelja žiga da ga koristi u nazivu domene ako na strani korisnika domene postoji obrazac ovakvog ponašanja

**3)** sa svrhom da se ometa poslovanje konkurenta

**4)** ako korisnik naziva domene, pokušavajući privući korisnike interneta na svoje web-odredište radi dobiti,namjerno stvara zabunu u pogledu izvora svog web-odredišta ili njegove povezanosti s nositeljem žiga

**Odredbe o promjeni statusa domene**

- UDRP pravilima se uređuju uvijeti pod kojim voditelj registracije može napraviti promjene u registru naziva domene vezane uz dptični domenu

- najčešće korištena promjena statusa domene je ona koju voditelj registracije poduzima na zahtjev korisnika domene ili od njega ovlaštene osobe (većina voditelja omogućava korisnicima da te promjene naprave sami, elektroničkim putem)

- korisnik naziva domene može bilo kad napraviti promjene u registru naziva domene

- rutinske promjene su one koje se tiču DNS servera na koje domena upućuje,podataka za kontakt korisnika naziva domene ili od njega ovlaštenih osoba za administraciju domene

- bilo kad se u registru može promijeniti identitet registriranog korisnika domene, pri čemu se pravo korištenja domenom prenosi na drugu osobu

- prema čl.8/a, korisnik domene nije ovlašten prenijeti i svoje pravo na drugu osobu za vrijeme trajanja UDRP postupka i 15 dana nakon njegova završetka

- ako se spor rješava arbitražnim ili sudskim putem,pravo korištenja domenom se ne smije prenositi dok traje takav postupak osim ako osoba na koju se domena prenosi potvrdi u pisanom obliku da će biti vezana budućom sudskom ili arbitražnom odlukom

- ako korisnik postupi protivno pravilima o zabrani prijenosa, voditelj reg. je ovlašten otkazati njegovo pravo korištenja domenom

- prema čl. 3/1/b, voditelj registracije je ovlašten napraviti promjenu statusa naziva domene ako primi nalog od strane nadležnog suda ili arbitražnog tijela

- osoba, koja uspije u sporu u postupku,neće morati provoditi složen postupak priznanja odluke stranog suda ili arbitražnog foruma, a koji bi inače bio nužan u slučaju kada se provođenje odluke traži od voditelja registracije koji se nalazi u državi različitoj od one u kojoj je odluka donesena

- prema čl. 3/1/c, voditelj registracije će promijeniti status naziva domene i u slučaju kada primi odluku UDRP panelista kojom se naziv domene prenosi na podnositelja zahtjeva iz UDRP postupka

**b) Arbitražni postupci za rješavanje sporova o nazivima domena unutar .hr vršne domene**

- arbitražna pravila za rješavanje sporova o nazivima domena sadržana su u čl.32.-56. **Pravilnika o ustrojstvu i upravljanju vršnom nacionalnom internetskom domenom**

- spor se vodi između podnositelja zahtjeva i korisnika domene,a razlika od UDRP postupka je u tome tko može biti podnositelj zahtjeva

- .hr arbitražna pravila omogućavaju zaštitu bilo kojeg imena na koje treća osoba ima pravo (pružena zaštita nazivima trgovačkih društava,tvrtkama)

- .hr arbitražna pravila omogućava da se zaštita pruži svakom nazivu u pogledu kojega neka pravna ili fizička osoba ili javnopravni subjekt, ima subjektivna prava koja prepoznaje hrvatsko pravo

- jedina institucija koja organizira .hr arbitražne postupke je **CARNet**

- podnositelj zahtjeva pokreće postupak pisanim putem, slanjem zahtjeva u pisanom obliku poštom,a mora i priložiti potvrdu o uplati predujma troškova postupka

- nakon što primi zahtjev za provođenje arbit. post., CARNet obaviještava korisnika domene

- obavijest o pokretanju postupka se s kopijom zahtjeva šalje preporučenom poštom korisniku domene,a ako ne može tako onda ga se obavještava putem e-pošte (tad se navodi kad i gdje može preuzeti kopiju)

- **Povjerenstvo za .hr** **domenu** može odlučiti da se korisnika kontaktira telefonom/telefaxom

- ako korisnik domene ne odgovori na zahtjev, smatra se da je dostava uredno obavljena u trenutku objave obavijesti o započinjanju postupka na web-stranici dns.hr

- nakon što se zahtjev dostavi korisniku domene pozvat će ga da **u roku od 8 dana** na njega podnese odgovor

- kad se utvrdi da je zahtjev potpun i dopušten i predujam troškova uplaćen, Povjerenstvo za .hr imenuje arbitra, o tome obavještava obje stranke, predaje spis predmeta arbitru te ga poziva da započne s postupkom

- postupak se vodi pred **arbitrom pojedincem**, a mogućnost imenovanja vijeća od 3 člana je predviđeno kao iznimka (izbor arbitra pojedinca vrši Povjerenstvo za .hr domenu)

- arbitri moraju biti nezavisni i nepristrani u odnosu prema strankama u sporu

- moguće je da arbitar uskrati pristanak za vođenje postupka prije njegovog započinjanja ili da zatraži od Povjerenstva za .hr domenu da ga razriješi dužnosti nakon što je postupak započeo ako smatra da postoje ili da su nastale okolnosti koje njegovu nepristranost ili nezavisnost dovode u pitanje (arbitar uvijek dužan iznijeti sve okolnosti)

- stranke mogu zatražiti izuzeće arbitra kad za to postoje važni razlozi,a o tome odlučuje Povjerenstvo za .hr domenu čija je odluka konačna

- arbitar ne može donijeti odluku u predmetu spora prije nego Povjerenstvo odluči o zahtjevu (nakon što bude postavljen zahtjev za izuzećem)

- Povjerenstvo je ovlašteno bilo kad razriješiti arbitra i imenovati drugoga

- Pravilnik 2010 zahtijeva od arbitra da odluku donese u roku od 60 dana od dana preuzimanja predmeta

- u .hr arbitražnim postupcima se plaća fiskalni iznos od 2600 kn

- prema čl.32/2. Pravilnika 2010 se traži:

**1)** da je ime domene isto ili u velikoj mjeri slično nekom imenu na koje treća osoba ima pravo

**2)** da zbog zbunjujućeg učinka istovjetnosti ili velikog stupnja sličnosti imena postoji opravdana opasnost da će značajan broj osoba biti doveden u zabludu

**3)** da korisnik domene nema pravo ili legitiman interes za korištenje domene takvog naziva

**4)** da je korisnik domene registrirao domenu i/ili da je koristi suprotno načelu savjesnosti i poštenja

**7.5. Pravna zaštita topografije poluvodičkih proizvoda**

- kraj 70-ih i poč. 80-ih – razvoj osobnih računala pri čemu presudnu ulogu ima izum **integriranog kruga** koji je sklop elektroničkih komponenti,proizvedenih kao jedinstvena cjelina, u kojem su minijaturni aktivni uređaji (npr. diode i tranzistori) i pasivni uređaji (kondenzatori i otpornici) kao i njihove međusobne veze izgrađeni na tankoj podlozi od poluvodičkog materijala ( obično Si )

- najsloženiji čipovi su mikroprocesori sastavljeni od milijuna ili čak milijardi tranzistora

- danas su poluvodički proizvodi mozak unutar važnih elektroničkih sustava

- kopiranje topografija takvih proizvoda je jednostavan postupak, dok ulaganja u njihov razvoj i unapređenje iziskuju goleme troškove

- sred. 80-ih se pristupilo pravnoj zaštiti poluvodičkih proizvoda

- pravna zaštita topografije poluvodičkih proizvoda odvijala se pod pritiskom SAD-a ( njihov Zakon o poluvodičkim čipovima iz 1984.g. sadržavao je zahtjev o uzajamnoj zaštiti takvih proizvoda i pod njihovim pritiskom EZ donosi **Direktivu o pravnoj zaštiti topografije poluvodičkih proizvoda** 1987.g. )

- u RH zaštita počinje 1999.g. donošenjem Z**akona o zaštiti planova rasporeda integriranih sklopova**, a 2003.g. donijela je **Zakon o zaštiti topografija poluvodičkih proizvoda**

- topografija poluvodičkih proizvoda je prikaz trodimenzionalnog rasporeda slojeva vidljivog, izolacijskog i poluvodičkog materijala u poluvodičkim proizvodima namijenjenima izvođenju određene elektroničke funkcije

- da bi bila predmetom pravne zaštite, mora biti rezultat vlastitog intelektualnog rada njezina stvaratelja i ne smije biti uobičajena u industriji poluvodiča (pri tome se zaštita ne odnosi ni na koji koncept, postupak, sustav,tehniku proizvodnje topografije ili informaciju sadržanu u njoj,već isključivo na samu topografiju

- ako je stvorena u radnom odnosu,a ugovorom nije drugačije određeno,pravo na zaštitu ima poslodavac, a kada je stvorena na temelju ugovora između stvaratelja i naručitelja,a drugačije nije ugovoreno,pravo na zaštitu ima naručitelj

- **redovni put za ostvarenje pravne zaštite** podrazumijeva pokretanje postupka za registraciju topografije od strane stvaratelja

- to čini podnošenjem prijave Zavodu za intelektualno vlasništvo koja mora sadržavati sve elemente koji su propisani Zakonom,a ako je uvijet ispunjen, Zavod će izdati podnositelju **rješenje o registraciji topografije** koja se upisuje **u Registar topografija** i objavljuje u službenom glasilu Zavoda koji je javan)

- prijavu se ne može podnijetinakon isteka roka od 2 godine od datuma početka prvog komercijalnog iskorištavanja topografije

- podnositelj prijave kojem je Zavod izdao rješenje ima **isključivo pravo odobriti ili zabraniti:**

**a)** umnožavanje

**b)** komercijalno iskorištavanje topografije

- njegova su prava vremenski ograničena i prestaju protekom 10 godina od kraja godine kada ju je počeo prvi put komercijalno iskorištavati ili godine u kojoj je podnio prijavu za registrac.

- iznimno, ako nije podnesena uredna prijava a topografija nigdje nije komercijalno iskorištavana, taj rok može biti 15 godina od dana njezina prvog fiksiranja ili kodiranja

- zaštićena topografija osigurava njezinom vlasniku isključivo pravo (u navedenom vremenu) da zabrani ili odobri umnožavanje topografije te uvoz, prodaju i dr. stavljanje u promet topografije ili poluvodičkog proizvoda proizveenog njezinim korištenjem kao i proizvoda u koji je ugrađen poluvodički proizvod koji sadrži zaštićenu topografiju

- nositelj isključivih prava može podnijeti tužbu zbog povrede prava, zahtjev za utvrđenjem i zahtjev za prestankom povrede te zahtjev za naknadu štete

- u svim slučajevim se primijenjuje Zakon o patentu

**8. cjelina: ELEKTRONIČKO POSLOVANJE**

**8.1. Uvod**

- elektroničko poslovanje je omogućilo nove načine poslovne komunikacije,suradnje i razmjene informacija uz unapređenje internih poslovnih odnosa

- razvoj internetskih tehnologija zahtijeva uspostavu odgovarajućeg regulatornog okvira te izgradnju infrastrukture javnog ključa izgradnjom mreže ovlaštenih davatelja usluga certificiranja i osnivanjem registracijskog i nadzornog tijela koje će provoditi registraciju i nadzirati rad davatelja usluga certificiranja

\* ***Infrastruktura javnog ključa je*** *sustav digitalnih certifikata,certifikacijskih vlasti i ostalih ustanova ovlaštenih za registraciju koji provjerava i autentificira fizičke i pravne subjekte uključene u neki internetski posao*

**8.2. Elektroničko poslovanje i automatizacija poslovnih procesa**

- začetke elektroničkog poslovanja nalazimo već u elektroničkom prijenosu novca (kraj 19.st.)

- krajem 60-ih 20.st. se počela razvijati **elektronička razmjena podataka** (Electronic Data InterChange – EDI) – izravan prijenos strukturiranih poslovnih podataka i poruka između računala elektroničkim putem

- svrha elektr.razmjene podataka je da se na računalo primatelja prenesu podaci unaprijed određene strukture koji se mogu obraditi bez izravne intervencije čovjeka (ograničava se na razmjenu poslovnih podataka)

- tijekom vremena u raznim djelatnostima su se počeli primijenjivati razni standardi elektr. razmjene podataka poput X12,TRADACOMS-a i EDIFACT-a (nisu općeprihvaćeni)

- troškovi imlementacije i nepostojanje jedinstvenog standarda se navode kao razlog što br. korisnika nije veći (iako se nekim oblikom EDI-ja koristi izmwđu 200 i 300 tisuća organizacija)

- često se elektr.poslovanje koristi kao sinonim za elektroničku razmjenu podataka ili elekt. trgovanje (e-commerce) 🡪 poistovjećivanje pogrešno

- elektroničko poslovanje ne treba nužno biti povezano s upotrebom interneta, nego se može odvijati unutar zatvorenih,privatnih mreža između ograničenog kruga korisnika

- elektr. poslovanje nije isključivo povezano s gospodarskim subjektima i trgovačkim transakcijama

- **elektroničko poslovanje je** primjena informacijsko-komunikacijskih tehnologija u svrhu podrške svim poslovnim procesima, neovisno o subjektu unutar kojeg se ona primijenjuje ili vrsti poslovne transakcije koja se odvija putem elektroničkih komunikacijskih mreža

- **Manuel Castells** – elektroničko poslovanje su sve poslovne radnje pri kojim se izvedba ključnih operacija upravljanja,financiranja,inovacija,proizvodnje,distribucije,prodaje, odnosa sa zaposlenicima te odnosa s kupcima odvija ili na internetu ili na dr.računalnim mrežama bez obzira na vrstu veze između virtualnih i fizičkih dimenzija tvrtke

- razvoju elektr.poslovanja pridonijeli su i trendovi poput globalizacije,demokratizacije, brzog tehnološkog razvoja,internetizacije, konvergencije tehnologija,digitalizacije podataka te mobilnosti i minijaturizacije informacijskih novih tehnologija

- promjene u RH počinju usvajanjem **Strategije razvitka RH - Hrvatska u 21.stoljeću** 2002.g. u Hrvatskom saboru te se nastavljaju donošenjem **Strategije razvitka elektroničkog poslovanja u RH za razdoblje 2007.-2010.** kojim se želi postići nekoliko **ciljeva:**

**1)** da RH do pristupanja EU uspostavi široku razinu elektroničkog poslovanja radi ravnopravnog sudjelovanja na unutarnjem tržištu EU i sudjelovanja u inform.društvu EU-a

**2)** iskoristiti prednosti koje pruža inform. i komunik. tehnologija te znanje o automatizaciji poslovnih procesa radi povećanja stupnja umreženosti i konkurentnosti hrv. gospodarstva

**3)** povećanje učinkovitosti javnog sektora te pozicioniranje RH kao regionalnog lidera u razvoju i primjeni e-poslovanja

- **elektr. poslovanje je u RH u najužem smislu uređeno :**

**a)** Zakonom o elektroničkom potpisu

**b)** Zakonom o elektroničkoj trgovini

**c)** Zakonom o elektroničkoj ispravi

- postoje i **dr.zakoni koji urešuju to područje:**

**a)** Zakon o zaštiti osobnih podataka

**b)** Zakon o tajnosti podataka

**c)** Zakon o informacijskoj sigurnosti

**d)** Zakon o elektroničkim komunikacijama

**e)** Zakon o zaštiti potrošača

**f)** Zakon o pravu na pristup informacijama

**g)** Zakon o autorskom pravu i srodnim pravima

**h)** Zakon o porezu na dodanu vrijednost

**i)** Zakon o računovodstvu

- **računarstvo u oblaku** je posebna vrsta usluge gdje se korištenje računalnim resursima pruža u obliku usluge koja se dostavlja putem interneta,a korisnici je plaćaju onoliko koliko se koriste (može se pružati kao javna usluga,privatna usluga ili hibridna usluga koja kombinira javni i privatni pristup)

- usluga računarstva u oblaku je skup hardvera,mreža,memorijskog prostora za pohranu podataka,usluga i sučelja koji omogućavaju provedbu računalstva kao usluge

