ELEKTRONIČKI DOKAZI U SUDSKOM POSTUPKU I RAČUNALNA FORENZIČKA ANALIZA

Dr. sc. Jozo Čizmić, redoviti profesor
Dr. sc. Marija Boban, docentica
Pravni fakultet Sveučilišta u Splitu

UDK: 343.14:004.056
Ur.: 23. siječnja 2017.
Pr.: 6. veljače 2017.
Izvorni znanstveni rad

Sažetak

Današnja slika informacijskog društva usvaja terminologiju suvremenog rječnika globalizacije i uključuje termine kao što su konvergencija, digitalizacija (medija, tehnologija i/ili telekomunikacija) i mobilnost bilo ljudi bilo tehnologija. Iz svake riječi odiše napredak, razvoj, pozitivan predznak uspona informacijskog društva. S druge strane u virtualnom okruženju tradicionalni dokazi u sudskom postupku s dokumenta na papirnatoj podlozi postaju elektronički dokazi, a njihovi upravljački procesi i kriteriji dopuštenosti mijenjaju se u odnosu na tradicionalne dokaze. Brzi rast računalnih podataka stvorio je nove mogućnosti i rast novog oblika računalnog, ali i kibernetičkog kriminaliteta, a tako i nove načine dokazivanja u sudskim postupcima, nedostupne prije samo nekoliko desetljeća.

Autori u ovom radu opisuju nove trendove razvoja informacijskog društva i nastanak elektroničkih dokaza s naglaskom na utjecaj razvitka računalnog kriminaliteta na elektroničke dokaze; na pojam, pravno uređenje i dokaznu snagu elektroničkih dokaza i posebno elektroničkih isprava te na problematiku vještačenja elektroničkih dokaza i elektroničkih isprava u sudskom postupku.

Ključne riječi: *(građanski) sudski postupak, računalni kriminalitet, elektronički dokazi, informacijska tehnologija.*

1. UVOD

1.1. Opći trendovi razvitka informacijskog društva, vezani progresivnim tehnološkim razvojem i napretkom informacijskih tehnologija, uvelike otvaraju nova pitanja – pitanja ne samo zaštite tjelesne, prostorne, već i kibernetičke sigurnosti i zaštite podataka.[1] Ipak, samim procesom globalizacije utječe se na stvaranje

1 O kibernetičkoj sigurnosti i novim oblicima organiziranog kriminaliteta u digitalnom dobu i okruženju informacijskih tehnologija vidi u BOBAN, M., *Information and communication technologies and the new forms of organized crime in network society,* 39th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2016 - Proceedings, 2016., str. 1857-1862

potrebe za postavljanjem zaštite ne samo u fizičkom smislu, već postoji konstantan trud da se stvori zaštićen "osobni svijet", zadrži vlastita privatnost osobe što se u suvremenom svijetu i okruženju informacijskih tehnologija sve više čini nemogućom misijom.[2] Također, *nove informacijske tehnologije povezuju svijet u globalne mreže instrumentalnosti*.[3] Globalizacija kao svjetski proces utječe na otvaranje bilo državnih granica, bilo lokalnih zajednica i poboljšava uvjete svjetskog tržišta i svjetskih ekonomija potičući konkurentnost tržišta.[4] Nova (informacijska ekonomija) i razvoj svjetskog globalnog tržišta uvelike omogućava približavanje i smanjivanje prostornih komunikacijskih granica, međutim, utječe i na pojavu novih oblika kaznenih djela: *kibernetičkog kriminaliteta*. Samo procesiranje informacija korištenjem suvremenih informacijskih tehnologija potiče kontinuirani razvoj i unaprjeđenje informacijskog društva, a time i novog znanja. Stoga u informacijskom društvu koje se temelji na informacijskim tehnologijama i na tehnologijama za generiranje znanja, postoji bliska veza između kulture i proizvodnih snaga, iz čega zaključuje da je za očekivati nastajanje novih oblika društvene interakcije, kontrole i promjene, a još jedna veza između kulture i informacijskog društva koju opisuje je ta što je informacijsko društvo okarakterizirano važnošću koju u njemu ima *kulturni identitet* kao njegov *organizacijski princip*.[5]

U svijetu koje obilježavaju *simultana globalizacija* i *fragmentacija,* nameće se ključno pitanje: *Kako spojiti nove tehnologije i pravnu znanost, kako pratiti nove oblike zlouporabe računalnih sustava i kako prikupljati dokaze?* Iz gore navedenoga proizlazi zaključak da se u svijetu zamjećuje trend porasta – sve veća poveznaost između *informacijskih tehnologija* i *razvoja pravne znanosti koja prati računalnu forenziku.* Jedina nepobitna činjenica, unatoč ovakvom uočenom trendu globalizacije, jest da nemaju svi jednaku mogućnost pristupa *informacijskoj tehnologiji* i i*nternetu*[6]

2 Prvi koraci informacijskih društava daju sliku društva kojemu identitet prevladava kao načelo organizacije dok je osobiti društveni trend 1990-ih prevladavao oko izgradnje društvenog djelovanja i politike oko primarnih identiteta – bez obzira jesu li oni bili pripisani, ukorijenjeni u povijest i geografiju ili novoizgrađeni prilikom potrage za smislom ili duhovnošću. Društveni odnosi, definirani su *vis-a vis* ostalih na temelju onih kulturnih vrijednosti koje definiraju identitet. Pod identitetom u tom smislu podrazumijevan je proces kojim se društveni sudionik reorganizira i izgrađuje smisao ponajprije na temelju zadanog kulturnog atributa ili seta atributa, pri čemu se isključuje iz šireg odnosa prema ostalim društvenim strukturama. Vidi CASTELLS, M., *The information age: economy, society and culture,* Vol. I: The rise of the network society, Cambridge: Blackwell Publishers, 2000., str. 57.

3 U razmatranju tih vrsta promjena ističe se sociolog Manuel Castells. Njegovo je mišljenje da su ljudi sada preopretećeni tom pretpostavkom. Toliko su okruženi medijima, kao interpretatorima stvarnosti, da stvarnost koja se zbiva izvan dosega ljudskih osjetila, ljudskog zdravog razuma, ne mogu drukčije dohvatiti nego putem onoga što nam mediji serviraju. Zato prema Castellsu, virutalna stvarnost postaje "stvarna virutalnost". Ibid., CASTELLS, M., str. 357.

4 O utjecaju globalizacije i novim oblicima korištenja informacijskih tehologija vidi šire u MONROE E. PRICE, *Free Expression, Globalism, and the New Strategic Communication*, Cambridge University Press, 2014., str. 101

5 Usp. TOURAINE, A., *Qu'est-ce que la democratie?,* Fayard, Pariz, 1994., str. 4.

6 *Internet* predstavlja globalni komunikacijski sustav koji povezuje i spaja računalne mreže pojedinih zemalja i organizacija te tako omogućava posjednicima računala ciljem svijeta da putem svojih lokalnih mreža i telefonskih mreža međusobno komuniciraju, razmjenjuju

stvarajući time novi oblik *kulturološkog razdora* između informacijski bogatih i informacijski siromašnih koja se u novoj terminologiji naziva *digitalna podjela*. Je li upravo taj aspekt u ovoj podjeli i sudbonosan? Jesu li na neki način *informacijski siromašni* zaštićeni od globalizacijskih efekata novih aspekata kaznenih djela i njihovog zadiranja u *informacijsku privatnost i osobnost* – pokazat će budućnost.[7]