- usluge oblaka uključuju osiguravanje softvera,infrastrukture i prostora za pohranu podataka putem interneta prema zahtjevima korisnika

- **glavne prepreke iskorištavanja svih potencijala računarstva u oblaku su:**

**a)** nedovoljno poznavanje tehnologije

**b)** previsoka cijena usluga

**c)** pravna i zakonska nesigurnost

**d)** sigurnosni rizici

- dokument **Iskorištavanje prednosti elektroničkog fakturiranja za Europu** – Europska komisija predviđa da će do 2020.g. elektr.poslovanje biti dominantan način fakturiranja ( jednak cilj postavlja i **Digitalna agenda za Europu do 2020**.godine )

- **elektronički račun je** najraširenija elektronička isprava u svijetu koja ima središnju ulogu u razvoju elektr.poslovanja i automatizaciji poslovnih procesa (predstavlja razmjenu računa između prodavatelja i kupca u elektr.obliku pogodnom za automatsku obradu)

- kod računa u elektr.obliku je nužno osigurati vjerodostojnost podrijetla,cjelovitost sadržaja i čitljivost računa od trenutka izdavanja do kraja razdoblja za pohranu računa neovisno o tome u kojem je obliku račun izdan, a to je nužan osigurati subjekt koji obavlja isporuku kao i subjekt koji prima isporuku

- subjekt koji isporučuje e-račun mora utvrditi na koji će način osigurati vjerodostojnost podrijetla,cjelovitost sadržaja i čitljivost računa pri čemu mora postojati suglasnost primatelja (to se ostvaruje pomoću elektr.razmjene podataka(EDI-a) ili naprednog e-potpisa)

- **e-račune možemo podijeliti na:**

**a) e-račune u strukturiranoj formi** pogodnoj za automatsku obradu (pomoću HML standarda i EDI-a)

**b) e-račune nestrukturirane forme** (npr.kad se račun šalje e-poštom te se pritom koristi e-potpis, certifikat i vremenski žig)

- račun koji je izrađen u e-obliku pomoću računala,a ne sadrži elemente vjerodostojnosti i cjelovitosti se neće smatrati e-računom nestrukturirane forme

**8.3. Elektronička trgovina (e-Commerce)**

- **elektronička trgovina je** oblik električkog poslovanja pri čemu se koriste inform.-komunik. tehnologije za provedbu transakcije kao što su kupovina,prijenos ili razmjena roba,usluga i/ili informacija putem elektroničkih komunikacijskih mreža

- **s obzirom na dobra kojima se na elektroničkom tržištu trguje,razlikujemo:**

**a) indirektno (neizravno) elektroničko trgovanje** – obuhvaća elektroničku nabavu tjelesnih dobara koja se isporučuju na tradicionalan način

**b) direktno (izravno) elektroničko poslovanje** – podrazumijeva elektroničku narudžbu, plaćanje i isporuku netjelesnih dobara i usluga poput softvera,audiovizualnih sadržaja ili drugih nematerijalnih proizvoda u digitalnom obliku

- e-trgovanje obuhvaća i niz drugih poslovnih aktivnosti koje se odvijaju u online načinu rada putem lokalnih, rasprostranjenih i globalnih mreža,a na taj način su omogućeni brza i jeftina komunikacija,ponuda,potražnja,prodaja,razmjena informacija,itd.

- to je moguće bez neposrednog fizičkog kontakta i posredništva između zainteresiranih stranaka neovisno o njihovoj udaljenosti i vremenu

- **4 temeljna oblika e-trgovine s obzirom na subjekte među kojima se odvija:**

**a)** između gospodarskih subjekata ( business to business, B2B)

**b)** gospodarski subjekti – njihovi kupci (B2C ili C2B)

**c)** između samih kupaca (customer to customer, C2C)

**d)** gospodarski subjekti - javna vlast (B2G ili G2B)

- **mobilno trgovanje (m-commerce)** – ponuda,prodaja i kupnja roba i usluga korištenjem ručnih bežičnih uređaja ka što su pametni telefoni ili tableti

- primjenjujući tehnologije kao što su NFC (Near Field Communication) koja se koristi bežičnom tehnologijom na malim udaljenostima za prijenos informacija, omogućeno je da mobilni uređaji zamijene razna sredstva plaćanja,od gotovine do kreditnih kartica

- Strategija jedinstvenog digitalnog tržišta za Europu – želi se uspostaviti jedinstveno digitalno tržište

- **3 temeljna stupa na kojima počivaju ti zakonodavni prijedlozi:**

**1)** bolji pristup potrošača i poduzeća digitalnim dobrima i uslugama na internetu u Europi

- zakonodavni prijedlozi koji počivaju na ovom stupu uključuju promjene u prekograničnom sklapanju ugovora između potrošača i poduzetnika, revizija pravila za zaštitu potrošača, mjere za poboljšanje dostave robe i usluga, zabrana nepotrebnog blokiranja sadržaja na zemljopisnoj osnovi (geo-blocking),preispitivanje pravila tržišnog natjecanja u e-trgovini i online razmjeni dobara i usluga, reforma autorskopravne zaštite sadržaja,revizija satelitske i kabelske direktive te smanjenje poreznih opterećenja

**2)** stvaranje odgovarajućih uvjeta za procvat digitalnih mreža i usluga

- zakonodavni prijedlozi na ovom stupu uključuju promjene pravila koje uređuju telekomun. tržište,revizija Direktive o audiovizualnim medijskim uslugama,analiza uloge platformi putem kojih se nezakonito dijeli sadržaaj, revizija Direktive o e-Privatnosti te uspostavljanje javno-privatnog partnerstva za kibernetičku sigurnost

**3)** iskorištavanje punog potencijala rasta europskog digitalnog gospodarstva

- na ovom stupu je zasnovana inicijativa za slobodan protok podataka na europskom tržištu, uključujući uspostavu Europskog oblaka,usvajanje standarda i uspostava interoperabilnosti javnih mreža,usvajanje akcijskog plana za elektroničku vlast te uspostavu povezanih poslovnih poslovnih registara

- 2003.g. je donesen Zakon o elektroničkoj trgovini 🡪 tim zakonom je u zakonodavstvo RH implementirana Direktiva 2000/31/EZ o odeđenim pravnim aspektima usluga informacijskog društva,posebno e-trgovine na unutarnjem tržištu kojoj je cilj osigurati uvjete za slobodno kretanje usluga informacijskog društva između država članica EU-a

- ZET uređuje pružanje usluga informacijskog društva,pravila u vezi sa sklapanjem ugovora u e-obliku te odgovornost davatelja usluge informacijskog društva,a njegove odredbe se ne primjenjuju na zaštitu podataka,oporezivanje,javnobilježničku djelatnost,zastupanje stranaka i zaštitu njihovih interesa pred sudovima te na igre na sreću s novčanim ulozima (uključujući lutrijske igre,igre u kasinima,kladioničke igre i igre na sreću u automatima)

**8.3.1. Pružanje usluga informacijskog društva**

- **usluga informacijskog društva** (po ZET) je definirana kao usluga na daljinu koja se pruža,u pravilu uz nakandu, elektroničkim putem i na individualan zahtjev primatelja usluga

- pri korištenjuu takvom uslugom korisnik usluge ne mora nužno plaćati naknadu za korištenje već je moguće da sama usluga za korisnike bude besplatna,a da se njeno financiranje vrši u potpunosti ili djelomično na drugi način

- **u usluge informacijskog društva po ZET-u ubrajamo:**

**1)** internetsku prodaju robe i usluga

**2)** nuđenje podataka na internetu

**3)** reklamiranje putem interneta

**4)** elektroničke pretraživače

**5)** mogućnost traženja podataka i usluga koje se prenose elektroničkom mrežom

**6)** posredovanje u pristupu mreži ili pohranjivanju podataka korisnika

- **davatelj usluga informacijskog društva** je pravna ili fizička osoba koja pruža usluge informacijskog društva te se jamči sloboda obavljanja takvih usluga

- on je dužan postupati i pružati usluge u skladu sa zakonima i dr. propisima RH

- od pravnih subjekata koji ih pružaju ne smije se zahtijevati prethodno odobrenje ili ispunjenje uvjeta istoznačnog učinka,a registracijom pri nadležnom Trgovačkom sudu u RH pravni subjekt mora imati registriranu djelatnost pružanja usluga inform.društva

- ograničenja pružanja usluga inf.društva moguće je jedino prema davateljima takvih usluga sa sjedištem u zemljama članicama EU ako se nanosi šteta ili prijeti opasnost nanošenja štete i to u smislu:

**1)** prevencije,istraživanja,otkrivanja i progona počinitelja kazenih djela,uključujući zaštitu maloljetnika i borbu protiv potianja na mržnju zbog rase,spola,vjere ili nacionalnosti i povrede ljudskog dostojanstva pojedinih osoba

**2)** zaštite javnog zdravlja

**3)** javne sigurnosti,uključujući obranu i nacionalnu sigurnost

**4)** zaštite potrošača,uključujući ulagače

- davatelj usluga informacijskog društva mora u obliku i na način koji je neposredno i stalno dostupan korisnicima i nadležnim tijelima državne uprave Republike Hrvatske pružiti **informacije kao što su:**

**a)** ime i prezime ili tvrtku davatelja usluga

**b)** sjedište obrta ili sjedište pravne osobe davatelja usluga

**c)** ostale podatke o davatelju usluga na temelju kojih korisnik može brzo i nesmetano stupiti s njim u vezu, uključujući elektroničku adresu putem koje je moguće uspostaviti izravan kontakt

**d)** broj sudskog ili drugoga javnog registra u koji je davatelj usluga upisan, te podatke o registru

**e)** pojedinosti o nadležnom tijelu, ako djelatnost davatelja usluga podliježe službenom nadzoru

**f)** porezni broj ako je davatelj usluga obveznik plaćanja poreza na dodanu vrijednost

– **u** **pogledu posebno reguliranih djelatnosti/profesija:**

**1)** profesionalna ili slična institucija kod koje je davatelj usluga registriran

**2)** profesionalni naziv i zemlja koja ga je odobrila

**3)** uputa o profesionalnim pravilima u zemlji u kojoj se obavlja djelatnost i mjestu njihove dostupnosti

- cijene moraju biti jasno i nedvosmisleno naznačene,a posebno se mora naznačiti jesu li u prikazane cijene uključeni troškovi dostave,ostali manipulativni troškovi i drugi troškovi koji na bio koji način utječu na prikazanu cijenu

- davatelj usluge je nužan da svako komercijalno priopćenje bude jasno identificirano u trenutku kada ga korisnik primi,da se osoba u čije je ime takvo priopćenje sastavljeno može jasno identificirati, da svaki promotivni poziv za stavljanje ponude iz komercijalnog priopćenja mora biti jasno identificiran kao takav te da uvjeti koji se moraju ispunjavati za stavljanje ponude iz komercijalnog priopćenja moraju biti lako dostupni te predočeni jasno i nedvosmisleno

**8.3.2. Neželjena komercijalna e-pošta (SPAM)**

- slanje neželjene e-pošte (spamming) je vid neovlaštene upotrebe informacijskog sustava

- cilj počinitelja je poslati što je moguće veći broj poruka e-pošte na stotine tisuća ili milijune e-adresa odjednom,najčešće iz komercijalnih razloga

- zabilježeni su i drugi oblici spama: instant messaging spam,spam na blogovima i wiki stranicama, Usenet grupama, SMS porukama itd.

- prema podacima tvrtke Trend Micro se mjesečno pošalje 50-100 milijardi spam poruka, a godišnje 7 bilijuna što stvara troškove poduzećima i organizacijama u iznosu od 10 milijardi eura zbog izgubljene produktivnosti te troškova nabave softvera i opreme za borbu protiv spama

- **razlozi popularnosti spama:**

**a)** jednostavnost slanja velikog broja poruka u kratkom vremenu

**b)** niski troškovi održavanja

**c)** upravljanje listama elektroničkih adresa (mailing liste)

**d)** manjkava i nedosljedno provedena regulacija protiv slanja spam poruka

- **počinitelji spama se dijele u 2 skupine:**

**a)** organizatori spamemerskih mreža (botnetovi) koji povezuju velik broj inficiranih računala

**b)** korisnici spammerskih mreža

- **botnet** (skraćeno od robot net) je mreža računala kojima pristup i nad kojima kontrolu ima haker,a ne njihovi vlasnici i redovni korisnici

- haker dobiva kontrolu nad računalom slanjem malicioznog programa u okviru poruke e-pošte ili iskorištavanjem ranjivosti operativnog sustava ili programa na korisničkom računu

- botneti služe kao platforma za brzo masovno slanje velikog broja poruka

- korisnici koji se koriste uhodanom mrežom kako bi slali poruke za to naplaćuju najam počinitelja iz prve skupine

- i jedni i drugi često djeluju u okviru skupina organiziranog kriminala 🡪 **prva skupina:** tehnički osposobljeni hakeri, **druga skupina:** red klasičnog organiziranog kriminala koji traže markentiški kanal kojim bi oglašavali prodaju krivotvorene robe,farmaceutskih proizvoda, oružja,droge i dr. proizvoda ograničene,nadzirane ili zabranjene distribucije

- spam poruke slabe povjerenje online korisnika,smanjuju produktivnost,mogu ugroziti sigurnost,širenje nemoralnih i nezakonitih sadržaja

- **ovisno o sadržaju,razlikujemo:**

**a)** netražena komercijalna priopćenja (UCM – unsolicited commercial material)

**b)** netražena nekomercijalna priopćenja (UNM - unsolicited non-commercial material)

- u borbu protiv spam-a su se uključile i međunarodne organizacije poput OECD-a i UN-a 🡪 jačanje svijesti korisnika,usklađivanje zakonodavstva i promocija naprednih tehničkih sredstava za borbu protiv spama

- **razlikujemo nekoliko mogućnosti regulacije:**

**1) potpuna zabrana** – spaming je ilegalan dok god nema osnove za njegovo opravdanje

**2) eksplicitni opt-in-sustav** – spaming je zabranjen dok god nema izričitog pristanka primatelja prije nego se pošalje prvo priopćenje (spamer mora čak provjeriti je li pristanak doista dao primatelj – **dvostruki opt-in sustav**)

**3) opt-in-sustav** – spaming je ilegalan dok nema bezuvjetnog pristanka primatelja

**4) prvi-slobodni-sustav** – spamer može tražiti pristanak slanjem poruke primatelju i samo ako on to odobri,spaming je dozvoljen

**5) imlicitni prvi-slobodni-sustav** – spamer može tražiti pristanak slanjem poruke primatelju i samo ako on ne odobri spaming je dozvoljen

**6) registracijski opt-out-sustav** – spaming je dozvoljen sve dok primatelj nije prigovorio individualno pošiljatelju

**7) opt-out-sustav** – spamming je dozvoljen sve dok primatelj nije prigovorio individualnom pošiljatelju

**8)** **spamming je potpuno legalan**

- karakterizaciju slanja spama uređuju KZ i ZEK

- čl.267. KZ-a – ometanje rada računalnog sustava (kazna do 3 godine)

- čl.107. ZEK-a ( Neželjena elektronička komunikacija) – upotreba automatskih pozivnih i komunikacijskih sustava, SMS i MMS poruka u svrhu promidžbe i prodaje dopuštena je samo uz prethodno pribavljenu privolu pretplatnika ili korisnika usluga

- fizička ili pravna osoba trgovca može upotrebljavati podatke o adresama e-pošte koje je pribavila u svrhu prodaje proizvoda i usluga uz uvjet da ti potrošači imaju jasnu i nedvojbenu mogućnost besplatnog i jednostavnog prigovora na takvu uporabu podataka o adresama e-pošte u slučaju da potrošač nije unaprijed odbio takvu uporabu podataka

- zabranjeno je i slanje e-pošte,uključujući SMS i MMS poruke, u kojima se pogrešno prikazuje ili prikriva identitet pošiljatelja u čije se ime šalje e-pošta ili poruka i koja je protivna posebnim propisima o e-trgovini

- zabranjeno je i slanje e-pošte ili poruka bez ispravne adrese e-pošte ili broja na koji primatelj može,bez naknade,poslati zahtjev za sprječavanje daljnje komunikacije određujući da se navedene odredbe ne odnose na pozive pravnim osobama u svrhu izravne promidžbe i prodaje

- ponašanja opisana u čl.107. ZEK-a ne smatraju se neželjenom e-komunikacijom ako su upućene iskključivo pravnim osobama,za razliku od poruka upućenih fizičkim osobama

- u hrvatskom zakonodavstvu je načelno na snazi opt-in-sustav uz iznimke (opt-out sustav vrijedi za pravne osobe)

- ZEK određuje da operatori usluga e-pošte moraju pretplatnici tih usluga omogućiti filtriranje dolazne e-pošte koja sadržava neželjene e-pošte ili štetan sadržaj

- pretplatnicima se mora omogućiti jednostavan način oblikovanja,uključivanja i isključivanja takvih filtara,a operatori usluga e-pošte moraju na prikladan i javno dostupan objaviti adresu e-pošte za prijavu zlouporaba te odgovoriti na svaki prigovor u vezi sa zlouporabom e-pošte u roku od najviše 15 dana od dana zaprimanja tog prigovora putem e-pošte

- operatori su dužni pretplatničkim ugovorom obvezati svoje pretplatnike na zabranu slanja neželjenih e-poruka te na poduzimanje odgovarajućih mjera radi sprječavanja zlouporaba pretplatnikova korisničkog računa e-pošte

- kada operator zaprimi dokaz da je pretplatnik poslao neželjenu e-poruku ili da je pretplatnikov korisnički račun e-pošte bio zlouporabljen,obvezan je utvrditi činjenično stanje i poduzeti odgovarajuće mjere (mjere ovise o stupnju počinjene zlouporabe, pa operator može izdati upozorenje ili privremeno onemogućiti uporabu pretplatnikova korisničkog računa e –pošte bez odgode,u pisanom obliku obavijestiti pretplatnika)

- ako pretplatnik ne ispunjava obveze utvrđene pretplatničkim ugovorom,operator ima pravo trajno izbrisati pretplatnikov korisnički račun e-pošte i raskinuti pretplatnički ugovor u skladu s općim uvijetima poslovanja

- ZEK određuje da se odredbe ne primijenjuju na pretplatnike za koje je utvrđeno da je zloporabu pripadajućeg korisničkog računa e-pošte prouzročila treća strana, osim u slučaju kad se pretplatnik oglušio na opetovana upozorenja operatora za poduzimanje mjera zaštite

**8.3.3.. Pravila u vezi sa slapanjem ugovora u elektroničkom obliku**

- primijenjuju se odredbe ZET-a i ZOO-a (Zakon o obveznim odnosima)

- čl.293. ZOO-a - ugovor je sklopljen elektroničkim putem kad su se strane suglasile o bitnim sastojcima te ponuda učinjena elektroničkim putem smatra se ponudom nazočnoj osobi, ako se u konkretnom slučaju može na izjavu odmah dati protuizjava

- uporaba elektroničkog potpisa prilikom sklapanja ugovora uređuje se posebnim propisima, a to su ZET i ZEP

- **ugovori u elektroničkom obliku** (po ZET-u) su ugovori što ih pravne i fizičke osobe u cijelosti ili djelomično sklapaju, šalju, primaju, raskidaju, otkazuju, pristupaju i prikazuju elektroničkim putem koristeći elektronička, optička ili slična sredstva, uključujući, ali ne ograničavajući se na prijenos Internetom

- nije moguće osporavanje pravne valjanosti takvih ugovora samo na temelju činjenice da je sastavljen u elektroničkom obliku

- **odredbe ZET-a neće se primjenjivati na sljedeće ugovore:**

**a)** imovinske, predbračne, odnosno bračne ugovore i druge ugovore koje uređuje Obiteljski zakon

**b)** ugovore o opterećenju i otuđenju imovine za koje je potrebno odobrenje centra za socijalnu skrb

**c)** ugovore o ustupu i raspodjeli imovine za života, ugovore o doživotnom uzdržavanju, ugovore o dosmrtnom uzdržavanju i sporazume u vezi s nasljeđivanjem, ugovore o odricanju od nasljedstva, ugovore o prijenosu nasljednog dijela prije diobe, oporučne poslove i druge ugovore koje uređuje Zakon o nasljeđivanju

**d)** darovne ugovore

**e)** ugovore o prijenosu prava vlasništva na nekretninama ili druge pravne poslove kojima se uređuju stvarna prava na nekretninama, osim ugovora o najmu i zakupu nekretnina

**f)** druge ugovore za koje je posebnim zakonom propisano da se sastavljaju u obliku javnobilježničkog akta, odnosno isprave

**g)** ugovore i očitovanja volje jamaca, ako je jamac osoba koja djeluje izvan svoje trgovačke, poslovne ili profesionalne djelatnosti

*Primjer! Sklapanje kupoprodajnog ugovora e-putem između neke inetrentske trgovine (web shopa) i krajnjeg kupca*

*- internetska trgovina prema ZET-u je usluga informacijskog društva*

*- prije same prodaje dobara,tj.prije nego se sklopi ugovor u e-obliku pružatelj usluge je dužan potencijalnom kupcu osigurati na jasan,razumljiv i nedvosmislen način podatke o raznim stupnjevima koji slijede u postupku sklapanja ugovora*

- današnje inetrnetske trgovine imaju jadno naznačene korake koji slijede pri kupnji dobara koji se nude te pružatelj usluge mora upoznati kupca s ugovornim odredbama i općim uvijetima poslovanja te na kojim jezicima ugovor može biti sklopljen

- to se čini javnom objavom na internetskoj stranici trgovine jer moraju biti dostupni kupcu

- njima se definiraju prava i obveze pružatelja usluge i kupca (mogućnost raskida ugovora, povrat sredstava,vrijeme dostave,otklanjanje nedostataka,itd.)

- davatelj usluga informacijskog društva mora bez odgode elektroničkim putem, posebnom elektroničkom porukom, potvrditi primitak elektroničke poruke koja sadrži ponudu ili prihvat ponude za sklapanje ugovora

- ugovor u elektroničkom obliku sklopljen je onoga trenutka kad ponuditelj primi elektroničku poruku koja sadrži izjavu kupca da prihvaća ponudu

- za neke vrste ugovora je moguće kao pretpostavku valjanosti i samog nastanka ugovora zahtijevati potpis ugovornih strana,a ako je riječ o skalapnju takve vrste ugovora u e-obliku, vlastoručni potpis je moguće zamijeniti e-potpisom u skladu s ZEP-om

**8.3.4. Odgovornost davatelja (posrednika) usluga informacijskog društva u pristupu mreži ili pohranjivanju podataka korisnika**

- davatelj usluga inf.društva ima ulogu posrednika u pristupu mreži ili pohranjivanju podataka korisnika,a takvu vrstu usluga najčešće pružaju **davatelji internetskih usluga** (Internet Service Provider, ISP) – imaju specifičan položaj o pitanju odgovornosti za preneseni i pohranjeni sadržaj

- njihova odgovornost je regulirana Direktivom o elektroničkoj trgovini EU-a 2000/31/EZ člancima 12.-15. što odgovara čl.16.-21. ZET-a

- **specifične usluge koje posrednici** **pružaju** podrazumijevaju prijenos podataka trećih osoba u mreži (mere conduit),prijenos i privremenu pohranu informacija trećih radi učinkovitijeg daljnjeg procesa drugim primateljima usluge na njihov zahtjev (caching) i usluge smještaja informacija na poslužitelju (hosting)

- pružanje takvih usluga u odnosu na sadržaj mora biti neutralno,tj.sami posrednici ne bi trebali imati nikakav utjecaj na sadržaj koji prenose ili pohranjuju

- usluga gdje posrednici imaju **isključivu ulogu prijenosnika informacija (mere conduit)** se sastoji od prijenosa informacija korisnika ili od pružanja pristupa mreži i podacima

- davatelj usluga informacijskog društva koji prenosi elektroničke poruke koje mu je predao korisnik usluga nije odgovoran za sadržaj poslane poruke i njezino upućivanje, a **pod uvjetom:**

**1)** da nije inicirao prijenos

**2)** da nije izvršio odabir podataka ili dokumenata koji su predmet prijenosa

**3)** da nije izuzeo ili preinaĉio podatke u sadržaju poruka ili dokumenata

**4)** da nije odabrao korisnika prijenosa

- pružanje usluga pristupa mreži ili prijenosa podataka mora biti obavljeno na način da omogućuje automatsku,posredničku i privremenu pohranu podataka,ali samo ako je ta pohrana nužna zbog prijenosa u komunikacijskoj mreži te pod uvjetom da se informacije ne pohranjuju dulje no što je to razumno nužno za svrhu prijenosa te da sam posrednik nema znanje ni kontrolu nad prenesnim informacijama

- to se pravilo jednako odnosi na prijenos e-pošte,razmjenu poruka unutar sustava za automatsku razmjenu podataka(EDI) ili na sadržaj koji se prenosi u svrhu postavljanja i pohranjivanja na poslužitelje posrednika

- posrednici ne odgovaraju za sadržaj koji prenose,a sadržajno ga ne mijenjaju pri čemu se tehničke manipulacije sadržaja tijekom prijenosa ne smatraju mijenjanjem sadržaja

- posrednici će snositi odgovornost za nezakonite informacije,tj.radnje korisnika ako s njima surađuju s namjerom poduzimanja nezakonitih radnji

- 2.specifična vrsta usluga koju posrednici pružaju je **privremeni smještaj informacija (caching)** – usluga automatske,privremene i prolazne pohrane informacija koja je izvršena isključivo u svrhu učinkovitijeg daljnjeg prijenosa informacija prema ostalim primateljima usluge na njihov zahtjev

- **za tako pohranjene informacije je isključena odgovornost posrednika pod uvjetom da:**

**1)** ne mijenja podatke

**2)** uvažava uvjete za pristup podacima

**3)** postupa u skladu s pravilima za ažuriranje podataka

**4)** djeluje u skladu s dopuštenom primjenom tehnologija za prikupljanje podataka

**5)** trenutačno ukloni ili trenutačno onemogući pristup podacima koje je pohranio odmah čim je saznao da su podaci u polazištu uklonjeni iz prijenosa putem mreže ili je onemogućen pristup do njih ili je sud ili drugo nadležno tijelo naredilo njihovo uklanjanje ili onemogućavanje pristupa

- 3. specifična usluga koji posrednici pružaju je **smještaj informacija na poslužitelju (hosting)** – usluga putem koje korisnici na vlastiti zahtjev pohranjuju informacije na poslužitelje posrednika

- **odgovornost posrednika za tako pohranjene sadržaje isključena je ako sam posrednik:**

**1)** ako nema saznanja niti je mogao znati o nedopuštenom djelovanju korisnika ili sadržaju podataka

**2)** ako odmah čim je saznao ili postao svjestan da se radi o nedopuštenom djelovanju ili podatku ukloni ili onemogući pristup podacima

- ta pravila se neće primijeniti u slučajevima kada je korisnik usluge osoba povezana i ovisna na bilo koji način o davatelju usluge (npr. trgovačka društva koji imaju udjele jedno u drugome, trgovačka društva u kojima udjele imaju iste fizičke osobe)

- ako posrednici na vrijeme ne uklone nezakonit sadržaj sa svojih poslužitelja,posrednici mogu snositi kaznenopravnu,tj. građanskopravnu odgovornost u vezi s navedenim sadržajem

- **ZET isključuje odgovornost posrednika za informacije koje se učine dostupnim putem upućivanja (linkinga) u slučajevima ako posrednik:**

**1)** ako nema saznanja niti je mogao znati o nedopuštenom djelovanju korisnika ili sadržaju podataka, kao i o sudskim postupcima vezanim za naknadu štete koja bi proizlazila iz nedopuštenog djelovanja korisnika ili sadržaja pohranjenih podataka i ako nije bio niti mogao biti upoznat sa činjenicama ili okolnostima iz kojih bi nedopuštena aktivnost korisnika bila očigledna

**2)** ako odmah čim je saznao ili postao svjestan da se radi o nedopuštenom djelovanju ili podatku ukloni ili onemogući pristup podacima

- slučaj internetske stranice The Pirate Bay – riječ je o postavljanju linkova koji omogućavaju nezakonito dijeljenje sadržaja (ponajprije programskih i audiovizualnih sadržaja zaštićenih autorskopravnom zaštitom) putem peer-to-peer sustava *(pročitati slučaj na 306.str.)*

**8.3.5. Obveze posrednika**

- na temelju Direktive 2000/31/EZ države članice mogu nametnuti i pojedine obveze davateljima usluga informacijskog društva na trenutačno obavještavanje nadležnih tijela vlasti o navodno nezakonitim radnjama

- **specifične obveze koje su nametnute posrednicima prema ZET-u omogućuju:**

**1)** obvezu da odmah po saznanju obavijeste nadležno državno tijelo ako utvrde postojanje osnovne sumnjeda korištenjem njegove usluge korisnik poduzima nedopuštene aktivnosti i/ili pruža nedopuštene podatke

**2)** obvezu da na temelju odgovarajućeg sudskog ili upravnog akta predoče sve podatke na temelju kojih se može poduzeti otkrivanje ili progon počinitelja kaznenih djela,tj.zaštita prava trećih osoba

- Direktiva i ZET ne podrazumijevaju nametanje općeg nadzora od strane posrednika u pogledu sadržaja i/ili informacija,a isključena je i mogućnost nametanja aktivne uloge posredniku u traganju za činjenicama ili okolnostima koje bi upućivale na nezakonite aktivnosti

- sudovi i druga nadležna tijela na zahtjev ovlaštene osobe, nalažu davateljima usluga informacijskog društva i njihovim korisnicima otklanjanje i sprječavanje povreda važećih propisa, te da prema njima poduzimaju i druge na zakonu zasnovane mjere

- **mjera filtriranja prometa je** mjera po kojoj bi posrednik bio dužan filtrirati komunikaciju svih korisnika njegove usluge radi npr. identifikacije sadržaja s djelima zaštićenih autorskim pravom i eventualnog naknadnog sprečavanja njihova prijenosa

- primjer slučaja u kojem je sud naložio davatelju usluge mjeru filtriranja je slučaj C-70/10 Scarlet Extended SA v SABAM *(pročitati slučaj na 307.str.)*

- Europski sud je u tom slučaju utvrdio da sustva filtriranja podrazumijeva aktivno promatranje svih e-komunikacija koje se prenose putem mreže davatelja usluge i da su pod nadzorom sve informacije koje će se prenositi kao i korisnici koji se mrežom koriste

- riječ je o općem nadzoru koji bi davatelj usluge pristupa interneta aktivno i trajno morao poduzimati kako bi spriječio povredu prava intelektualnog vlasništva

**8.4. Elektronički potpis**

- e-potpis je ključan dio e-trgovine bez kojeg je ona pravno nesigurna i nepouzdana

- čin stavljanja potpisa,osobnog pečata ili kakvog drugog osobnog traga na ispisani dokument se stoljećima smatra temeljnim uvjetom nastanka presumpcije slaganja potpisnika sa sadržajem isprave

- **bez potpisa,isprava nema pravnu snagu!!**

**8.4.1. Važnost elektroničkog potpisa za elektroničko poslovanje**

- e-potpis podrazumijeva i upotrebu e-certifikata

- e-potpis u širem smislu obuhvaća i e-potpis užem smislu kao metodu zaštite sadržaja elektroničkog dokumenta ili e-komunikacije te e-certifikat čija je uloga pouzdano utvrditi identitet neke pravne ili fizičke osobe

- e-potpis u užem smislu i e-certifikat čine funkcionalnu cjelinu

- e-potpis je važan za legalizaciju rada elektroničkih agenata (definira ih UETA 1999.g.)

- osnovni zadatak e-potpisa je potvrđivanje izvornosti,tj.autentičnosti potpisnika i sadržaja potpisane komunikacije

- potrebno je pravno izjednačiti učinke e-potpisa i vlastoručnog potpisa

- prvi Zakon o informatičkoj djelatnosti u RH je donesen 1977.g.