Suvremeni način poslovanja i komuniciranja putem globalnih informacijskih mreža doveo je do sve veće povezanosti ne samo ljudi već i informacijskih sustava. Uz sve svoje blagodati takav način rada nosi u sebi i brojne opasnosti po sigurnost svih sudionika, kao i samih informacijskih sustava. Podatci i informacije, koji se unutar takvih sustava obrađuju, memoriraju i distribuiraju, kao i tehnička osnovica koja to omogućuje sve su češće cilj takvih zloupotreba, pa se zato i postavlja kao osnovni zadatak zahtjev za njihovom učinkovitom i cjelovitom zaštitom.[8]

Sve veća povezanost i upućenost informacijskih sustava na uključivanje u globalne informacijske mreže, u prvom redu internet, ali i na neke druge koje su nastale logičkim slijedom vremena, ali na istim principima doveli su do toga da se njihova zaštita više ne može promatrati i rješavati izolirano, već samo kao dio tog sustava. Takva otvorenost informacijskih sustava prema sve većem broju korisnika dodatno je oslabila njihovu sigurnost. Stoga je nužno da se pitanjima zaštite pristupi s jednog šireg, globalnog aspekta – aspekta globalnih informacijskih mreža koje ih sve više objedinjuju. Dakle, pitanja sigurnosti i zaštite interneta postaje jedno od osnovnih pitanja kako za same informacijske sustave i njihove korisnike tako i za cijelu međunarodnu zajednicu.[9]

1.2. Elektronički podatci danas su sveprisutan i značajan izvor informacija. Razvitkom informatike i informacijskih sustava stvorena su brojna elektronička i tehnička sredstva koja omogućavaju zapisivanje i snimanje svih vrsta informacija, događaja i pojava na elektroničke/digitalne medije te njihovu reprodukciju. Računala i komunikacijski uređaji mogu stvoriti i pohraniti u svojoj memoriji ogromne količine digitalnih podataka. Praksa široke primjene suvremenih informacijsko-komunikacijskih tehnologija na svim područjima ljudskog komuniciranja dovela je do toga da se, zbog niza prednosti (brzine i učinkovitosti) ove tehnologije primjenjuju i u sudovima u poslovnom (organizacijskom) i u funkcionalnom (postupovnom)

informacije i koriste brojne druge usluge. U fizičkom smislu, to je niz međusobno povezanih računalnih mreža, organiziranih na jedinstven način, sa zajedničkim komunikacijskim protokolima i mrežnim uslugama. Za razliku od ostalih informacijskih sustava, informacijsko-komunikacijski sustavi bave se prikupljanjem, obradom i distribucijom različitih informacijskih sadržajnih formi u cjelokupnom fizičkom komunikacijskom prostoru. Fizički komunikacijski prostori su komunikacijske mreže koje omogućavaju pretraživanje bilo koje lokacije u mreži s bilo koje druge lokacije u istoj mreži." Tako i šire GRBAVAC, V., PLENKOVIĆ, M., *Komunikacijski sustavi na prijelazu u 21. stoljeće*, Informatologija, br. 27., 1995., str. 1.

7 Tako i šire ČIZMIĆ, J., BOBAN, M., ZLATOVIĆ, D., *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost*, Sveučilište u Splitu Pravni fakultet, Split, 2016., str. 39.

8 Vidi NOORDA, C., HANLOSER, S., *E-discovery and data privacy: a practical guide*, Kluwer Law International, 2010., str. 191 - 199.

9 O tome vidi više u NOUWT, S., DE VRIES, B. R., PRINS, C., *Reasonable expectations of privacy?: eleven country reports on camera surveillance and workplace privacy,* Cambridge University Press, 2005.

pogledu.[10] Bitno je istaknuti kako tradicionalni dokazi prelaze s dokumenta na papirnatoj podlozi u virtualno okruženje i postaju *elektronički dokazi*, a njihovi upravljački procesi i kriteriji dopuštenosti mijenjaju se u odnosu na tradicionalni dokaz.[11] Brzi rast elektroničkih informacija stvorio je nove mogućnosti dokazivanja prema novim *elektroničkim dokazima* u sudskim postupcima, nedostupne prije samo nekoliko desetljeća. Ljudi često olako koriste nove oblike komunikacije, ne vodeći računa o tome da bi jednog dana elektroničke informacije mogle biti upotrebljene kao dokazno sredstvo u sudskom postupku.[12] S druge strane, samim elektroničkim dokazima lako je manipulirati pa je pri njihovoj uporabi u sudskom postupku nužno obratiti dodatnu pozornost.

2. RAČUNALNI KRIMINALITET

2.1. Pojam

Za valjanu primjenu elektroničkih dokaza u sudskom postupku, osim ocjene njihove dokazne snage, nužna je provjera njihove izrade, pohrane, prijenosa, čuvanja, vjerodostojnosti i nepromjenjivosti (arg. Zakon o elektroničkoj ispravi, čl. 12. st. 2.). Elektronički dokazi jedan su od najvažnijih čimbenika u području računalnog kriminaliteta. Računalo se pojavljuje kao ključan čimbenik počinjenja kaznenog djela i iako nema izravan učinak na slučaj ono sadržava elektroničke dokaze vrlo važne za istraživanje počinjenog računalnog kriminaliteta. Takav postupak, bilo da se radi o djelu počinjenom u stvarnom fizičkom svijetu ili putem mreže istražitelji mogu učiniti pretraživanje putem mreže u potrazi za elektroničkim dokazima, naziva se *računalna forenzička analiza* (dalje - RFA). Prema definiciji predstavlja *postupak utvrđivanja činjenica nad digitalnim medijima primjenom različitih metoda.* [13] Najčešće se koristi u postupcima sudskog dokazivanja, a sastoji se od niza analitičkih metoda za otkrivanje, prikupljanje, ispitivanje i skladištenje podataka te često podrazumijeva ispitivanje računalnih sustava kako bi se utvrdilo njihovo korištenje u ilegalnim ili neautoriziranim aktivnostima poput krađe poslovnih tajni, uništavanja intelektualnog vlasništva ili prijevare. [14]

Razvojem interneta i njegovim masovnim zadiranjem u sve pore ljudskog života, računalni kriminalitet sve više se širi na područje gospodarstva i utječe na brži razvoj tehnika operativnog kriminalističkog nadzora i naprednijih metoda i

10 Vidi PALAČKOVIĆ, D., *E–dokument i E-isprava – Legislativa i mogućnost primene u parničnom postupku*, "Pravni život", Beograd, godina LX, knjiga 549, 2011., broj 11, str. 771.

11 U tom smislu kod *Dopustivost elektroničkog dokaza pred sudom: Suzbijanje visokotehnološkog kriminala – I. dio*, Odvjetnik, 5-6/2007., str. 39.

12 Tako CHARLES W. ADAMS, C. W., Spoliation of electronic evidence: sanctions versus advocacy**,** 18 MICH. TELECOMM. TECH. L. REV. 1 (2011), str. 1., podatak dostupan na stranici: http://www.mttlr.org/voleighteen/adams.pdf. Vidi i CHORVAT, T. J., *E-Discovery and Electronic Evidence in the Courtroom*, Business Law Today, vol. 17, broj 1, Sept./Oct. 20.

13 Tako i šire CARNET, LS&S, *Osnove računalne forenzičke analize*, CCERT-PUBDOC-2006-11-174, 2006., dostupno na http://security.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2006-11-174.pdf, str. (03. 01. 2017.).

14 *Ibidem.*

tehnika operativne kriminalističke analitike i računalne forenzike jer se proširuje i krug mogućih počinitelja, kao i krug sredstava i metoda kojima se ostvaruju računalni napadi i napadi povezani s računalima.[15] Posebno zabrinjava povezanost počinitelja s raznim oblicima organiziranog kriminaliteta, a gotovo svakodnevno se javljaju nove metode, sredstva i oblici zlouporabe.[16]

Pravna regulativa u RH i u svijetu je dosta neujednačena, a prečesto i u novijoj praksi neučinkovita. S obzirom na to da se radi o globalnom problemu, za djelotvorno suzbijanje nisu dovoljni samo stručnjaci za sigurnost, ekspertne skupine i ostali organi za sprječavanje i suzbijanje kiberentičkog kriminaliteta, već treba ostvariti cjelovitiju koordinaciju i sveobuhvatnu akciju zakonodavstva i snaga reda u prevenciji računalnog kriminaliteta u sferi financijskog poslovanja. [17]

Nažalost, također svakodnevni rad putem računalnih mreža: elektroničke pošte, plaćanja računa i drugih oblika komunikacije, omogućava i razvoj svih oblika napada na informacijske sustave. Virtualni čovjekov svijet postaje sve više onaj prirodni ambijent u kojem on svakodnevno živi i djeluje. U tom svijetu i pomoću njega zadovoljava svoje povijesno nastale potrebe i razvija svoje ljudske snage svestranim komuniciranjem i podjednakim korištenjem tekovina kulture i civilizacije.[18] Da je to ipak tek početak jednoga novog epohalnog svjetskog zaokreta pokazuje i zbiljnost

15 Internet i digitalna tehnologija pružaju nove prilike za učenje, omogućuju pojedincima direktnu prodaju ideja, usluga ili proizvoda, pristup informacijama te zadovoljavanje emocionalnih i psiholoških potreba. Kao prošireni aspekt utjecaja javljaju se tzv. virtualne zajednice utemeljene na zajedničkim interesima koje često prerastaju u društvene mreže. Postupak ostvarivanja kontakta na daljinu i vezivanje zajedničkim interesima neminovno značajano utječe na kulturološko širenje temeljnih odrednica pojedine nacije. S jedne strane, definitivno znači obogaćivanje osobe na osobnoj razini kao i njen daljnji utjecaj na svoju okolinu. Ipak, postoji neodređena "meka" granica koja razdvaja to obogaćivanje od globalnog nadiranja u domenu osobnosti pojedinca. Vidi šire u KIM J. ANDREASSON, K. J., *Cybersecurity: Public Sector Threats and Responses*, CRC Press, 2012., str. 101.

16 O razvoju informacijskih i komunikacijskih sustava i utjecaju na društvene promjene te samom procesu digitalizacije vidi GRBAVAC, V., PLENKOVIĆ, M., *Komunikacijski sustavi na prijelazu u 21. stoljeće*, Informatologija, br. 27., 1995., str. 1-5.

17 Prema DRAGIČEVIĆU, A. i DRAGIČEVIĆU, D., "*Kiberkomunizmu je budućnost osigurana, zajamčena, i ne mogu ga u tom povijesnom pohodu zaustaviti sve birokracije, policije, špijunske službe i vojske ovoga svijeta a još manje pohlepne kaste kojima je profit važniji od čovjeka"*. Nadalje, autori smatraju da ovaj oblik "novog svijeta" ujedno znači i *novi društveni moral* i *novu društvenu etičnost*, s naglaskom na *obvezi prema ljudima, institucijama, predmetima, vjerovanjima, idejama, mjestima, prirodi, projektima, iskustvima, pustolovinama i pozivu*. Upravo taj novi društveni moral i nova društvena etika trebali bi pomicati obveze u osi dalje od osobnog ja - bilo samoodricanja ili samoispunjenja – i bliže povezanosti sa svijetom što predstavlja sudbonosan i nepovratan fenomen.. Usp. DRAGIČEVIĆ, A. i DRAGIČEVIĆU, D., *Doba kiberkomunizma*, str. 30-31.

18 Opisujući elemente bitne za razumijevanje informacijskog društva M. Castells uvodi pojam koji naziva *paradigma informacijskih tehnologija* i kaže da se suvremene društvene promjene mogu sagledati kao pomak od tehnologija koje su se temeljile na jeftinoj energiji prema tehnologijama koje se temelje na uglavnom jeftinim informacijama, što je izazvano razvojem i novim spoznajama na područjima mikroelektronike i telekomunikacija. Kroz tu paradigmu pokušava opisati novonastale društvene transformacije precizirajući elemente koje čine osnovu te paradigme, a time i osnovu informacijskog društva. Tako i šire CASTELLS, M., str. 56.

svakodnevnog života u kojoj polovica čovječanstva još nije stigla do tog stupnja razvoja, a druga polovica obitava u različito razvijenim zajednicama u kojima se staro i novo povezuje i isprepliće u raznovrsnim oblicima i kombinacijama. [19]

Ključnu ulogu imaju: veće zlouporabe komunikacijskih sredstava koje su prethodile konkretnom djelu računalnog kriminaliteta; brži razvoj i širenje telekomunikacijskih uređaja; nezaustavljiv razvoj i sve teže korištenje operativnih metoda i tehnika kriminalističke analitike, te računalnih mreža koje omogućuju neovlaštene pristupe; sve veća dostupnost računala i osobama bez velikog stručnog znanja; hakerski BBS-ovi (engl. *Bulletin Board System*)[20] koji omogućavaju tajnu komunikaciju i programe namijenjene provalama u sustave; pojava medija koji često neopravdano veličaju hakerske vještine i napade; sporost i relativna složenost (kompleksnost) donošenja pravne regulative na području materijalnog, procesnog i fiskalnog zakonodavstva u cilju prevencije računalnog kriminaliteta u sferi financijskog poslovanja. [21]

Mješovito informacijsko društvo, kao i svako ranije tranzicijsko zajedništvo, zakonito prate ostatci i tragovi prošlosti među kojima se pored pozitivnih susreću i brojni negativni suputnici. Od trenutka spoznaje da postoji nešto što je nazvano računalni kriminalitet, sagledavajući njegov opseg i sadržaj, još uvijek ne postoji općeprihvaćena definicija. Razlog za to su njegove osnovne karakteristike; šarolikost oblika kroz koje se izražava, brzina kojom se širi i različitost stajališta pravnih teoretičara. Računalni kriminalitet još uvijek ne predstavlja jednu zaokruženu i jedinstvenu kategoriju da bi ga se moglo staviti u točno određene okvire koji bi bili prihvaćeni jednako od teoretske struke i prakse. Međutim, jedno je sigurno, to je forma kojom se ispoljavaju različiti oblici kriminalne aktivnosti, forma koja će u budućnosti postati dominantna.

Neke od postojećih definicija su prejednostavne jer svode računalni kriminalitet samo na ona kaznena djela koja se ne bi mogla obaviti bez korištenja računala uz visoko stručno znanje računalnih operacija, iako praksa dokazuje suprotno. [22] Sve

19 Današnja suvremena Hrvatska nastoji se približiti procesima europskih integracija uz uzdizanje vlastitih kulturnih svojstava budući da jedino priznavanje vlastitog identiteta predstavlja osnovu za priznavanje kulturne raznolikosti. Ipak, proces globalizacije i još opasniji proces "kulturne globalizacije" prijeti integraciji u multimedijsku kulturu. Jedini ključ spasa predstavlja zapravo jednostavnim riječima očuvanje "vlastite posebnosti" i vlastitog kulturnog identiteta. Tako i šire vidi u TUĐMAN, M., *Informacijsko ratište i informacijska znanost,* Hrvatska sveučilišna naklada, Zagreb, 2008., str. 263 – 267.