**8.4.2. Tehnička infrastruktura elektroničkog potpisa**

- **infrastruktura javnog ključa** (PKI) je složena informacijska infrastruktura čija je svrha osigurati pouzdano i neporecivo identificiranje korisnika e-komunikacija

- PKI se temelji na upotrebi **asimetrične kriptografije** (kriptografska metoda zasnovana na algoritmima koji koriste 2 ključa – **javni ključ** dostupan svima putem same komunikacijske infrastrukture i **privatni ključ** poznat samo korisniku) – javni i privatni ključ su različiti kod asimetrične kriptografije

- svaki korisnik PKI-ja ima svoj javni i privatni ključ

- **simetrična kiptografija** se zasniva na upotrebi 1 ključa koji znaju samo sudionici komunikacije

- javni i privatni ključ su povezani složenim matematičkim algoritmom

- za krajnjeg korisnika je jednostavno stvoriti javni i privatni ključ,a neovlašteni korisnik ne može jednostavno doći do tajnog provatnog ključa(osim krađom ili socijalnim inženjeringom)

- naknadno određivanje privatnog ključa na temelju poznatog javnog je nerješiv problem, pa zbog toga objava javnog ključa ne prestavlja sigurnosni rizik

- autorizacija PKI-jem se koristi za osiguranje e-komunikacije preko otvorenih mrežnih sustava (kao interneta),a to ne zahtijeva poseban,tajni komunikacijski kanal kojim se neovlašteni korisnici ne mogu koristiti jer mu nemaju pristup,već se komunikacija šalje putem otvorenog kanala gdje ih je moguće presresti i zabilježiti,ali ne i razumijeti

- ako je komunikacija zaštićena asimetričnom kriptografijom i složenim ključem, njen sadržaj će ostati tajan

- **2 najčešće svrhe korištenja PKI-ja :**

**1)** zaštita povjerljivosti e-komunikacije

**2)** kao osnova e-potpisa

- u slučaju osiguranja e-komunikacije,poruka se kriptira (šifrira) s primateljevim javnim ključem,pa je jedino ovlašten primatelj (jedini zna odgovarajući privatni ključ) sposoban dekriptirati takvu poruku

- u slučaju e-potpisa, poruka se kriptira s pošiljateljevim privatnim ključem,a svatko tko ima pristup pošiljateljevom javnom ključu može provjeriti da je pošiljatelj zaista upotrijebio odgovarajući privatni ključ te da je riječ o autentičnom pošiljatelju

- sustav će provjeriti i je li poruka u međuvremenu promijenjena

**8.4.3. Elektronički potpis u poredbenom pravu**

- zakonodavac je za ZEP inspiraciju crpio iz dokumenta EU i iz nekih multilateralnih međunarodnih organizacija poput WTO-a ili UNCITRAL-a

- 1996.g. UNCITRAL-ov model zakona o e-trgovini (uređuje pitanje primjene e-potpisa na području trgovine) je ipak definirao pojmove e-potpisa,certifikata i pružatelja usluge certificiranja i dr. na tehnološki neutralan način

- **tehnološka neutralnost obuhvaća 2 aspekta:**

**1)** odnosi se na usporedbu on-line i off-line aktivnosti,tj. poduzimanje neke pravne radnje e-putem ili klasičnom komunikacijom (niti jedna od ove 2 aktivnosti se ne smije diskriminirati)

**2)** drugi aspekt se sastoji u zahtjevu da se ne preferira određeno tehnološko rješenje,tj. pravni propisi bi trebali biri sročeni na način da se ne favorizira ili diskriminira neku tehnol.)

- tehnološka neutralnost je nužan uvjet postizanja pravne sigurnosti i učinkovito osiguravanje propisa na budućnost kada trenutno aktualna tehnologija možda neće biti u upotrebi

**a) Prva generacija zakona o elektroničkom potpisu**

- prvi zakon koji definira pojam i efekte e-potpisa je **Digital Signature Act** (Utah, 1995.g.) 🡪 presumirana uporaba arhitekture javnog i privatnog ključa kao temelja infrastrukture e-potpisa (ne vodi računa o tehnološkoj neutralnosti)

- 1997.g. - njemački Zakon o digitalnom potpisu i talijanski Bassinijev zakon

- 1 od prvih zakonskih prijedloga je bio UNCITRAL-ov model zakona o e-potpisu, zatim i US Federal Electronic Signatures in Global and National Commerce (2000.g.) i zakon savezne države Kalifornije 🡪 nisu prejudicirali upotrebu tehnologija javnog i privatnog ključa

- određenje specifične tehnologije na razini općeg propisa može značiti pouzdanost u razinu tehničke zaštite koja pruža višu razinu pravne sigurnosti korisnicima

- apstraktnija norma znači jednostavniju mogućnost usvajanja budućih tehnologija koje se mogu pojaviti bilo kad bez potrebe za zakonodavnim izmjenama

**b) Druga generacija zakona o elektroničkom potpisu**

- **cilj druge generacije propisa** je pomiriti oba prijašnja pristupa,tj.preuzeti najbolje strane i od 1 i od 2 što je dovelo do tzv. dvostrukog kolosijeka,odnosno definiranja 2 zasebne vrste e-potpisa, običnog i naprednog koji se razlikuje po uvjetima nastanka i pravnom učinku

- ključnu ulogu u promoviranju dvostrukog kolosijeka je odigrao europski zakonodavac nadoknađujući zaostatak prema zemljama razvijenije e-trgovine (SAD,VB,Njemačka)

- snažan razvoj američkog gospodarstva krajem 90-ih 20.st. (tzv. Dotcom boom) je potaknuo EU na intezivan zakonodavni napor da bi se europski pravni okvir prilagodio novim okolnostima

- u kratkom vremenu,tijela EU su pripremila nekoliko dokumenata koji su trebali promovirati e-trgovinu kao aktivnost od najvišeg interesa za gospodarstvo EU

- središnju ulogu je imala **Direktiva o elektroničkoj trgovini** čiji je cilj bio stvoriti pravni okvir e-trgovine u Europi baziran na načelima slobodnog tržišta, štiteći javni interes

- nastanak Direktive je potakla različita praksa rješavaja sporova koji su nastajali na području e-trgovine u pravnim porecima zemalja članica

- poč. 2000.g. na snagu stupa **Direktiva o elektroničkom potpisu** 1999/93/EC čiji je zadatak stvoriti jedinstveni zakonodavni okvir za primjenu e-potpisa na području EU

- osnovna ideja Direktive je razlikovanje **2 tipa e-potpisa :**

**a)** elektronički potpis (osnovni)

**b)** napredni elektronički potpis

- direktiva uvodi i pojam kvalificiranog certifikata

- čl.5. Direktive određuje da zemlje članice neće uskratiti e-potpisu mogućnost ostvarivanja pravnih učinaka i upotrebe e-potpisa kao dokaza u pravnim postupcima samo zato jer je potpis dan u e-obliku,potpis nije baziran na kvalificiranom certifikatu izdanom od strane ovlaštenog certifkacijskog tijela ili potpis nije učinjen putem posebnog uređaja za stvaranje e-potpisa

- 2001.g. - njemački Gesetz uber Rahmenbedingungen fur elektronische Signaturen (i druge zemlje donose zakone)

**8.4.4. Zakon o elektroničkom potpisu**

- usvojen 2002.g.,a doneseni su i rpavilnici koji detaljnije reguliraju ZEP

- osnovni zadatak ZEP-a je urediti pravni okvir korištenja e-potpisom, tj. ustrojiti sustav potvrđivanja izvornosti i autentičnosti e-komunikacije bez kojeg nema pouzdanog e-poslovanja, e-trgovine,a ni e-komunikacije građana prema tijelima države

- neke vrste usluga (npr. internet bankarstvo) se koriste posebnim uređajima, **tokenima**, kako bi osigurali autentifikaciju svojih korisnika i njihovih interakcija s bankarskim sustavom

- nakana hrvatskog zakonodavca je bila zakonom propisati i usvojiti prihvaćen sustav e-potpisa zasnovan na tehnologiji infrastrukture javnoh ključa (PKI)

- **odabir PKI ima za cilj:**

**1)** stvoriti povjerenje poslovne zajednice i najšire javnosti u pouzdanost upotrebe e-potpisa u svakodnevnom poslovanju te potaknuti njegovu najširu primjenu

**2)** urediti prava,obveze i odgovornosti fizičkih i pravnih osoba u vezi s pružanjem usluga certificiranja e-potpisa

- **PKI sustav e-potpisa** podrazumijeva mrežu certifikacijskih tijela koje će voditi računa o ispravnosti korisničkog certifikata (po ZEP-u)

**8.4.5. Zakonska definicija pojma elektronički potpis i drugih pojmova**

- **elektronički potpis je** skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koji služe za identifikaciju potpisnika i vjerodostojnosti potpisanoga elektroničkog dokumenta

- **napredan elektronički potpis je potpis koji:   
  
1)** je povezan isključivo s potpisnikom   
  
**2)** nedvojbeno identificira potpisnika  
  
**3)** nastaje korištenjem sredstava kojima potpisnik može samostalno upravljati i koja su isključivo pod nadzorom potpisnika   
  
**4)** sadržava izravnu povezanost s podacima na koje se odnosi i to na način koji nedvojbeno omogućava uvid u bilo koju izmjenu izvornih podataka

- ZEP uređuje kako napredni e-potpis ima istu pravnu snagu i zamjenjuje vlastoručni potpis i otisak pečata na elektroničkom dokumentu ako je izrađen u skladu s odredbama Zakona te ako su ispunjeni ostali uvjeti propisani Zakonom i propisima donesenima na temelju ZEP-a

- **nije dopušteno osporavanje elektroničkog potpisa samo na osnovu toga što:**

**a)** je u elektroničkom obliku

**b)** nije zasnovan na kvalificiranom certifikatu

**c)** nije zasnovan na kvalificiranom certifikatu koji izdaje akreditirani davatelj usluga certificiranja

**d)** nije izrađen uporabom sredstva za izradu naprednoga elektroničkog potpisa

**8.4.6. Pojam i uloga vremenskog žiga (digitalnog vremenskog biljega) i elektroničkog zapisa**

- pojam vremenskog žiga uveden izmjenama 2008.g.

- **vremenski žig ili digitalni vremenski biljeg je** metoda označavanja nastanka elektroničkog dokumenta i bilježenja promjena njegova sadržaja tijekom vremena,tj. riječ je o mehanizmu provjere kada je digitalni dokument kreiran,odnosno promijenjen

- **ZEP definira vremenski žig** kao elektronički potpisanu potvrdu izdavatelja koja potvrđuje sadržaj podataka na koje se odnosi u navedenom vremenu, a **napredan vremenski žig je** elektronički potpisana potvrda ovjerovitelja koja ispunjava uvjete za napredan elektronički potpis

- elektronički zapis je cjelovit skup podataka koji su elektronički generirani, poslati, primljeni ili sačuvani na elektroničkom, magnetnom, optičkom ili drugom mediju, a sadržaj elektroničkog zapisa uključuje sve oblike pisanog i drugog teksta, podatke, slike i crteže, karte, zvuk, glazbu, govor, računalne baze podataka

**8.4.7. Potpisnik elektroničkog potpisa**

- **potpisnik e-potpisa je** osoba koja posjeduje sredstvo za izradu e-potpisa kojim se potpisuje, a koja djeluje u svoje ime ili u ime fizičke ili pravne osobe koju predstavlja

- **e-potpisom se može služiti** svaka fizička osoba u vlastito ime kao i osobe ovlaštene na zastupanje pravnih osoba ili drugih fizičkih osoba

**8.4.8. Sredstva i podaci za izradu elektroničkog i naprednog elektroničkog potpisa**

- za izradu e-potpisa su potrebna sredstva za izradu (računalna oprema ili računalni program) kojim se potpisnik koristi pri izradi e-potpisa (može se raditi o prilagođenim računalima opće namjene i o specijaliziranim rješenjima koja kombiniraju hardverska i softverska rješenja)

- **sredstvo za izradu naprednoga elektroničkog potpisa mora osigurati:   
  
1)** da se podaci za izradu naprednoga elektroničkog potpisa mogu pojaviti samo jednom te da je ostvarena njihova sigurnost  
  
**2)** da se podaci za izradu naprednoga elektroničkog potpisa ne mogu ponoviti te da je potpis zaštićen od krivotvorenja pri korištenju postojeće raspoložive tehnologije  
  
**3)** da podatke za izradu naprednoga elektroničkog potpisa potpisnik može pouzdano zaštititi protiv korištenja od strane drugih

- sredstvo za izradu naprednoga elektroničkog potpisa ne smije prilikom izrade naprednoga elektroničkog potpisa promijeniti podatke koji se potpisuju ili onemogućiti potpisniku uvid u te podatke prije procesa izrade naprednoga elektroničkog potpisa

- upotrebom kriptografskih algoritama generira javne i privatne ključeve koji su jedinstveni za svakog potpisnika i ne mogu se rekonstruirati ili reproducirati bez znanja potpisnika

**8.4.9. Sredstva i podaci za verificiranje elektroničkog potpisa**

- dokumenti i komunikacija potpisana e-potpisom moraju odgovarati zabilježenom jedinstvenom e-potpisu potpisnika i trebaju se moći podvrgnuti provjeri (verifikaciji,ovjeri) 🡪 u tu svrhu služi odgovarajuća računalna oprema i programi te kontrolni kodovi,tj. javni ključevi kao podaci dostupni certifikacijskim tijelima kako bi se provela provjera autentičnosti i integriteta podataka zaštićenih e-potpisom

**8.4.10. Certifikati i kvalificirani certifikati**

- **digitalni,tj. elektronički certifikat** je isprava u digitalnom obliku kojom se potvrđuje identitet fizičke ili pravne osobe

- najčešći oblik digitalnog certifikata je onaj kriptografski zaštićen,povezan s uporabom javnih ključeva u PKI-u

- digitalni certifikat služi za provjeru pripadnosti javnog ključa nekoj fizičkoj ili pravnoj osobi,a izdaje ga davatelj usluge izdavanja digitalnih certifikata,tj. neko tijelo javne vlasti ili trgovačko društvo koje pruža tu vrstu usluge

- certifikacijsko tijelo izdaje certifikate pod određenim uvijetima i odgovorno je svojim korisnicima za podatke u certifikatu

- ZEP definira **elektronički certifikat** kao potvrdu u e-obliku koja povezuje podatke za verificiranje e-potpisa s nekom osobom i potvrđuje identitet te osobe

- ZEP uvodi i pojam **kvalificiranog certifikata** – elektronička potvrda kojom davatelj usluge izdavanja kvalificiranih certifikata potvrđuje napredni e-potpis

- uvjeti koje ZEP propisuje za valjanost kvalificiranog certifikata odnose se na sadržaj tog certifikata i **traže da kvalificirani sadržaj ima:**

**1)** oznaku o tome da se radi o kvalificiranom certifikatu,   
  
**2)** identifikacijski skup podataka o osobi koja izdaje certifikat (osobno ime; ime oca ili majke; nadimak, ako ga osoba ima; datum rođenja; prebivalište, odnosno boravište; naziv pravne osobe i sjedište, ako certifikat izdaje pravna osoba),  
  
**3)** identifikacijski skup podataka o potpisniku (osobno ime, ime oca ili majke, nadimak, ako ga osoba ima, datum rođenja, prebivalište, odnosno boravište)  
  
**4)** podatke za verificiranje elektroničkog potpisa koji odgovaraju podacima za izradu elektroničkog potpisa koji su pod kontrolom potpisnika  
  