20 BBS (eng. *bulletin board system*) je računalni sustav namijenjen razmjeni poruka, podataka, informacija i softvera daljinskim komuniciranjem uz pomoć modema. Pojavili su se i koristili i prije pojave WWW-a, a i danas su u širokoj uporabi. O protokolima i komunikacijskim paketima vidi više u CERF, V. G., KAHN, R. E., *A protocol for packet network interconnection,* IEEE Trans. Comm. Tech., vol. COM-22, V 5, May 1974., str. 627-641.

21 Vidi United Nations International cooperation in combating transnational crime, dostupno na http://www.uncjin.org/6e.pdf (28. 12. 2016.).

22 Kod računalnog kriminaliteta riječ je o više objekata zaštite jer se zaštita odnosi kako na sam računalni sustav, odnosno tehniku osnovicu u širem smislu, tako i na netjelesna dobra koja se pri njegovu radu pohranjuju, obrađuju i prenose. Riječ je o računalnim podatcima i programima. Problemi se javljaju jer se oni ne moraju nalaziti unutar samog računalnog sustava (npr. kod komunikacije i prijenosa podataka), a ne mogu se zbog svojih specifičnosti poistovjetiti s

je veći broj kaznenih djela u kojima se, posredno ili neposredno, koristi računalo i ne podrazumijeva specifična znanja zbog jednostavnosti i dostupnosti informatičke tehnologije, a posebno brojnih programa namijenjenih isključivo takvoj nezakonitoj aktivnosti. Čak postoje i primjeri kada je moguće ugroziti različite programe i podatke i bez neposrednog korištenja računala oštećenjem medija na kojemu se nalaze. U najopasnije se među njima ubraja i *računalni kriminalitet*. Ta uobičajena i sada već općenito prihvaćena sintagma *obuhvaća ukupnost počinjenih kaznenih djela kojima se neovlašteno utječe na korištenje, cjelovitost i dostupnost tehničke, programske ili podatkovne osnovice kompjutorskog sustava ili na tajnost digitalnih podataka.*[23] Zloupotrebe ove vrste postaju informacijskim razvojem sve učestalije, a po posljedicama sve opasnije.

Zaštita od računalnog kriminaliteta postaje važnom funkcijom društva jer se sa svakom tehnološkom inovacijom javljaju nove zloupotrebe počinjene na računalima ili uz njihovu pomoć. Susrećemo se na svim lokalnim, nacionalnim i regionalnim razinama, a ispreplitanjem računalnih mreža i ekspanzijom interneta i na svjetskim prostranstvima. Tomu uvelike pridonosi digitalni oblik dostupnih podataka i informacija, a isto tako i mogućnost da se zlodjela počine pristupom na daljinu, korištenjem, upravljanjem i manipuliranjem podatcima. Pogoduje im, također, okolnost da se u istim pojavama i procesima nalazi i prepleće dopušteno i nezakonito, a učinci se postižu istim sredstvima i podjednakim metodama i postupcima koje se koriste u svakodnevnom radu i korištenju informatičke tehnologije. Također, kriminalne aktivnosti potpomognute novim tehnologijama razvijaju se takvom brzinom da je istražiteljima gotovo nemoguće držati korak i pratiti ih.

2.2. Nastanak računalnoga kriminaliteta

Jednako kao ni za unificiranu definiciju računalnog kriminaliteta, tako ni za njegov nastanak, nema jedinstvenoga stajališta. Čak postoje oprečna mišljenja, jedni uzimaju u obzir pojavu prvih računala, dok se drugi baziraju na pojavu elektroničkih računala.[24]

Nadalje, nastanak negativne manipulacije računalima kroz povijest veže se

nositeljem čak i onda kada se na njemu nalaze. Štoviše, moguće ih je ugroziti i bez neposrednog posredovanja računala (npr. oštećenje gotovo bezvrijednog medija na kojem se nalaze). Vidi šire BAČIĆ, F., *Krivično pravo-opći dio,* str. 99.

23 Važno je napomenuti da se u ovoj definiciji izraz «utjecaj» odnosi na svaku onu radnju kojom se neovlašteno i namjerno otuđuje, oštećuje, mijenja ili onemogućava korištenje tehničke, programske ili podatkovne osnovice, kao i one radnje kojima se neovlašteno pribavljaju ili odavaju tuđi digitalni podatci. Vidi Dragičević, D., Kompjutorski kriminalitet..., str. 113. Tako i Horvatić, Ž., polazeći od objekta zaštite odnosno samog računalnog sustava i njegove dvojake uloge te specifičnosti načina na koji se takva djela izvršavaju, računalni kriminalitet predstavlja *ukupnost kriminalnih ponašanja na određenom prostoru kroz određeno vrijeme*. Usp. HORVATIĆ, Ž., *Osnove kriminologije*, Ministarstvo unutarnjih poslova Republike Hrvatske, Zagreb, 1998., str. 3. Sličnu definiciju daje i BAČIĆ, F., *Krivično pravo – opći dio,* Informator, 1995., str. 15.

24 O povijesti i pretečama suvremenih digitalnih kompjutera vidi EVANS, C., *Kompjutorski izazov,* Zagreb, 1982., str. 10. Vidi i GRBAVAC, V., *Informatika,* Zagreb, 1995., str. 1-8.

uz pojavu i primjenu prvih ručnih i mehaničkih računala, izum tkalačkog stroja tj. utiskivanjem uzoraka tkanine uz pomoć bušene kartice (za posljedicu je imalo bojazan radnika za gubitkom zaposlenja, te su posezali za sabotažama nad tim strojevima što se evidentira kao prvo kazneno djelo vezano uz računalni kriminalitet), pojavu tzv. poslovnog kriminaliteta poznatijeg kao kriminalitet "bijelih ovratnika" (eng. *white collar crime*) početkom 20. stoljeća i uglavnom se povezuju s financijskim poslovanjem s motivom osobnog koristoljublja.[25]

Oblik računalnoga kriminaliteta s kakvim se danas susrećemo veže se uz razvoj telekomunikacijskih medija i modema tijekom šezdesetih godina 20. stoljeća kada se javljaju prvi tehnički obrazovani delinkventi koji počinju razvijati metode i sredstva za neovlašteno korištenje telefonskih usluga. Tada su ujedno i izmišljeni prvi računalni programi za provaljivanje u tuđe sustave ("crvi", "virusi", "trojanski konj"). Ono što je vrlo značajno kao osnovna karakteristika počinitelja visoki je stupanj povezanosti, razmjenjivanja iskustva i računalnih programa namijenjenih zlouporabi različitih informatičkih tehnologija putem raznih publikacija koje redovito izdaju. Napredovanje komunikacijske tehnologije bilo je samo poticaj počiniteljima za usavršavanje svojih informatičkih sposobnosti u smjeru zlouporabe onog što je nastalo stvaranjem širokih globalnih komunikacijskih mreža.[26]

2.3. Fenomenologija računalnog kriminaliteta

Zajedno s postojanjem raznovrsnih pojavnih oblika računalnoga kriminaliteta, tako su i brojni uzroci i motivi što u konkretnoj situaciji dovode do takvih djela i potiču počinitelje. Ponajprije je potrebno utvrditi *zakonitosti* koje vladaju tim fenomenom da bismo ga lakše shvatili i razjasnili kao pojavu masovnih razmjera. Uzroci se ne mogu tražiti samo u pojedincu koji takvo djelo počini jer je on kao jedinka uvjetovan društvenim uvjetima. Uzroci su isprepleteni i mora ih se proučavati zajedno jer se jedino tako može dobiti cjeloviti uvid u cjelokupan niz čimbenika koji utječu na pojavu računalnoga kriminaliteta u konkretnom slučaju.[27]

Kao prvi korak utvrđuje se *objektivni kriminogeni čimbenik*, odnosno *opći uvjet koji je doveo do pojave i rasprostranjenosti računalnog kriminaliteta i brzina razvoja informacijske tehnologije*. Osobitosti prema kojima se ovaj oblik kriminaliteta razlikuje od drugih *nalaze se u njegovim karakteristikama u kojima se odražava kao kriminalitet suvremenog i razvijenog društva, kriminalitet urbanih sredina, globalni kriminalitet, kriminalitet obrazovanih ljudi, posljedica brojnih slabosti (ljudskih, tehničkih), teško ga je suzbijati i zaustaviti, digitalni oblik podataka, najštetnije posljedice za pojedinca i društvo u cjelini te kao kriminalitet 21. stoljeća*. Kao posljedica može se i navesti nesnalaženje i nepravodobno prilagođavanje novonastalim tehnološkim promjenama

25 Usp. WASIK, M., *Crime and computer*, Clarendon Press, Oxford. 1991., str. 24.

26 Suočavajući se s nizom novonastalih problema s kojim se pravo nije prije susretalo (naviknuti na fizička kaznena djela), dovelo se u pitanje *načelo zakonitosti* i uslijedila je aktivnost zakonodavstava i međunarodnih organizacija u cilju pronalaženja adekvatnih rješenja. O načelu zakonitosti vidi BAČIĆ, F., *Krivično pravo – opći dio,* str. 59.

27 O različitom definiranju kompjutorskog kriminaliteta vidi DRAGIČEVIĆ, D.: *Kompjutorski kriminalitet i informacijski sustavi,* Informator, Zagreb, 1999. str. 110-113.

koje su postale veliki oslonac društva što se javlja kao subjektivni čimbenik koji pridonosi ovoj vrsti kaznenih djela. Otuđenost, frustracija, psihička oboljenja, motivacija i različiti stavovi najčešće su pojave povezane uz razvoj informatičkog educiranja, pojedinca i društva. Sve je brže potrebno donositi odluke iz sve veće mase podataka i razabrati one ispravne. Stoga se računalni kriminalitet ne izučava samo kao pravni, već kao i sociološki, filozofski i etički fenomen.[28]

3. PRAVNO UREĐENJE RAČUNALNOG I KIBERNETIČKOG KRIMINALA

3.1. Pravno uređenje u Republici Hrvatskoj

Zakonodavni okvir elektroničkih dokaza počiva ponajprije na izmjenama i dopunama Kaznenog zakona (NN 125/11, 144/12, 56/15, 61/15 – dalje KZ) i njegovom usaglašavanju s europskom Konvencijom o kibernetičkom kriminalitetu, čime je u Republici Hrvatskoj doneseno novo, kvalitetno, premda ne i potpuno zakonsko rješenje u ovom području. Najvažnija novina u Kaznenom zakonu jest njegovo usuglašavanje s obvezama preuzetim potpisivanjem Konvencije o kibernetičkom kriminalitetu Vijeća Europe (NN-MU 9/02, 4/04). Konvencija predstavlja najvažniji i najopsežniji europski dokument o takvoj vrsti kriminaliteta koju su potpisale i neke neeuropske informatičke velesile, ponajprije Sjedinjene Američke Države, Kanada i Japan. Konvencija je svečano potpisana 23. studenog 2001. u Budimpešti, te je predstavljena kao međunarodno pravni instrument kojim se po prvi put pravno regulira korištenje i prijenos informacija i podataka putem informacijskih i telekomunikacijskih sustava. Naime, progresivan *razvoj tehnologija rezultirao je integracijom informacijskih i telekomunikacijskih tehnologija čime dolazi do pojačane povezanosti i većih oblika njihove zlouporabe* pa se pojam *"računalni kriminalitet" zamjenjuje širim pojmom "kibernetički kriminalitet"*. Upravo stoga se zove Konvencija o kibernetičkom, a ne o računalnom kriminalu.

3.2. Konvencija o kibernetičkom kriminalu

Konvencija o kibernetičkom kriminalu (engl. *Convention on Cybercrime - Narodne novine – Međunarodni ugovori br. 9/2002., br. 4/2004.* – u daljnjem tekstu *Konvencija*)[29] predstavlja oblik međunarodnog ugovora. Također, ova je Konvencija

28 Šire o tome vidi ŠEPAROVIĆ, Z., *Kriminologija i socijalna patologija*, Pravni fakultet Zagreb i dr., 1987., str. 17.

29 Konvencija o kibernetičkom kriminalu Država članica Vijeća Europe potpisana je u Budimpešti 23. rujna 2001. godine. Njeno je značenje, među inim, i u tome što prelazi granice Vijeća Europe, jer su je osim članica toga Vijeća prihvatile SAD, Kanada, Japan i Južna Afrika. Povijesno gledano, Konvencija je nastala tako da je Vijeće Europe 1997. godine osnovalo posebnu komisiju, Committee of Experts On Crime in Cyber Space, čiji je zadatak bio utvrditi stanje i započeti rad na međunarodnim instrumentima za borbu protiv kriminala na internetu. Nakon tri godine rada u tajnosti, Nacrt konvencije prvi put je predstavljen javnosti krajem 2000. godine. Njime je predviđeno da će stranke usvojiti zakonska i druga rješenja nužna da se

ujedno i prvi međunarodni ugovor o kaznenim djelima počinjenim putem interneta i drugih računalnih mreža koje se posebno bave kršenjem autorskih prava, računalnih kaznenih djela vezanih uz prijevare, dječju pornografiju i povrede sigurnosti mreže. Na određen način računalni kriminalitet, u današnjem suvremenom dobu neslućenog tehnološkog napretka, može se definirati komprimiranjem Preambule Konvencije u kojoj se ističe da je *ratio* donošenja Konvencije odvraćanje od *postupaka usmjerenih protiv tajnosti, cjelovitosti i dostupnosti računalnih sustava, mreža i računalnih podataka, kao i za odvraćanje od njihovih zlouporaba, jer utvrđuje, na način opisan u ovoj Konvenciji, kriminalizaciju takvog ponašanja.*[30] Konvencija o kibernetičkom kriminalu dopunjena je *Dodatnim protokolom uz Konvenciju o kibernetičkom kriminalu* o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava *(Narodne novine – Međunarodni ugovori br. 4/2008.)*.

Kibernetički kriminal prema tekstu Konvencije definira inkriminacije vezane uz internet prema sljedećim grupama: *grupu djela protiv tajnosti, nepovredivosti i dostupnosti podataka spremljenih na računala i samih sustava* (ovdje spadaju takve povrede kao što su neovlašteni pristup računalu; *neovlašteno presretanje podataka; neovlašteno mijenjanje i uništavanje podataka, zloupotreba računala i programa radi počinjenja kaznenih djela, ometanje nesmetanog rada računala*, itd.); *kaznena djela poput prijevare i krivotvorenja uz pomoć računala; kaznena djela vezana uz sadržaj podataka na računalima, prvenstveno uz distribuciju i širenje dječje pornografije; djela vezana uz kršenje autorskih i srodnih prava.*[31]

Također, nakon kaznenih djela slijede i odredbe o sankcioniranju pomaganja i prikrivanja pri izvršenju gore navedenih djela te o kaznenoj odgovornosti pravnih osoba za navedena kaznena djela.