**5)** podatke o početku i kraju važenja certifikata  
  
**6)** identifikacijsku oznaku izdanog certifikata (brojčanu ili drugu oznaku te datum izdavanja)  
  
**7)** napredni elektronički potpis davatelja usluge izdavanja kvalificiranih certifikata  
  
**8)** ograničenja vezana za uporabu certifikata, ako ih ima  
  
**9)** ograničenja u odnosu na važnost pravnih radnji za koje se daje certifikat, ako ih ima

**8.4.11. Obveze i odgovornost davatelja certifikacijskih usluga**

- u sustavu zaštite e-komunikacije infrastrukturom javnog ključa (PKI), centralno mjesto zauzimaju **davatelji usluga certificiranja** (CA,Certification Authority),tj. tijela koja pohranjuju ključeve,odnosno elektroničke kodove koji služe autentifikaciji i kriptografskoj zaštiti e-komunikacije (njihova uloga definirana u ZEP-u)

- **certifikacijska tijela s obzirom na motiv bavljenja tom djelatnosti:**

**a) komercijalna certifikacijska tijela** – naplaćuju svoju djelatnost izdavanja e-certifikata

**b) javna certifikacijska tijela** – tijela državne uprave,javne institucije i dr.javna tijela koja ne naplaćuju svoju djelatnost

- da bi davatelj usluge mogao davati uslugu certificiranja, mora biti sposoban osigurati sigurnost i kvalitetu certifikacije,tj. mora voditi ažuran upisnik potpisnika kako bi se u svakom trenutku moglo identificirati potpisnika ili mu u kratkom vremenu omogućiti opoziv usluge

- od davatelja usluge se traži i da raspolaže odgovarajuće osposobljenom tehničkom službom koja posjeduje specijalistička znanja i iskustvo na području primjene tehnologija e-potpisa i njima srodnih sigurnosnih tehnologija (trebaju primijeniti međunarodne standarde za informacijsku sigurnost)

- važan je i zahtjev osiguranja pohrane svih relevantnih podataka što se odnose na kvalificirani certifikat tijekom odgovarajućeg razdoblja

- od davatelja usluge traži se pohrana podataka o potpisnicima,izdanim certifikatima, listama opozvanih certifikata kao i tehničke podatke nastale bilježenjem rada sustava

- Uredba od davatelja usluge traži i izradu sigurnosnih kopija (backupa) podataka pohranjenih na zaštićenom mjestu

- rok za pohranu podatak je ograničen na 10 godina s opaskom da Uredba zahtijeva da elektronički mediji trebaju garantirati opstojnost podataka na rok od najmanje 20 godina

**8.4.12. O odgovornosti davatelja usluge izdavanja elektroničkog certifikata**

- čl.6. europske **Direktive o elektroničkom potpisu** daje minimalan okvir odgovornosti davatelja usluge izdavanja elektroničkog certifikata

- prema Direktivi, **davatelj usluge izdavanja elektroničkog certifikata odgovara za:**

**1)** preciznost vremena izdavanja i eventualnog povlačenja certifikata

**2)** sadržaj podataka sadržanih u certifikatu u trenutku izdavanja certifikata

**3)** komplementarnu upotrebu podataka za izradu i verifikaciju e-potpisa u slučaju da davatelj usluge generira oba skupa podataka

**4)** za nepravovremeno djelovanje u slučaju povlačenja ili suspenzije certifikata

- u ZEP su unesene odredbe iz europske direktive po kojima je određena obveza za davatelja usluga da osigura rizik od odgovornosti na štetu na temelju obavljanja usluge izdavanja elektr. certifikata

- ZEP propisuje i obvezu ugovaranja osiguranja za sve davatelje usluge certificiranja

- ZEP (kao i europska Direktiva) uključuje odgovornost za štetu nastalu uporabom certifikata bilo kojem tijelu,tj. fizičkoj ili pravnoj osobi do koje je došlo zbog propuštanja certifikacijskog tijela da nadzire certifikacijski postupak,odnosno odgovara za točnost podataka sadržanih u kvalificiranom certifikatu u vrijeme izdavanja certifikata te za ispunjavanje ostalih uvjeta koje zakon traži za izdavanje kvalificiranog certifikata

- čl.30. ZEP-a regulira uvjete pod kojima davatelj usluge certificiranja ima obvezu prekidanja te usluge,tj.stavljanja certifikata i certificiranog e-potpisa izvan snage

- postoji mogućnost da osoba posjeduje više e-potpisa,tj. e-certifikata (smrt ili gubitak poslovne sposobnosti fiz.osobe će utjecati na opoziv ostalih certifikata,ali promjena statusa ili neke kvalitete se može odnositi samo na 1 od njegovih e-identiteta)

**8.4.13. O priznanju certifikata koji izdaje davatelj usluga certifikacije sa sjedištem u inozemstvu**

- zakonodavni rad tijela EU promovira zajednički europski pravni okvir razvoja e-trgovine i e-komunikacije

- **Direktiva o elektroničkoj trgovini** traži od zemalja članica Unije da diskriminiraju rad certifikacijskih tijela smještenih u drugim državama pod uvjetom da ista poštuju pravila koja Unija Direktivom stavlja pred certifikacijska tijela u zemljama članicama

- **certifikate koja izdaju strana certifikacijska strana tijela, hrvatski zakon će priznat valjanim ako:**

**1)** davatelj usluga certificiranja ispunjava uvjete za izdavanje kvalificiranih certifikata iz ZEP-a te je dobrovoljno akreditiran u RH ili jednoj od država članica

**2)** ako neki domaći davatelj usluga certificiranja koji ispunjava uvjete za izdavanje kvalificiranih certifikata iz ZEP-a jamči za takve certifikate jednako kao da su njegovi

**3)** ako tako odredi bilateralni ili multilateralni sporazum između Republike Hrvatske i drugih zemalja ili međunarodnih organizacija,

**4)** ako tako odredi bilateralni ili multilateralni sporazum između Europske unije i trećih zemalja ili međunarodnih organizacija

**8.4.14. Elektronički potpis u drugim hrvatskim propisima**

- sred. 2008.g. zakonodavac je sustavno počeo uvoditi pojam e-potpisa i e-komunikacije u postupovne propise hrvatskog prava - Zakon o općem upravnom postupku, Zakon o kaznenom postupku, Zakon o parničnom postupku

**a) Elektronički potpis u Zakonu o općem upravnom postupku**

- uvodi mogućnost pokretanja postupka,odustanka od zahtjeva, ulaganja podnesaka, obavještavanja,dostave i izdavanja potvrda elektroničkim putem

- čl.75.st.2. ZUP-a kaže da podnesci dostavljeni u e-obliku s e-potpisom će se smatrati vlastoručno potpisan 🡪 izjednačava se e-komunikacija s tradicionalnom komunikacijom

- zakonodavac u ZUP-u ne traži primjenu naprednog e-potpisa, iako se samo takav potpis smatra ravnopravnom zamjenom

**b) Elektronički potpis u Zakonu o kaznenom postupku**

- ZKP je donesen krajem 2008.g. i predviđa mogućnost elektroničke komunikacije i ponašanja podnesaka u obliku elektroničkih isprava

- čl.79.st.1. spominje elektroničku ispravu istaknuvši utvrđenje jednoznačnog obilježja kojim se utvrđuje sastavljač e-isprave kao nužan uvjet kako bi se neki podnesak mogao podnijeti i zaprimiti e-putem

**c) Elektronički potpis u Zakonu o parničnom postupku**

- uvedena je zakonska mogućnost e-komunikacije suda i stranaka

- ZPP omogućuje dostavu pismena,podnašanje podnesaka,zakazivanje ročišta te dostavu obrazaca i drugih očitovanja u sklopu ostvarivanja pravosudne suradnje u EU sukladno odredbama Uredbe br. 1393/2007 Europskog parlamenta i Vijeća o dostavi sudskih i izvansudskih isprava u građanskim i trgovačkim predmetima i državama članicama

**8.4.15. Elektronička isprava kao poseban pravni institut**

- uz ZET i ZEP , **Zakonom o elektroničkoj ispravi** definira se posebna vrsta dokumenta, **elektronička isprava** koja u praksi treba biti izjednačena s ispravama izdanim na papiru

- digitalni dokument potpisan ispravnim i certificiranim elektroničkim potpisom čini praktičnu,uporabnu cjelinu koju je zakonodavac odlučio regulirati i u našem pravu

- e-potpis i e-certifikat osiguravaju oznaku identiteta osobe i sadržaja elektron. dokumenta

**8.5. Elektronička vlast (e-Government)**

- **pojam elektroničke vlasti** kao oblik elektroničkog poslovanja najčešće označava mogućnost odgovarajućih postupaka,metoda i tehnologija pogodnih za rad i elektroničko pružanje usluga i online komunikacije s građanima,poslovnim subjektima i tijelima državne vlasti

- ključan element e-vlasti su sami korisnici, a o njihovom zadovoljstvu ovisi i daljni razvoj

- **ciljevi elektroničke vlasti:**

**1)** komunikacija s drugim državnim organima i institucijama unutar zemlje kao i s institucijama drugih zemalja i međunarodnih organizacija

**2)** poticanje gospodarskog razvoja i ubrzanje gospodarskih aktivnosti komunikacijom i pružanjem usluga i poslovnih informacija gospodarskim subjektima

**3)** poticanje digitalne demokracije e-glasovanjem i neporednom interaktivnom komunikacijom s građanima te online sudjelovanje u radu vlasti

**4)** pružanje online usluga i omogućavanje pristupa javnim i drugim informacijama od interesa za građane i gospodarstvo

- **poslovanje se odvija između:**

**a)** vlasti i tijela lokalne i područne samouprave i dr. državnih organa i institucija (G2G)

**b)** vlasti i građana ( G2C, government to citizen)

**c)** vlasti i gospodarskih subjekata (G2B,government to business)

**d)** vlasti i korisnika iz drugih država

**e)** vlasti svih njenih službenika (G2E,government to employes)

-u širem smislu, obuhvaća i komunikaciju između građana (C2C) o radu vlasti i pitanjima općeg interesa

- 2002.g. je donesena strategija **Informacijska i komunikacijska tehnologija – Hrvatska u 21.st.** kojom je naglašena usmjerenost RH prema informacijskom društvu te su postavljeni **ciljevi u razvoju e-vlasti u RH u razdoblju 2003.-2007.,a to su:**

**a)** gospodarski rast RH,povećanje zaposlenosti i osvajanje novih tržišta

**b)** priključenje RH razvijenim zemljama u istraživanju i razvoju inform. i komunik. tehnologije te u njenoj primjeni pri stvaranju novih proizvoda i usluga

**c)** unapređenje učinkovitosti i kvalitete usluga koje uprava pruža građanima i tvrtkama

**d)** izgradnja jeftine,brze i sigurne inform. i komunik. infrastrukture zbog zadovoljenja potreba građana i gospodarstva

- na temeljima strategije donesen je **Program e-Hrvatska 2007** s ciljem uspostave i umrežavanja sustava koji će građanima i poslovnim subjektima omogućiti komunikaciju s državnom upravom i upotrebu niza njenih usluga putem interneta

- za provedbu tog programa osnovan je **Središnji državni ured za e-Hrvatsku** kao središnje tijelo državne uprave za oblikovanje,praćenje i vrednovanje javne politike razvoja informacijskog društva u RH

- za razdoblje 2009.-2012.g. donesena je **Strategija razvoja elektroničke uprave u RH** čija je svrha utvrditi okvir i ciljeve postojećih i novih aktivnosti e-uprave s naglaskom na zadovoljstvo korisnika,racionalizaciju administrativnih postupaka te pripremu i pružanje modernih e-usluga i stvoriti cjelovitu e- javnu upravu u RH

- **temelji na kojima počiva cjelovita e-javna uprava u RH:**

**a)** računalna i komunikacijska infrastruktura

**b)** podatkovno/informacijska i dokumentacijska osnovica

**c)** dostupnost elektroničkih usluga

**d)** ljudski potencijali

- bilo je potrebno uspostaviti sustav interoperabilnosti te središnji sustav autentifikacije i autorizacije svih sudionika

- **sustav interoperabilnosti** koji je u RH još uvijek u razvoju treba osigurati mogućnost povezivanja različitih informacijskih sustava tijela javne vlasti te razmjenu podataka između njih da različiti inform.sustavi mogu djelovati kao da se radi o jedinstvenom sustavu

- cilj **sustava autentifikacije i autorizacije** je upravljanje elektroničkim identitetima čijim se uvođenjem stvara jedinstven sustav autentifikacije i autorizacije u virtualnom okruženju pri komunikaciji korisnika usluga e-vlasti i tijela javne vlasti

- takav sustav građanima omogućuje sigurno i vremenski neograničeno korištenje usluga e-vlasti putem interneta ili primjenom ostalih sustava elektr.komunikacijskih mreža

- donošenjem Zakona o državnoj informacijskoj infrastrukturi, uspostavom e-Građani, državne informacijske infrastrukture, Središnjeg državnog portala i sustava NIAS (Nacionalni identifikacijski i autentifikacijski sustav) prevladane su prepreke

- **državna informacijska infrastruktura (DII)** prema Zakonu o državnoj informacijskoj infrastrukturi (donesen u svrhu uspostave sustava interoperabilnosti) je definirana kao sustav koji čine zajednička državna osnovica za sigurnu razmjenu podataka i alati za interoperabilnosti kao što su Metaregistar,tehnički standardi,klasifikacije, javni registri, sustav e-Građani te mreže CARNet i HITRONet

- **svrha uspostavljanja DII je** osiguranje interoperabilnosti javnih registara i informacijskih sustava tijela javnog sektora te osiguranje zajedničkih elemenata za interakciju s građanima ili drugim korisnicima

- kao najvažniji dio DII je uspostavljen sustav **e-Građani**, a njega čine Središnji državni portal, NIAS i sustav osobnog korisničkog pretinca

- uspostavom sustava e-Građani objedinjuju se e-usluge tijela javne vlasti,uspostavlja se jedinstveni mehanizam za verifikaciju e-identiteta i izdavanje vjerodajnica za njegovu potvrdu,jedinstveni mehanizam za sigurnu dostavu personaliziranih informacija korisnicima te se rješava pitanje neinformiranosti javnosti o dostupnosti usluga e-vlasti

- **Središnji državni portal** je mjesto pristupa informacijama na internetu na kojem se objedinjuju na jednom mjestu i u lako dostupnim formatima informaicje o javnim uslugama kao i druge informacije i dokumenti u vezi s obavljanjem poslova tijela javnog sektora

- **pojam vjerodajnice** po ZDII je skup podataka kojim se predstavlja korisnik e-usluge,a služi kao dokaz za provjeru e-identiteta kako bi se omogućio pristup e-uslugama

- **NIAS ima ulogu** posrednika između korisnika e-usluge,pružatelja e-usluge i izdavatelja vjerodajnice,a skup podataka koji NIAS prosljeđuje e-usluzi je dovoljan za jednoznačnu identifikaciju korisnika

- **sustav osobnog korisničkog pretinca** služi za primanje poruka od tijela javne vlasti (trenutačno može primiti više od 40 različitih poruka i obavijesti od raznih tijela javne vlasti)

- jedan od glavnih strateških planova **Strategije e-Hrvatska 2020** je daljnji razvoj e-usluga

- kao glavni nedostaci u implementaciji e-vlasti u dokumentima ( Digitalna agenda za Europu 2020. i EU eGovernment izvještaj za 2015.g.) se navode izostanak interakcije s tijelima javne vlasti,repetitivno traženje podataka, nedostatak kvalitetnog korisničkog sučelja,raspršenost podataka,sigurnost te nedostatak prekograničnih usluga za javne i fizičke osobe

**9. cjelina: INFORMACIJSKO RATOVANJE I INFORMACIJSKA SIGURNOST**

- osim kiberkriminala,sve opasnije postaje informacijsko ratovanje i kiberratovanje

**9.1. Informacijsko ratovanje**

- informacijsko ratovanje postaje sredstvo i način da se ostvari prednost pred postojećim ili potencijalnim neprijateljem,poslovnim konkurentima te obavještajnim i vojnim službama

- nema jedinstvenog mišljenja o tome što je informacijsko ratovanje, ali postoji suglasnost da su mu u osnovi informacijski sustavi i informacije, čija se tajnost,cjelovitost i dostupnost žele očuvati (**obrambeni informacijski rat**) ili ugroziti (**napadački informacijski rat**)

**9.1.1. O pojmu i nastanku**

- **Cohen** – informacijski rat je oblik sukoba u kojem je informacijska tehnologija oružje,meta, cilj ili metoda

- **Goldberg** – inform. rat je ofenzivno i defenzivno korištenje informacijama i informacijskim sustavima da bi se poreklo,iskoristilo,korumpiralo ili uništilo protivnikove informacije, informacijske procese,sustave i računalne mreže uz zaštitu vlastitih,a takve se akcije poduzimaju da bi se ostvarila prednost nas vojnim ili poslovnim suparnicima

- riječ je o novijem obliku ratovanja kojem su cilj,odnosno objekt napada i zaštite informacijski resursi protivnika,a može se ostvariti raznim oblicima psihološkog ratovanja ili drugim tradicionalnim metodama i sredstvima

- cilj takvog napada nisu samo informacijski resursi protivnika,već se često vlastite informacije ili dezinformacije prezentiraju način kako bi se postigao određeni učinak

- pogrešno je upotrebljavanje pojmova kibernetički rat i umreženi rat kao sinonim inf.rata

- **pojam kibernetičkog rata** (**John Arquilla i David Ronfrldt: Cyberwar Is Coming**) se odnosi na izvođenje i pripremu izvođenja vojnih operacija prema informacijskim načelima, znači ometanje,ako ne uništavanje, informacijskih i komunikacijskih sustava,široko definiranih kako bi uključili čak i vojnu kulturu na koju se oslanja protivnik kako bi saznali: tkp je on, gdje je on,što može učiniti i kada,zašto se bori,koje prijetnje treba uzeti u obzir,itd.