Ono što je zajedničko svim državama i ono na temelju čega se Konvencija temelji je suglasnost da je potrebno voditi zajedničku kaznenu politiku usmjerenu su zaštiti društva od računalnog kriminala. Nadalje, dužnosti su država potpisnica da u svoj kaznenopravni sustav unesu odredbe koje će osigurati da kaznena djela mogu biti

u domaćem zakonodavstvu mogu goniti počinitelji kaznenih djela protiv tajnosti, integriteta i dostupnosti kompjuterskih podataka i sustava, kaznenih djela u vezi s kompjutorom, sadržajem i povredama autorskih i srodnih prava. Nacrtom je predviđeno i rješavanje procesnih pitanja vezanih za pretragu i pribavljanje dokaza, ovlaštenja redarstvenih vlasti, nadležnost suda, izručenje počinitelja, uzajamnu suradnju te obveze internet providera. O tome vidi ŠKRTIĆ, D., *Implementacija odredbi Konvencije o kibernetičkom kriminalu u hrvatsko Kazneno i Kazneno procesno pravo*, 10. SLOVENSKI DNEVI VARSTVOSLOVJA, Varstvoslovje med teorijo in prakso, UM, Fakulteta za varnostne vede, Ljubljana, 4. - 5. junij 2009, Zbornik prispevkov, str. 1 – 12.

30 Usp. Preambula Konvencije, NN MU br. 9/2002.

31 Na nekoliko mjesta u Konvenciji spominje se obveza zemalja potpisnica da u svoj pravni poredak unesu odredbe koje će omogućiti i pristup i pretragu podataka na računalima korisnika osumnjičenih za počinjenje neke od inkriminacija gore opisanih. Poseban je naglasak stavljen i na omogućavanje suradnje između država potpisnica u vezi s istražnim radnjama. To je pogotovo očito u odredbama koje određuju dužnost država potpisnica da osnuju službu koja će biti 24 sata na raspolaganju ako se pojavi potreba za suradnjom glede nadgledanja prometa na dijelu mreže u nadležnosti neke od država potpisnica. Izvorni tekst vidi u *Convention on cybercrime,* Conseil de l'Europe, Conseil de l'Europe, 2001. Dostupno na http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (05. 12. 2016.).

kažnjavana s efektnim kaznama, uključivši i kaznu zatvora. [32]

Cilj je Konvencije ponajprije: *usklađivanje domaćeg kaznenog materijalnog prava, elementi djela i povezanih odredbi u području* kibernetičkog kriminaliteta; *pružanje ovlasti za domaće kazneno procesno pravo nužne za istragu i progon tih kaznenih djela, kao i druga djela počinjena pomoću računalnog sustava ili dokaza u elektroničkom obliku; postavljanje brzog i djelotvornog režima međunarodne suradnje*.[33]

Pomnijom analizom kazneno-materijalnih odredbi Konvencije (čl. 2 – 10.) dolazi se do zaključka da se kaznena djela mogu grupirati u dvije skupine. U prvoj skupini su kaznena djela koja se mogu primijeniti na računalni sustav i na računalne podatke. Unutar te skupine su dvije podskupine. Podskupina inkriminacija protiv tajnosti, cjelovitosti i dostupnost računalnih podataka i sustava – *nezakoniti pristup (čl. 2. Konvencije), nezakonito presretanje (čl. 3.), ometanje podataka (čl. 4.), ometanje sustava (čl. 5.) i zlouporaba naprava (čl. 6.) te podskupina s dva modificirana klasična kaznena djela – računalno krivotvorenje (čl. 7.) i računalna prijevara (čl. 8.)*. Drugu skupinu čine kaznena djela sa sadržajem informacija kao bitnom komponentom njihova bića, računalnim podatcima u svezi s komunikacijom, stvorenih pomoću računalnog sustava kao dijela komunikacijskog lanca, a koji naznačuju podrijetlo komunikacije, njeno odredište, put, vrijeme, datum, veličinu, trajanje i vrstu te usluge (*podaci u prometu* – čl. 1.d Konvencije).[34]

Također, navedeni delikti od čl. 2. do čl. 8 mogli bi se definirati i kao *računalni kriminalitet u užem smislu, kao katalog tradicionalnog, postojećeg kataloga kaznenih djela*. U definiciji *računalnog kriminaliteta u širem smislu* taj je katalog proširen na *kaznena djela vezana uz dječju pornografiju* (čl. 9. Konvencije) i *kaznena djela povrede autorskih i srodnih prava* (čl. 10. Konvencije).[35]

---

32 Potpisivanjem Konvencije o kibernetičkom kriminalu Vijeće Europe pokušalo je dati smjernice u borbi protiv računalnog kriminala, pogotovo onog vezanog za internet. O tome vidi TURKALJ, K., *Kako se Europska Unija suočila s modernom prijetnjom terorizma? Gdje je tu Hrvatska kao država u procesu pristupanja Europskoj Uniji?*, Hrvatska pravna revija, br. 11., godina VII., studeni 2007., str. 1- 16.

33 Upravo područje računalnog kriminaliteta najjasnije nameće potrebu izgradnje međunarodnog kaznenog prava: *solidarnost i suradnja među državama, eliminiranje relacije momenta, djelotvorna borba s kriminalitetom, pravičnost, zaštita prava i sloboda čovjeka, humanitarni pristup*. O tim načelima, na tragu kojih je i ujedno i kreirana Konvencija vidi u ZLATARIĆ, B., *Međunarodno krivično pravo*, (priredio: Šeparović, Z.), Informator, Zagreb, 1979., str. 33 – 37.

34 Tako i šire PAVLOVIĆ, Š., *Kompjutorska kaznena djela*, Kompjuterska kaznena djela – I. dio", Hrvatska pravna revija, br. 4, 2004., str. 44.

35 Radnje počinjenja djela iz čl. 9. Konvencije postoje u inkriminacijama Glave XIV. KZ (Kaznena djela protiv spolne slobode i spolnog ćudoređa) – iskorištvanaja djece ili maloljetnika za pornografiju (čl. 196.) i upoznavanja djece s pornografijom (čl. 197.). Usp. KZ čl. 196. i 197. Također, kaznena djela povrede autorskih i srodnih prava iz čl. 10. Konvencije u Glavi XVII. KZ–a (kaznena djela protiv imovine) – povreda prava autora ili umjetnika izvođača (čl. 230.) i povreda prava proizvoditelja zvučne slike ili slikovne snimke i prava u svezi s radio difuzijskim emisijama (čl. 231.) te u čl. 188. Zakona o autorskom pravu i srodnim pravima (Narodne novine, br. 167/2003.). O tome vidi šire u ZLATOVIĆ, D., *Položaj autorskog prava u informacijskom društvu,* Hrvatska pravna revija, br. 3., god. IX., 2009., str. 35–42. Vidi i MOSLAVAC, B., *Kaznenopravne odrednice autorskog prava*, Hrvatska pravna revija, br. 10.,