- **umreženi rat** se odnosi na nastajući način vođenja sukoba na socijetalnoj razini izvan tradicionalnog vojnog ratovanja u kojem se protaonisti koriste mrežnim oblicima organizacije i s njima povezanim doktrinama,strategijama i tehnologijama prilagođenim inform. dobu

- **umreženi rat se sastoji od** disperznih organizacija,malih skupina i pojedinaca koji komuniciraju,koordiniraju i vode kampanje na internetski način,često bez precizne centralne kontrole

- informacijsko ratovanje je širi pojam od kibernetičkog i mrežnog ratovanja

- **kibernetičko ratovanje podrazumijeva** postojanje informacijsko-komunikacijske infrastrukture putem koje se taj kiberprostor stvara i održava,a **mrežno ratovanje** se odnosi na mrežnu organizaciju,a ne toliko na infrastrukturu putem koje se ono provodi

- informacijsko ratovanje obihvaća razne oblike tradicionalnog,kibernetičkog i umreženog ratovanja pri čemu su informacije,informacijski resursi,tehnologije i procesi cilj ili sredstvo kojim se taj ofenzivni ili defenzivni rat vodi

- danas podrazumijeva široku upotrebu informacijsko-komunikacijskih tehnologija

- nastanak inf.ratovanja neki povezuju s otkrićem i razvojem informacijske, drugi informatičke tehnologije,dok treći smatraju da korijeni sežu u prošlost čovječanstva

- **Toffler : War and Anti-War** – opisuje povijest ratovanja kroz 3 vala:

**a)** poljoprivredni

**b)** industrijski

**c)** informacijski (rat protiv Iraka,Zaljevski rat, predstavlja prvi oblik inform.ratovanja)

- **Denning** smatra da se inform.ratovanje javlja već od prvih nastajanja ljudi da sačuvaju tajnost nekih važnih i povjerljivih informacija

- osim za priskluškivanje čelnika drugih zemalja i progon političkih neistomišljenika, suvremene tehnologije se mogu iskoristiti i za stvaranje kompleksnih dosijea o najširem krugu građana

**9.1.2. Učinci informacijskog ratovanja**

- inform. ratovanje može izazvati dramatične posljedice u fizičkom svijetu

- danas je sve učestalije korištenje sofisticiranim malicioznim programima kako bi se pribavile informacije protivnika (SAD i Izrael prednjače u tome) 🡪 npr. 2012.g. je The Washington Post objavio podatke o zajedničkom programu u koji su uključene Agencija za nacionalnu sigurnost,CIA i izraelska vojska (upotrebljavaju destruktivni softver poput Flame i Stuxnet virusa koji uzrokuje kvarove u opremi u iranskom nuklearnom pogonu)

- djelovanjem takvih programa moguće je ugroziti kritičnu infrastrukturu jer je njačešći cilj napad na računalni i komunikacijski sustav kojim se koristi za nadzor i upravljanje raznim industrijskim i drugim sustavima naziva **SCADA** (Supervisory Control And Data Acquisition)

- 2013.g. je tvrtka Kaspersky otkrila maliciozni program Crveni oktobar, skraćeno Rocra namijenjen kibernetičkoj špijunaži (cilj su mu vladine institucije i diplomatska predstavništva zemalja I Europe,ali i nekih zemalja Z Europe i SAD-a, djeluje od 2007.g. i još je aktivan)

**9.1.3. Aktivizam,haktivizam i kiberterorizam**

- akteri inf.ratovanja su, osim hakera,kriminalaca i njihovih udruženja,terorista ili neprijateljske zemlje, i razni aktivisti,nevladine udruge te čak borci za ljudska prava

- haktivisti putem interneta ostvaruju neke,često s moralnog aspekta i opravdane ciljeve te oni tako ugrožavaju računalne sustave čineći kaznena djela u stjecaju

- tako su npr. napadima na razne internetske stranice Kazalište za elektroničko ometanje i njihove pristaše nastojali pružiti podršku meksičkim Zapatistima,a slično se događa i 1999.g. kada je NATO slučajno bombardirao kinesku ambasadu u Beogradu, pa su kineski haktivisti zasuli web-stranice američke vlade veliko količinom poruka

- **Ristović** – ovo je situacija u kojoj država i društvo nije suočeno s teško naoružanom i jakom vojnom silom na koju odgovara nesimetričnom ugrozom koja dolazi od slabog protivnika,skupine ljudi ili čak anonimnog pojedinca

- mrežno i kibernetičko ratovanje predstavljaju primjer asimetričnog ratovanja,a njima se može učinkovito djelovati na kritičnu nacionalnu inform.infrastrukturu radi izazivanja panike i političke krize u nekoj zemlji,ali istovremeno mogu poslužiti za ostvarenje ciljeva

- donedavno su se aktivnosti državnih tajnih i obavještajnih službi svodile na pribavljanje javnih i tajnih političkih i vojnih podataka,vrbovanje obavještajaca u drugim zemljama te obavještajne aktivnosti njihovih agenata na radu u inozemstvu, a cilj im je saznati njihovu spremnost,namjere i preduhitriti eventualne ofanzivne aktivnosti

- u novije vrijeme je češća **krađa intelektualnog vlasništva** čime se nastoji steći prednost i ostvariti korist smanjenjem troškova koje bi gospodarstvo imalo od ulaganja u vlastiti razvoj

- poslovna špijunaža (business intelligence) sve više postaje dijelom poslovne strategije mnogih tvrtki koje tako žele ostvariti prednos u odnosu na konkurenciju

- mogućnost novih tehnologija su uočile i terorističke organizacije (Toffler tvrdi da ćemo se uskoro suočiti s infoterorizmom)

- u budućnosti bismo se mogli suočiti s kibernetičkim ratom i kiberterorizma

**9.1.4. Budućnost informacijskog ratovanja**

- veliki gospodarski subjekti i državne institucije su sve češće mete raznih hakera,tajnih službi i terorista

- u budućnosti se očekuje da će se postojeći trend nastaviti,tj. da će biti velik broj sukoba manjeg intenziteta uz sve veće korištenje informacijskom tehnologijom

- sukobi,odnosno ratovi većih razmjera bi predstavljali primjer kombinacije tradicionalnog, kibernetičkog i umreženog ratovanja

- kiberterorizam će predstavljati djelotvorno sredstvo brojnih ekstremističkih organizacija, posebno u kombinaciji s tradicionalnim metodama i sredstvima napada

**9.2. Informacijska sigurnost**

- Zakonom o informacijskoj sigurnosti je informacijska sigurnost definiran akao stanje povjerljivosti,cjelovitosti i raspoloživosti podataka koje se postiže primjenom propisanih mjera i standarda informacijske sigurnosti te organizacijskom podrškom za poslove planiranja,provedbe,provjere i dorade mjera i standarda

- da bi se to ispunilo,potrebno je ispuniti odgovarajuće strateške,oganizacijsko-tehnološke i pravne pretpostavke

- na nacionalnoj razini to podrazumijeva donošenje Strategija kibersigurnosti i kiberkriminala, dok na razini državnih institucija,javnih poduzeća i privatnog sektora to znači uspostavljanje cjelovite sigurnosne politike,odnosno strategije

- pravna infrastruktura u RH koja uređuje to područje obuhvaća:

a) Zakon o informacijskoj sigurnosti

b) Zakon o tajnosti podataka

c) Zakon o kritičnim infrastrukturama

d) Zakon o zaštiti osobnih podataka

e) Zakon o pravu na pristup informacijama

f) Zakon o državnoj informacijskoj infrastrukturi

g) Zakon o sigurnosnim provjerama

h) podzakonski akti

**9.2.1. Strateške pretpostavke informacijske sigurnosti**

- cilj sveobuhvatne sigurnosne politike je poduprijeti druge politike EU za unutarnju i vanjksu sigurnost i osigurati kibernetičku sigurnost,jačati povjerenje i zaštititi privatnost na Jedinstvenom digitalnom tržištu (Digital Single Market)

- program EU za instraživanje i inovacije – **Obzor 2020.** (Horizon 2020) za razdoblje od 2014. do 2020.g. stavlja poseban naglasak na aktivnosti:

**a)** borbu protiv kriminala i terorizma

**b)** jačanje sigurnosti upravljanjem granicama

**c)** pružanje kibernetičke sigurnosti

**d)** jačanje otpornosti Europe na krize i prirodne katastrofe

**e)** osiguranje privatnosti i slobode na interentu i jačanje društvenih dimenzija

- odlučujuću ulogu pri ostvarenju tih ciljeva imaju strategije kibersigurnosti i strategije kiberkriminala

- nema općeprihvaćene definicije kibersigurnosti (u početku se govorilo o sigurnosti IKT-a, informatičkoj sigurnosti,a u novije vrijeme se piše o kibernetičkoj sigurnosti)

- **Jarno Limnell** smatra da je riječ o različitim pojmovima unatoč tome što se u jednoj mjeri preklapaju

- IKT sigurnost se svodi na sigurnost same opreme,a informatička sigurnost je koncept koji obuhvaća zaštitu podataka bez obzira na formu koju poprimaju (to nije zaštita samo digitalnih informacija)

- kibersigurnost se odnosi na cijeli digitalni svijet i temelji se na povjerenju koje se opet temelji na shvaćanju da će praktične mjere koje su primijenjene omogućiti preventivno odupiranje kibernetičkim prijetnjama i njihovim učincima

- Strategija kibersigurnosti Europske unije: Otvoren,siguran i zaštićen kiberprostor definira kibersigurnost kao skup mjera zaštite i aktivnosti kojim se mogu koristiti radi zaštite kiberprostora,kako u civilnom tako i vojnim područjima, od prijetnji koje su povezane sa ili koje mogu naškoditi njegovim neovisnim mrežama i informacijskoj infrastrukturi

- kibersigurnost nastoji očuvati dostupnost i integritet mreža i infrastrukture te povjerljivost informacija sadržanih unutar njih

- prema ITU (International Telecommunication Union) kibersigurnost je skup alata,politika,sigurnosnih koncepata,sigurnosne zaštite,smjernica,pristupa upravljanju rizikom,akcija,treninga,najbolje prakse,osiguranja i tehnologija kojim se mogu koristiti za zaštitu organizacija i imovine korisnika u kibernetičkom prostoru

- kibersigurnost nastoji osigurati postizanje i održavanje sigurnosnih svojstava organizacije i sredstava korisnika protiv relevantnih sigurnosnih rizika u kiberokruženju

- **opći sigurnosni ciljevi obuhvaćaju:**

**a)** dostupnost

**b)** integritet (može uključivati autentičnost i neosporavanje)

**c)** povjerljivost

**9.2.2. Strateški prioriteti i aktivnosti EU**

- negativne pojave se odražavaju na funckioniranje Jedinstvenog digitalnog tržišta u EU što ima za posljedicu sve veće gospodarsko zaostajanje za ostatkom razvijenog svijeta,a time se gubi na konkurentnosti,stvaranju novih radnih mjesta,razvoju kreativne ekonomije i inovativnog gospodarstva

- sigurnost računalnih mreža i informacijskih sustava EU su preduvjet osiguranja njezina prosperiteta i konkurentnosti njezinog digitalnog gospodarstva

- **Digitalna agenda EU** polazi od toga da je povjerenje i sigurnost u internet presudno za život građana i daljnji razvoj digitalnog društva (navodi 14 aktivnosti radi poboljšanja kibersigurnosti)

- te aktivnosti uključuju uspostavu i funkcioniranje mreže CERT-a na nacionalnoj razini, simulaciju kibernetičkih incidenata i odgovor na njih te jačanje kibersigurnosne pripravnosti diljem EU-a

- u Strategiji kibersigurnosti EU i prijedlogu Komisije za donošenju Direktive o mrežnoj i informacijskoj sigurnosti navode se zakonske mjere i predlažu inicijative sa svrhom izrade online okruženja EU-a koje će biti najsigurnije na svijetu

- strategija ima za cilj potaknuti konkurentnost te rast i otvaranje novih radnih mjesta u EU

- kibersigurnost ima globalnu dimenziju

- **osnovane su i institucije:**

**a)** European Network and Information Security Agency (ENISA)

**b)** Computer Emergency Response Team for the EU institutions (CERT-EU)

**c)** European Cybercrime Centre (EC3) – djeluje unutar Europola

- na međunarodnom planu aktivnosti i suradnja se odvijaju preko zajedničke Radne skupine EU-SAD za kibersigurnost i kiberkriminal, OECD, UN, Međunarodne telekomunikacijske unije (ITU), Organizacija za sigurnost i suradnju u Europi (OSCE), WSIS i Foruma za upravljanje internetom (IGF)

- sve važniju ulogu ima i NATO (napad na jednu državu članicu, treba smatrati kao napad na sve njih)

**Strategija kibersigurnosti EU-a**

- strategija ocrtava viziju EU,pojašnjava uloge i odgovornost te predlaže konkretne aktivnosti na razini EU

- njezin je cilj osigurati snažnu i učinkovitu zaštitu i promicanje prava građana kako bi se online okruženje EU učinilo najsigurnijim na svijetu

- **ove aktivnosti posebno uključuju:**

**a)** postizanje kibernetičke otpornosti

**b)** drastično smanjenje kiberkriminala

**c)** razvijanje kiberobrambene politike

**d)** poticanje industrijskih i tehnoloških resursa

**e)** jačanje međunarodne politike kiberprostora EU

- ova Strategija predstavlja opći pristup EU sa svrhom zaštite i sigurnosti računalnih mreža, sprječavanja kiberkriminala i zaštite potrošača

**Direktiva o mrežnoj i informacijskog sigurnosti EU-a**

- 7.2.2013.g. Europska Komisija donosi Strategiju kibersigurnosti EU

- sastavni dio Strategije čini nacrt Direktive o mrežnoj i informacijskoj sigurnosti (NIS Directive, poznatija pod nazivom Direktiva o kibersigurnosti)

- **glavni ciljevi Direktive su:**

**a)** osigurati minimalne sigurnosne standarde

**b)** promicanje suradnje

**c)** jačanje spremnosti i transparentnosti u važnim sektorima

- ona sadrži prijedloge za poboljšanje i jačanje otpornosti EU na prijetnje u kiberprostoru te osigurava ujednačenu i zajendičku razinu sigurnosti računalnih mreža i informacijskih sustava

- **Direktivom se članice obvezuju da će:**

**a)** implementirati nacionalnu Strategiju mrežne i informacijske sigurnosti i uspostaviti nadležno tijelo za njezino provođenje kao i nacionalni CERT, kako bi se spriječilo i učinkovito odgovorilo na sigurnosne prijetnje i incidente

**b)** stvoriti mrežu zajedničke suradnje unutar koje će se dijeliti informacijeo sigurnosti diljem EU u borbi protiv prijetnji NIS-u i incidenata

**c)** uspostaviti obvezu operatorima kritične infrastrukture i davateljima usluga inform.društva da, radi procjene sigurnosnih rizika,primijene odgovarajuće mjere i nadležnom nacionalnom tijelu prijave incidente koji mogu znatnije utjecati na sigurnost njihovih osnovnih usluga

- 13.3.2014. je Europski parlament izglasao predloženu Direktivu uz određene amandmane na predloženi tekst, koje će ispitati Vijeće EU

- **temeljne zamjerke i prijedlozi izmjena odnose se na:**

**1)** sužavanje kruga organizacija koje su obuhvaćene zahtjevima Direktive kako se ona ne bi odnosila na internetske pretraživače,društvene mreže,servise za internetsko plaćanje i usluge računarstva u bolaku te one koji se bave razvojem softvera i proizvodnjom hardvera

2) donošenje nacionalnih sigurnosnih strategija uz pomoć ENISE što će omogućiti članicama da razviju minimalne standarde na tom području

3) iemnovanje zajedničke točke kontakta između nacionalnih nadležnih tijela (NCAs) za sigurnost te uspostavu jedinstvenog mrežnog informacijskog sustava

**Strategija kiberkriminala EU-a**

- temelji se na aktivnostima Vijeća Europe i na Konvenciji o kibernetičkom kriminalu Vijeće Europe iz 2001.g.