3.3. Izmjene Kaznenog zakona i usklađivanje sukladno Konvenciji od trenutka potpisa Konvencije

Republika Hrvatska potpisala je Konvenciju o kibernetičkom kriminalu 23. studenog 2001. godine, a obveze koje su time preuzete odnosile su se na izmjenu Kaznenog zakona u koji je trebalo uvesti nova kaznena djela, i to: *nezakoniti pristup, nezakonito presretanje, ometanje podataka, ometanje sustava, zloporabu naprava, kompjutorsko krivotvorenje, kompjutorsku prijevaru, djela vezana uz dječju pornografiju i autorska prava,* u slučajevima kada se računala i internet koriste za zločin, tj. upravo ona djela za koja je rečeno da kompjutorski kriminalitet još uvijek ne predstavlja jedinstvenu fenomenološku kategoriju s jasno određenim i definiranim djelima koje bi trebao obuhvaćati. Također je trebalo uvesti i djela koja uključuju pokušaj, pomaganje i poticanje na sva ova već navedena djela.[36]

Najveća intervencija bila je unošenje u Kazneni zakon definicije kojom su inkriminirane nove zloupotrebe, tako da su od tada uz *oštećenje, izmjenu, brisanje, uništenje ili druge načine zlouporabe podataka* koji ih čine neuporabljivim, kažnjivi i svi načini kojima se oni čine nedostupnima. Ta je novina posebno bitna u situacijama u kojima podatci nisu izbrisani ili oštećeni, ali im se ne može pristupiti zbog djelovanja malicioznih programa, ponajprije virusa, tzv. "crva" i "trojanskih konja". Time se napokon programima i podatcima osigurava jednaka zaštita kao i tjelesnim predmetima. Naime, do sada se krađa računalnih podataka nije smatrala krađom, jer podatci nisu fizički ukradeni iz računala. Činjenicu da su prekopirani i dostupni drugima zakon nije uvažavao. Ovom se izmjenom rješava primjena KZ-a u praksi tih slučajeva.[37]

Novost je bila i sankcioniranje "onemogućavanja ili otežavanja rada ili korištenja" računala ili računalne komunikacije, kao još jedan način kažnjavanja izrade i prijenosa malicioznih programa, ali i sve druge načine uskraćivanja usluga, tzv. *Denial of Service* (DoS) napada. Interpretacija ove norme daje i mogućnost kažnjavanja tzv. *spamminga*, slanja velikog broja *e-mail* poruka s namjerom zagušenja servera ili stroja primatelja, zbog kojeg sustav prestaje raditi. Premda je namjera zakonodavca problem *spamminga* riješiti u posebnom zakonu, ne treba isključiti ni ovu mogućnost. Predviđena kazna za sva navedena djela je novčana ili zatvorska do tri godine.

To nas dovodi do druge bitne novosti, povećanja sankcija za počinitelje koje se sada i razlikuju ovisno o tomu je li kazneno djelo počinjeno na privatnom računalu (novčana kazna ili kazna zatvora do tri godine) ili "računalu, sustavu, podatku ili programu tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnog javnog interesa", u kojem slučaju je sankcija isključivo kazna zatvora od tri mjeseca do pet godina. Daljnje novine odnose se na kažnjavanje neovlaštene izrade i prodaje

god. VIII, 2008., str. 74 – 86.

36 Izmjene koje su provedene ipak su samo djelomične jer nisu inkriminirana sva Konvencijom predviđena djela. Vidi šire u DERENČINOVIĆ, D., *Uvod u kriminologiju i socijalnu patologiju - s osnovama kaznenog prava,* Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2004., str. 223 – 227.

37 Šire o tome vidi u PAVLOVIĆ, Š., "*op. cit*., str. 45

naprava i programa prilagođenih za činjenje kaznenih djela kibernetičkog (računalnog) kriminaliteta te kažnjavanje za pokušaj bilo kojeg od svih spomenutih kaznenih djela.

Važeći KZ, prema izmjenama iz 2015. godine, otišao je korak dalje uvevši novu glavu i članke KZ-a – Glava XXV. pod nazivom: Kaznena djela protiv računalnih sustava, programa i podataka te: Članak 266.: Neovlašteni pristup*;* Članak 267.: O*metanje rada računalnog sustava;* Članak 268.*: Oštećenje računalnih podataka;* Članak 269.: Neovlašteno *presretanje računalnih podataka;* Članak *270.: Računalno krivotvorenje; Članak 271.: Računalna prijevara; Članak 272.: Zloporaba naprava; i* Članak 273.: Teška kaznena djela protiv računalnih sustava, programa i podataka.[38] Time je riješeno i jedno od pitanja koje u ranijim izmjenama nije usuglašeno s Konvencijom, a radilo se o kaznenom djelu neovlaštenog pristupa podatcima ili programima, tzv. *hakingu.* Naime, Konvencija je predvidjela sankcioniranje samog neovlaštenog pristupa dok je naš tadašnji Kazneni zakon (u članku 223.) kažnjavao "samo" neovlašteni pristup "unatoč zaštitnim mjerama". To rješenje je bilo prilično zbunjujuće dok današnja definicija detaljno definira sve oblike neovlaštenog pristupa (članak 266. KZ), ometanja rada računalnog sustava (članak 267. KZ), oštećenje računalnih podataka (članak 268. KZ), neovlašteno presretanje računalnih podataka (članak 269. KZ) kao i sama teška kaznena djela protiv računalnih sustava, programa i podataka (članak 273. KZ) što ujedno predstavlja i novost u KZ-u.[39] Dok se to ne utvrdi, procjenu o postojanju zaštitnih mjera morat će dati sud u svakom posebnom slučaju, a hakerima ostaje izvrsna mogućnost obrane na sudu. Laički govoreći, svaki haker se može braniti da nisu postojale zaštitne mjere, jer da jesu, on ne bi mogao provaliti u sustav.[40] Osim nabrojanih novina, u članku 270. i 271. KZ-a navode se već ranije uvedena dva kaznena djela: računalno krivotvorenje i računalna prijevara koji predstavljaju najčešći oblik kaznenih djela u ovom području. Tako će pribavljanje protupravne imovinske koristi izmjenom tuđih računalnih podataka u svrhu računalne prijevare biti kažnjeno s šest mjeseci do pet godina zatvora. Na isti način bilo koji drugi oblik krađe, prijevare, pronevjere i drugih takvih djela putem informacijskih tehnologija bit će kažnjen zatvorom budući da se radi o sasvim novom, posebnom kaznenom djelu koje nije moglo biti kažnjivo prema klasičnoj interpretaciji krađe kakva je bila dostupna u ranijem Kaznenom zakonu.

U vrijeme ekspanzije elektroničke trgovine i elektroničkog poslovanja općenito, u pravnoj znanosti i primjeni prava naglasak mora biti podjednako stavljen na zaštitu elektroničkih dokumenata kao i onih papirnatih jer u postupku kriminalističke obrade upravo elektronički dokumenti predstavljaju *elektroničke dokaze.*

38 Vidi *Narodne novine,* br. 125, od 07.11.2011., Kazneni zakon: GLAVA DVADESET PETA.

39 O tzv. "hakingu" i drugim pojavnim oblicima računalnog kriminaliteta vidi šire u DRAGIČEVIĆ, D., *Novi izazovi kibernetičkog kriminala*, Hrvatska pravna revija, br. 7-8, godina V., 2005., str.153 – 16.

40 O kritici postojeće inkriminacije vidi BAČIĆ, F., PAVLOVIĆ, Š., *Kazneno pravo – Posebni dio,* Informator, Zagreb, 2001., str. 228 – 229.