- **ciljevi Konvencije su bili:**

**a)** usklađivanje nacionalnih zakonodavstava

**b)** propisivanje minimuma kaznenih djela koje treba sankcionirati

**c)** veće stražne ovlasti redarstvenim vlastima

**d)** uspostava učinkovitog sustava međunarodne suradnje i pravne pomoći

- značenje ove Konvencije je njezino ratificiranje u gotovo svim članicama Vijeća Europe,ali i u zemljama koje to nisu (ukupno 44 zemlje)

- 2005.g. je EU donijela Okvirnu odluku o napadima protiv informacijskih sustava koja je 2013.g. zamijenjena novom Direktivom o napadima protiv informacijskih sustava (temelji se na Okvirnoj odluci dodajući kriminalizaciju naprava i nezakonitog presretanja,otegotne okolnosti za kaznena djela,krađe identiteta,uzrokovanja ozbiljnije štete ili djela protiv kritične infrastrukture)

- predviđa i vrijeme odziva nadležnih organa od 8 sati za hitne slučajeve te obvezu prikupljanja statističkih podataka o zloporabama

**Međuodnos strategija kibersigurnosti i kiberkriminala**

- nemoguće je zamisliti efikasnu strategiju kibersigurnosti bez cjelovite borbe protiv kiberkriminala i obrnuto

- primarni cilj kibersigurnosti je očuvanje i zaštita cjelovitosti,tajnosti i dostupnosti inform. -komunik. tehnologija,posebno kada je riječ o kritičnoj infrastrukturi,a iz toga proizlazi da ona obuhvaća određene političke interese,ekonomske i socijalne interese i tehničke interese koji omogućavaju da se zaštiti i očuva tajnost,cjelovitost i dostupnost IKT-a koje čini infrastrukturu kiberprostora

- Strategije kibersigurnosti daju najviši prioritet zaštiti kritične infrastrukture javnog i privatnog sektora kao i državnim računalnim sustavima od:

**1)** nenamjernih incidenata uzrokovanih neispravnim funkcioniranjem tehnologije,slučajnim kvarovima,ljudskim propustima,elementarnim nepogodama i sl.

**2)** namjernih napada od strane državnih i nedržavnih aktera,uključujući botnet napade kako bi se ometala informacijska infrastruktura,neovlašteni pristup i presretanje podataka i komunikacija ili manipulaciju ili uništenje podataka i sustava

- strategije kiberkriminala su primarno usmjerene prevenciji i zaštiti od kriminalnih djela najšireg kruga fizičkih i pravnih osoba

- u **prvom redu se odnose na prevenciju,istragu i kazneni progon počinitelja:**

**1)** kaznenih djela protiv sigurnosti,tajnosti i cjelovitosti računalnih podataka i sustava (neovlaštenog pristupa, ometanje sustava, ometanje podataka i zloporabu naprava)

**2)** kaznenih djela počinjenih putem,tj.uz pomoć računalnih sustava (računalne prijevare,računalnog krivotvorenja,dječje pornografije,povrede autorskog i srodnih prava, rasizma i ksenofobije)

**3)** u širem smislu,obuhvaćena su i sva druga djela pri čijem počinjenju se javljaju elektronički dokazi

- njihova primarna uloga je prevencija i aktivnosti kaznenog pravosuđa kako bi se ostvarila vladavina prava i zajamčilo visok stupanj zaštite ljudskih prava i temeljnih sloboda

- u provođenju ovih strategija razlikuju se i strateški prioriteti kao i subjekti između kojih se odvija suradnja u realizaciji navedenih ciljeva, a ti **strateški prioriteti se odnose na:**

**1)** politike i strategije za borbu protiv kibernetičkog kriminala

**2)** potpunu i učinkovitu pravnu osnovu za kaznenopravnu akciju

**3)** specijalizirane jedinice za kiberkriminal

**4)** obuku policije

**5)** osposobljavanje u području pravosuđa

**6)** financijske istrage i prevenciju i kontrolu prijevara i pranja novca na internetu

**7)** suradnja između policije i davatelja usluga

**8)** učinkovitiju regionalnu i međunarodnu suradnju

- moguća su **2 pristupa promicanja kibersigurnosti:**

**1)** vlade mogu razvijati specifične strategije kiberkriminala usporedno s onima za kibersigurnost (u tom slučaju sinergija i komplementarnosti između inače odvojenih strategija trebaju biti ugrađene u njih)

**2)** vlade mogu ugraditi i poboljšati komponente kiberkriminala unutar strategije kibersigurnosti ( to će zahtijevati ponovno razmatranje i širenje koncepta kibersigurnosti kako bi ono obuhvatilo ciljeve i načela kaznenog pravosuđa)

**9.2.3. Organizacijsko-tehnološke pretpostavke informacijske sigurnosti**

- obuhvaćaju ukupnost mjera,metoda,postupaka i pravilnika kojima se postiže zadovoljavajući stupanj njihove sigurnosti,tj. nesmetano korištenje njihovim resursima od strane za to ovlaštenih korisnika

- podrazumijeva poduzimanje niza aktivnosti koje prethode uspostavi zaštitnih mehanizama

- njihova efikasna primjena ne ovisi samo o kvaliteti tehničke osnovice koja se uvodi i načinu na koji se koristi,nego ovisi o onima koji je isporučuju,uspostavljaju,koriste i nadziru,a to se odnosi na stručne kadrove i sve one koji se takvim sustavom koriste u svom radu

- **problemi** koji se pri tom javljaju su rezultat njihovih posebnih značajki, među kojima treba istaknuti one **koje se odnose na:**

**a)** gustoću podataka

**b)** nevidljivost podataka

**c)** dostupnost podataka

**d)** krivotvorenje

**e)** zadržavanje

**f)** razuzdanost

- tome treba dodati globalni karakter inform.-komunik. tehnologija i njihovu dostupnost i široku rasprostranjenost

- glavni koraj u ostvarivanju ciljeva je uspostavljanje i provođenje efikasne **sigurnosne strategije,tj. sigurnosne politike**

**Uspostavljanje sigurnosne strategije**

- njen primarni cilj je zaštititi kritičnu infrastrukturu

- **Zakon o kritičnim infrastrukturama** razlikuje nacionalne i Europsku kritičnu infrastrukturu

- **Europska kritična infrastruktura** označava kritičnu infrastrukturu koja je od interesa za najmanje 2 članice

- **nacionalne kritične infrastrukture** su sustavi,mreže i objekti od nacionalne važnosti čiji prekid djelovanja ili prekid isporuke roba ili usluga može imati ozbiljne posljedice na nacionalnu sigurnost,zdravlje i živote ljudi,itd.

- **sektori nacionalnih kritičnih infrastruktura** određuju se odlukom **Vlade RH,a odnose se na:**

**a)** energetiku

**b)** komunikacijsku i informacijsku tehnologiju

**c)** promet

**d)** zdravstvo

**e)** vodno gospodarstvo

**f)** hranu

**g)** financije

**h)** proizvodnju,skaldištenje i prijevoz opasnih stvari

**i)** javne službe

**j)** nacionalne spomenike i vrijednosti

- **sigurnosna strategija mora ispuniti 5 temeljnih funkcija:**

**1)** mora odvratiti ljude od pokušaja da čine neovlaštena djela

**2)** moraju spriječiti uspješno izvršenje računalnog kaznenog djela

**3)** mora otkriti zloupotrebe kako bi se onemogućilo izvršenje cijelog djela

**4)** mora minimizirati učinke i štete od računalnih zloupotreba

**5)** sigurnosne mjere moraju zadovoljiti određene pravne zahtjeve

- **ta strategija se provodi na svim nivoima i obuhvaća sve korisnike sustava,a sadrži:**

**1)** administrativne i organizacijske mjere

**2)** analizu rizika

**3)** donošenje sigurnosnih programa

**4)** donošenje plana u slučaju nužde

**Ad 1) Administrativne i organizacijske mjere**

- **svrha administrativnih i organizacijskih postupaka i mjera** je da stvore pretpostavke za definiranje i provođenje sigurnosne politike te nadzor nad ostvarivanjem postavljenih zadataka,a tim je postupcima obuhvaćen niz radnji,od kojih su posebno važne:

**a)** **Analiza sigurnosnih troškova**

**- obuhvaća:**

**1)** procjenu troškova za uspostavu i provođenje sigurnosne politike

**2)** procjenu šteta do kojih bi došlo u slučaju gubitka ili ugrožavanja računalnog sustava

**3)** procjenu troškova da bi se nakon napada na informacijski sustav izvršio povrat u prijašnje stanje

- ova analiza je neophodna radi ocjene ekonomičnosti informac. sustava,utvrđivanja prioriteta u zaštiti i planiranja sredstava potrebnih da bi se ostvario zadovoljavajući stupanj njihove sigurnosti

**b) Utvrđivanje nadležnosti i odgovornosti**

- važno je unaprijed odrediti nadležnost i odgovornost svakog pojedinca i timova zbog podataka i radnji koje je potrebno provesti radi donošenja i provođenja sigurnosne strategije

- unaprijed se mora znati tko je odgovoran za provođenje svake pojedinačne faze i za nadzor tih aktivnosti

- utvrđivanje odgovornosti podrazumijeva upoznavanje korisnika s njihovim pravima i dužnostima u odnosu na korištenje resursom inform.sustava,a nužno ih je upoznati i s mogućim posljedicama

**c) Provođenje klasifikacije podataka**

- potrebno je izvršiti klasifikaciju podatka s obzirom na stupanj važnosti,tj. povjerljivosti te odrediti one koji su odgovorni da o njihovoj tajnosti,dostupnosti,vjerodostojnosti i cjelovitosti vode računa

- prema **Zakonu o tajnosti podataka**, **neklasificirani podatak je** podatak bez utvrđenog stupnja tajnosti kojim se korisiti u službene svrhe kao i podatak koji je RH tako označenog predala druga država

- **klasificirani podatak je** onaj koji je nadležno tijelo, u propisanom postupku, takvim označilo i za koji je utvrđen stupanj tajnosti, kao i podatak kojeg je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom RH surađuje (takvim se mogu proglasiti podaci radi prikrivanja kaznenog djela,prekoračenja ili zlouporabe ovlasti te drugih oblika nezakonitih postupanja u državnim tijelima)

**- stupnjevi tajnosti podataka:**

**1) vrlo tajno** – podaci čije bi neovlašteno otkrivanje nanijelo nepopravljivu štetu nacionalnoj sigurnosti i vitalnim interesima RH, a osobito sljedećim **vrijednostima:**

**a)** temelji Ustavom utvrđenog ustrojstva RH  
**b)** neovisnost, cjelovitost i sigurnost RH  
**c)** međunarodni odnosi RH  
**d)** obrambena sposobnost i sigurnosno-obavještajni sustav  
**e)** sigurnost građana  
**f)** osnove gospodarskog i financijskog sustava RH  
**g)** znanstvena otkrića, pronalasci i tehnologije od važnosti za nacionalnu sigurnost RH

**2) tajno** – podaci čije bi neovlašteno otkrivanje **teško naštetilo** prethodnim vrijednostima

- **klasificiranje vrlo tajnih i tajnik podataka mogu provoditi:** Predsjednik Republike Hrvatske, predsjednik Hrvatskog sabora, predsjednik Vlade Republike Hrvatske, ministri, Glavni državni odvjetnik, načelnik Glavnog stožera Oružanih snaga RH i čelnici tijela sigurnosno-obavještajnog sustava RH te osobe koje oni za tu svrhu ovlaste (svi oni mogu pisanim putem ovu ovlast prenijeti na druge osobe isključivo u okviru njihovog djelokruga)

**3) povjerljivo** – podaci čije bi neovlašteno otkrivanje **naštetilo** prethodnim vrijednostima

**4) ograničeno** – podaci čije bi neovlašteno otkrivanje naštetilo djelovanju i izvršavanju zadaća državnih tijela u obavljanju poslova obrane, sigurnosno-obavještajnog sustava, vanjskih poslova, javne sigurnosti, kaznenog postupka te znanosti, tehnologije, javnih financija i gospodarstva ukoliko su podaci od sigurnosnog interesa za RH

- klasificiranje podataka povjerljivo i ograničeno mogu i čelnici ostalih državnih tijela

- sve osobe, osim predsjednika RH, predsjednika Sabora i predsjednika Vlade, kojima je pristup klasificiranim podacima ( vrlo tajno,tajno i povjerljivo) nužan za obavljanje poslova moraju prethodno dobiti **certifikat,tj. Uvjerenje o obavljenoj sigurnosnoj provjeri** koji izdaje **Ured Vijeća za nacionalnu sigurnost** o čemu vodi registar

- razlozi za neizdavanje certifikata mogu biti sigurnosne zapreke,kao što su: neistinito navođenje podataka u upitniku za sigurnosnu provjeru,činjenice koje su posebnim zakonom propisane kao zapreka za prijam u državnu službu te izrečene stegovne sankcije i druge činjenice koje predstavljaju osnovu za sumnju o povjerljivosti ili pouzdanosti osobe za postupanje s klasificiranim podacima

- u tom slučaju, Ured će izdati rješenje kojim odbija izdavanje certifikata (protiv rješenja nije dopuštena žalba,ali osoba kojoj se uskraćeno izdavanje certifikata može pokrenuti upravni spor u roku od 30 dana od primitka rješenja)

- postupak klasifikacije je podložan periodičnoj procjeni vlasnika podataka koji rezultira promjenom stupnja tajnosti ili deklasifikacijom podataka (procjena najmanje jednom u 5 g. za vrlo tajno, 4 g. za tajno,3 g. za povjerljivo i 2 g. za ograničeno) 🡪 u slučaju promjene stupnja ili deklasifikacije,pismenim putem treba obavijestiti sva tijela kojima je podatak bio dostavljen

- sve zainteresirane osobe mogu od vlasnika podataka zatražiti pristup pozivajući se na **Zakon o pravu na pristup informacijama**

- u tom slučaju,on je dužan ocijeniti razmjernost između prava na pristup informacijama i zaštite prethodno navedenih vitalnih interesa RH,a pri tome primijenjuje tzv. **test razmjernosti i javnog interesa** koji predstavlja procjenu razmjernosti između razloga za omogućavanje pristupa informaciji i razloga za ograničenje te onemogućavanje pristupa informacijama ako prevladava javni interes

- nakon probavljenog mišljenja Ureda Vijeća za nacionalnu sigurnost vlasnik može odlučiti o zadržavanju stupnja tajnosti,promjeni stupnja,deklasifikaciji ili oslobađanju od obveze čuvanja tajnosti podataka (osoba kojoj je uskraćen pristup inf. može pokrenuti upravni spor)

**d) Nadzor i kontrola nad provođenjem zadane sigurnosne politike**

- dužnost nadzora i kontrole se odnosi na sve ovlaštene korisnike sustava

**Zaštita podataka**

- **zaštita povjerljivih podataka** uključuje fizičku sigurnost,ljudsku sigurnost i sigurnost sustava za obradu podataka,a može uključivati i komunikacijsku sigurnost

- **zaštita tajnih podataka** obuhvaća samo ljudsku,fizičku i kriptografsku sigurnost jer se na mehanizme sustavne i komunikacijske sigurnosti ne može osloniti

- **zaštita strogo tajnih podataka** zahtijeva da se pažnja posveti eliminaciji neželjenog zračenja i kontroli tehničkog nadzora

- obvezu tehničke i ustrojstvene zaštite nalazimo i ZZOP-u, ZEK-u i Zakonu o državnoj informacijskoj infrastrukturi

- ZZOP propisuje da podaci u zbirkama OP moraju biti odgovarajuće zaštićeni od slučajne ili namjerne zloporabe,uništenja,gubitka,neovlaštenih promjena ili dostupa

- voditelj zbirke OP i primatelj su dužni poduzeti tehničke,kadrovske i organizacijske mjere zaštite OP koje su potrebne da bi se OP zaštitili od slučajnog gubitka ili uništenja te dr. zlouporaba te utvrditi obvezu osoba koje su zaposlene u obradi podataka, napotpisivanje izjave o povjerljivosti

- ZEK propisuje da operatori javnih komunikacijskih usluga moraju poduzeti odgovarajuće tehničke i ustrojstvene mjere kako bi se zaštitila sigurnost njihovih usluga,a zajedno s operatorima javnih komunikcijskih mreža poduzimaju potrebne mjere zaštite sigurnosti elektroničke komunikacijske mreže i usluge ; takve mjere moraju:

**1)** osigurati da OP mogu pristupiti samo ovlaštene osobe u zakonom dopuštene svrhe

**2)** štititi prenošene ili pohranjene OP od zloporaba

**3)** osigurati primjenu sigurnosne politike u odnosu na obradu OP

- nadzor nad provedbom tih mjera provode HAKOM i AZOP

- ZDII propisuje obvezu sustavne zaštite i sigurnosti informacijske infrastrukture sukladno propisima o sigurnosti informacijskih sustava

**Ad 2) Analiza rizika**

- analiza rizika označava razmatranje mogućih scenarija prijetnji kako bi se ocijenile ranjivosti i mogući učinak poremećaja u radu kritične infrastrukture ili njezina uništenja, odnosno prijetnji tajnosti,cjelovitosti i dostupnosti računalnih podataka,programa ili sustava u javnom ili privatnom sektoru

- ona prethodi samom donošenju sigurnosnog programa sa svrhom pružanja odgovora na **5 temeljnih pitanja:**

**1)** koji su najčešći ciljevi napada i kojim se dobrima pruža zaštita

**2)** koje su slabosti sustava

**3)** koje su opasnosti za sustav

**4)** koje su moguće protumjere

**5)** tko su mogući počinitelji

- da bi olakšali analizu,koristimo se raznim paketima

**Koji su ciljevi napada i koja dobra treba zaštititi?**

- **najčešći ciljevi napada su:**

**1)** vojna i obavještajna računala (meta špijunaže)

**2)** poslovna računala (cilj su konkurencije)

**3)** računala bankovnih i drugih financijskih institucija (cilj profesionalnih kriminalaca)

**4)** računala drugih organizacija,a pogotovo vladina i javnih službi (meta terorista)

**5)** računala svakog poduzeća (meta zapsolenika ili bivših zaposlenika, studenata i bivših st.)

**6)** svaka organizacija može biti cilj hakera

- primarni zadatak sigurnosne strategije je osigurati da se na ekonomičan način pribave informacije te da one budu povjerljive,točne i vjerodostojne

- **najčešći objekti zaštite od zloupotreba:** računalni podaci,programi,tehnička osnovica i sredstva komunikacije

- dostupnost je obilježje informacijskih sustava,dok se tajnost i cjelovitost odnose na podatke i informacije

- **dostupnost znači** da informacijski sustavi moraju biti u predviđeno vrijeme i na propisan način dostupni ovlaštenim korisnicima

- **tajnost znači** da podaci moraju biti prikupljeni,obrađivani i poznati samo ovlaštenim osobama, dok se **cjelovitost odnosi** na potpunost i točnost podataka i informacija

- zaštitu treba pružiti i korisnicima,komunikciji te objektima i prostorijama u kojima se nalazi tehnička osnovica i mediji s pohranjenim podacima i programima

**Koje su ranjivosti (slabosti) sustava?**

- ranjivost sustava se odnosi na njihove vitalne točke koje mogu biti cilj napada (potrebno ih je unaprijed identificirati i odrediti prioritete)

- većina slabosti proizlazi iz neodgovarajuće organizacije,nedostatnih ulaganja i manjkavog interesa za zaštitu i sigurnost sustava što rezultira neprovođenjem sigurnosne politike

- **razlikujemo:**

**a) statičnu ranjivost sustava** - ostaje relativno ista kroz duže vrijeme jer se uvjeti ne mijenjaju

**b) dinamičnu ranjivost sustava** - u kraćem roku može doći do promjene

- većinom se slabosti odnose na softver (sistemski,korisnički i komunikacijski),hardver, komunikaciju,pogrešnu implementaciju ili konfiguraciju sustava,neobaviještenost i neobrazovanost ljudi,nedostatan nadzor,itd.

- **glavne točke ranjivosti su** procesori,uređaji za pohranu podataka,komunikacijska oprema,udaljena računala i terminali,korisnici i sistemsko osoblje

- ranjivost računalnih i informacijskih sustava može biti posljedica fizičke ranjivosti, ranjivosti od prirodnih uzroka i katastrofa koje mogu dovesti do oštećenja ili uništenja tehničke, programske i podatkovne osnovice te ranjivosti softvera i hardvera , ljudske ranjivosti, komunikacijske ranjivosti,iskorištavanje raznih slabosti,ranjivosti medija za pohranu podataka

- **najslabiju točku čine** ljudi,zaposlenici ili vanjski suradnici organizacije koja je meta napada

**Koje su opasnosti za sustav?**

- opasnosti mogu biti izazvan elsučajnim ili namjernim radnjama poduzetim od strane unutarnjih ili vanjskih počinitelja ili pak događajima koji se mogu predvidjeti,ali to nije učinjeno ili se njihobo nastupanje ne može predvidjeti

- **opasnosti prijete od:** ljudi,stvari i događaja, a njihove radnje mogu biti slučajne i namjerne

- **opasnosti koje prijete sustavu mogu dovesti do** uništenja ili krađe hardvera,krađe izvornog koda,sabotaže računala,krađe podataka ili medija na kojima su pohranjeni,neovlaštenog korištenja računalnim resursima

- **najčešće su posljedica:**

**1)** prikrivenih napada zaposlenika (subverzija)

**2)** nenamjernih radnji zaposlenika (nehaj)

**3)** slučajnih događaja

**4)** namjernih napada osoba koji nisu zaposlenici (prikriveno i prijevarno)

**5)** otvorenih napada izvana (sila)

**6)** otvorenih napada zaposlenika

**7)** nenamjernih radnji vanjskih osoba (ulazne greške)

- s obzirom na to prema kome ili prema čemu su upravljene,**opasnosti možemo podijeliti u 4 skupine,a mogu se odnositi na:**

**1)** povrede fizičke sigurnosti

**2)** povrede sigurnosti ljudi

**3)** povrede komunikacija i podataka

**4)** povrede operativne sigurnosti

**Koje su moguće protumjere?**

- protumjere imaju za cilj da preventivno djeluju kako bi počinitelja odvratili od činjenja takvih radnji ili ako je radnja izvršenja već poduzeta, spriječile i zaustavile u dovršenju

- one obuhvaćaju tehničke mjere zaštite i niz postupaka i metoda kojima se takve zloupotrebe odbijaju ili se ublažuju njihove negativne posljedice

- **7 je vrsta obrambenih mehanizama,a među njima se posebno ističu one mjere kojima se štiti:**

**1)** fizička sigurnost – bavi se fizičkom kontrolom pristupa sustavu

**2)** kadrovska sigurnost – bavi se odabirom i nadzorom osoblja

**3)** enkripcija osjetljivih(tajnih) informacija- koristi se za zaštitu komunikacije čineći podatke u tranzitu nejasnima bilo kome drugome osim ovlaštenom korisniku

**4)** tehnička nadzorna inspekcija - bavi se obranom od ometanja rada uređaja

**5)** sprječavanje kompromitirajućeg zračenja – može biti potrebno zato što oprema proizvodi akustično i elektromagnetsko zračenje koje se može presresti i analizirati

**6)** sigurnost komunikacija (veza) – bavi se osiguranjem komunikacijskih linija od fizičkog pristupa koji je potreban da bi se neovlašteno pristupilo sustavu

- posebna grupa protumjera odnosi se na edukaciju kadrova

**Koji su mogući počinitelji (od koga se štitimo)?**

- ovisno o tome radi li se o **unutarnjim** ili **vanjskim počiniteljima**,razlikujemo njihove nakane i motive

- da bi ostvarili svoj cilj,koriste se svim mogućim sredstvima,a ovisno o vrsti napada razlikuju se mogući počinitelji,metode otkrivanja i dokazi koje treba prkupiti

- nakon što smo dobili odgovore na pitanja,te podatke treba dokumentirati,a s ostalim dijelovima koji se ne smatraju strogo povjerljivima i vitalnim za sigurnost,treba upoznati sve korisnike sustava

- **analizu rizika treba ponoviti u slučajevima:**

**a)** zloupotrebe unutar organizacije

**b)** većih kadrovskih promjena

**c)** zaključenja novih poslova koji zahtijevaju rad s povjerljivim podacima

**d)** spajanja ili dr.oblika neposredne suradnje s drugim organizacijama

**e)** kada sustav bude metom terorističkih ili militantnih grupa

**f)** otkrivanja novih prijetnji

**g)** političkih događaja koji utječu na organizaciju,itd.

**Ad 3) Donošenje sigurnosnog programa**

- **sigurnosni program se sastoji od 4 komponente koje se odnose na:**

**a) fizičku sigurnost**

**b) ljudsku sigurnost**

**c) komunikacijsku sigurnost**

**d) operativnu sigurnost**

**a) Fizička sigurnost**

- obuhvaća one postupke i mjere kojima je cilj da se spriječi neovlašten pristup i ugrožavanje računalnih sustava,druge opreme i okruženja u kojem se oni nalaze,a koje mu prijeti od:

**1)** vanjskih utjecaja čije se nastupanje i djelovanje ne može predvidjeti

**2)** kao i one koje neovlaštenim osobama onemogućavaju neposredan,fizički pristup sustavu ili nekom drugom zaštićenom dobru,tj.objektu i prostorijama u kojima se oni nalaze

- imaju za cilj ublažiti i ukloniti štetne posljedice do kojih je došlo zbog djelovannja tih događaja,stvari ili ljudi

- u tu svrhu koriste se raznim **sigurnosnim mjerama poput :**

**1)** fizičke službe sigurnosti

**2)** alarmni sustav

**3)** protupožarni sustav

**4)** sustav za nadzor okoline i vaćnih prostora unutar objekta

**5)** razne identifikacijske kartice za pristup zgradi ili prostoriji u kojoj se nalaze inf.resursi

**6)** biometrijske metode koje se temelje na fizičkim ili karakternim osobinama neke osobe

- kod fizičke sigurnosti važno je voditi računa o:

a) planiranju položaja

b) kontroli pristupa područjima gdje je takav pristup ograničen

c) zaštiti od fizičkog oštećivanja

d) zaštiti od strujnih i drugih kvarova u okruženju

e) zaštiti medija za elektroničku obradu podataka i opskrbi

**b) Ljudska sigurnost**

- obuhvaća sve one postupke i mjere kojima je cilj da se spriječe štete do kojih može doći namjernim ili slučajnim postupcima zaposlenika i drugih osoba koje imaju pristup sustavu kao i drugih osoba koje su mogući počinitelji zloupotreba (odnosi se na provjeru podataka o novim kadrovima ili o dobavljačima i na poticanje svijesti i opreza kod postojećih)

- radna motivacija podrazumijeva stalni nadzor rada i korištenja sustavom od strane zaposlenih i drugih osoba koje mu mogu pristupiti uz pomoć raznih metoda kojima se provjerava pristup i korištenje sustavom kao i ocjenu sposobnosti postojećih kadrova

**c) Komunikacijska sigurnost**

- obuhvaća mjere kojima je cilj da se osigura sigurna,nesmetana,cjelovita i tajna komunikacija i razmjena podataka između ovlaštenih korisnika,koja se odvija neposrednim daljinskim pristupom ili putem lokalne (Local Area Network),međumjesne ili međugradske (Wide Area Network) i globalne računalne mreže (Internet,Internet 2)

- te se mjere ponajprije odnose na kontrolu pristupa računalnom sustavu,zaštitu kablova i kontrolu komunikcijskih kanala,osiguranje tajnosti,točnosti,vjerodostojnosti i cjelovitosti podataka koji se razmjenjuju u komunikaciju te druge mjere zaštite kojima se štite resursi informacijskog sustava ili njegovi važniji dijelovi od raznih zloupotreba do kojih može doći pri takvom načinu rada

**d) Operativna sigurnost**

- odnosi se na zaštitu hardvera i softvera,a usmjerena je na očuvanje njihova funkcionalnog integriteta

- obuhvaća i mjere zaštite od napada na postupke kojim se koriste za sprječavanje i otkrivanje zloporaba

- zadatak operativne sigurnosti je da predvidi mjere kojima će se mogućim počiniteljima onemogućiti neovlašteni pristup sustavu, da pravovremeno otkrije pokušaje takvih povreda i spriječiti prenošenje ili aktiviranje malicioznih programa te da obuči zaposlenike kako da uoče i druge slične pokušaje

- **programom operativne sigurnosti treba:**

**1)** prepoznati informacije do kojih počinitelji žele doći na nekom računalnom sustavu

**2)** utvrditi metode koje se u tome mogu koristiti

**3)** razviti protumjere kako bi se spriječila učinkovitost takvih metoda

- sastavni dio ove sigurnosti čini **stalan nadzor i kontrola rada i korištenja sustavom** (koriste se raznim softverskim alatima za nadzor – SATAN, ISS, COPS, SPI)

**Ad 4) Planiranje u slučaju nužde (Contingency Planning)**

- contingency planning, crisis managment, disaster planning ili disaster recovery

- koristi se kada dođe do ugrožavanja zaštićenih dobara neovisno o razlogu zbog kojeg je do toga došlo i njime moraju biti predviđeni postupci u slučajevima kada je do ugrožavanja došlo kao posljedica djelovanja raznih događaja,stvari ili ljudi

- cilj tog plana je da se otklone štetne posljedice i smanji vrijeme od trenutka nastanka štete do ponovnog aktiviranja informacijskog sustava

- **plan u slučaju nužde ima 4 glavne komponente:**

**1) korištenje mjerama za otkrivanje napada**

**2) sastavljanje ekipe**

**3)** odlučivanje kako će ekipa **odgovoriti u različitim situacijama** i kako dokumentirati svoju aktivnost za kasnije pravne i financijske potrebe

**4)** osiguranje da se **plan s vremenom mijenja**

- planom moraju biti predviđeni i postupci koji će na djelotvoran, ekonomičan i siguran način omogućiti povrat u prijašnje stanje, tj. stanje koje je prethodilo samom početku izvršenja tog djela,odnosno početku događaja zbog kojih je nastupila šteta

- osnovni preduvjet efikasne sigurnosne strategije čini permanentno preispitivanje i analiziranje provođenja i ispunjavanja zadane sigurnosne politike te praćenje i implementiranje novih zaštitnih mjera