4. ELEKTRONIČKI DOKAZI U GRAĐANSKOM SUDSKOM POSTUPKU

4.1. Pojam i vrste elektroničkih dokaza

4.1.1. Pravilna primjena pravnih pravila na pravne odnose zavisi o potpunom i pravilnom utvrđivanju činjeničnog stanja u sporu,[41] a jedan od načina utvrđivanja je i dokazivanje (lat. *argumentatio, demonstratio*). Dokazivanje je procesna djelatnost suda i stranaka uz sudjelovanje i nekih dugih sudionika u postupku radi pravilnog i potpunog utvrđivanja činjeničnog stanja kako bi se osigurala pravilna podloga za sudsku odluku,[42] odnosno to je postupovna radnja utvrđivanja činjenica pravno relevantnih za rješenje stvari koja je predmet postupka.[43] Dokazivanje možemo definirati i kao skup procesnih radnji suda i stranaka upravljenih na utvrđivanje odgovaraju li činjenični navodi stranaka i pretpostavke suda o postojanju odlučnih činjenica istini, a jedno od sredstava za ostvarenje tog cilja su dokazna sredstva, koja su sudu izvor saznanja istine, odnosno objektivna stvarnost koja utječe na pravilnu odluku. Dokazna sredstva se u praksi i zakonu uobičajeno nazivaju "dokazi". Zakon o parničnom postupku (Urednički pročišćeni tekst, "Službeni list", broj 4/77, 36/77, 6/80, 36/80, 43/82, 69/82, 58/84, 74/87, 57/89, 20/90, 27/90, "Narodne novine", broj 35/91, 53/91, 91/92, 112/99, 88/01 – čl. 50. Zakon o arbitraži, 117/03, 84/08, 123/08, 57/11, 148/11, 25/13, 43/13 - Rješenje USRH i 89/14 – OUSRH, dalje – ZPP) ne daje definiciju dokaza, odnosno dokaznog sredstva. Dokaz je pojam koji se u pravnom i laičkom govoru koristi u više značenja.[44] Dokaz ili dokazno sredstvo je izvor, odnosno nositelj informacija od kojih sud dobiva obavijesti o činjenicama važnim za donošenje odluke,[45] to je svako sredstvo saznanja koje je podobno da kod suca stvori uvjerenje o istinitosti činjeničnih tvrdnji,[46] kao i ono (činjenica) iz čega se čulnim opažanjem crpi saznanje o postojanju ili nepostojanju činjenice čije je utvrđivanje važno u parnici.[47]

41 Tako TRIVA, S. – DIKA, M., Građansko parnično procesno pravo, Zagreb, 2004., dalje – TRIVA-DIKA, str. 480.

42 Vidi MATIĆ, I., *Dokazivanje – pojam dokazivanja*, slajd 2, http://www.prafak.ni.ac.rs/files/nast_mat/DOKAZIVANJE_39340.pdf.

43 Usp. AVIANI, D., *Dokazivanje*, http://www.pravst.unist.hr/dokumenti/novosti/blog/blog_dodfile_dokazivanje.pdf.

44 Terminu dokaz (njem. *Beweis)* u praksi i procesnopravnoj teoriji pridaju se različita značenja. U jednom značenju dokaz su podatci određene dokazne vrijednosti do kojih se dolazi ispitivanjem tzv. dokaznih sredstava (*media probandi*) na temelju kojih sud zaključuje o činjenicama koje treba utvrditi; u drugom - sama ta dokazna sredstva; u trećem smislu sam uspješan rezultat dokazivanja. Tako i podrobnije o tome kod DIKA, M. - ČIZMIĆ, J., *Komentar Zakona o parničnom postupku Federacije Bosne i Hercegovine*, Sarajevo, 1999., dalje – DIKA-ČIZMIĆ, str. 50-51. Drugim riječima izraz dokaz upotrebljava se da označi dokazno sredstvo (izvor saznanja o činjenicama); sadržaj obavijesti koje proizlaze iz dokaznog sredstva te uspješan rezultat provjeravanja istinitosti tvrdnje koja je neposredni predmet dokazivanja. TRIVA-DIKA, str. 482.

45 Vidi KEĆA, R. – STAROVIĆ, B., *Građansko procesno pravo*, Novi Sad, 2004., str. 277.

46 Tako STANKOVIĆ, G., *Građansko procesno pravo*, prva sveska – *Parnično procesno pravo*, Niš, 2010., str. 428.

47 Usp. TRIVA-DIKA, str. 482.

ZPP među dokazna sredstva ubraja predmete očevida, isprave, svjedoke, stranke, vještake i tumače. Dokazna sredstva se u procesnopravnoj teoriji, s obzirom na objektivne osobine, uobičajeno dijele u dvije vrste: osobna (svjedoci, vještaci, tumači i stranke) i stvarna (isprave i predmeti očevida). Ovo zakonsko nabrajanje dokaznih sredstava nije taksativno pa stranke u pogledu utvrđivanja njihovih činjeničnih navoda mogu predlagati i druga raspoloživa sredstva saznanja. Teško je vjerovati da se u dogledno vrijeme može pojaviti izvor informacija koji se zbog sadašnje određenosti vrsta dokaznih sredstava ne bi mogao upotrijebiti u svrhu dokazivanja, odnosno koji se ne bi mogao uvrstiti u neko od sada predviđenih dokaznih sredstava. To bi dopustilo da se zaprimanje ili ishođenje informacije nedopušteno provede izvan propisanih postupovnih pravila (primjerice, da se s istim pravnim učinkom umjesto saslušanja svjedoka pred sudom, upotrijebi pisana izjava svjedoka).[48]

Svaka stranka dužna je iznijeti činjenice i predložiti dokaze na kojima temelji svoj zahtjev ili kojim pobija navode i dokaze protivnika (ZPP, čl. 219. st. 1.). ZPP ne propisuje izrijekom elektronička sredstva kao dokazno sredstvo, ali je jasno da ona to mogu biti jer se putem njih može u postupku utvrđivati istinitosti tvrdnje koja je neposredni predmet dokazivanja.

4.1.2. Danas gotovo sva nacionalna zakonodavstva poznaju pojam elektroničkog (elektronskog, digitalnog) dokaza, i imaju određena pravila koja uređuju načine na koje se elektronički podatci, odnosno dokumenti, mogu upotrijebiti kao dokazna sredstva. Elektronički dokazi počeli su se pojavljivati u sudskim i drugim postupcima usporedno s povećanjem važnosti elektroničkih tehnologija, posebno računala, u svakodnevnoj komunikaciji i poslovanju. Elektronički dokaz definira se kao "dokument u elektronskom obliku koji se koristi u pravnim poslovima i drugim pravnim radnjama, kao i u upravnom, sudskom i drugom postupku pred državnim organom". S obzirom na to da ovakvi dokumenti imaju snagu javne isprave, logično je očekivati da će se pojavljivati u većoj mjeri u različitim postupcima pred državnim tijelima.[49]

Elektronički dokazi su specifični po tomu što sudu ili drugom organu pred kojim se vodi postupak mogu biti predstavljeni i u neelektroničkoj formi. Primjerice, komunikacija e-poštom može se predstaviti u "izvornoj" formi, računalom ili nosačem/čitačem elektroničkih podataka, ali se također može provesti i u papirnatoj formi kao tiskana elektronička pošta.[50] Elektronički dokazi posebna su vrsta stvarnih/materijalnih dokaza, novi instrument kojim je moguće dokazivati i kao takvi dobivaju sve veću važnost u sudskim postupcima. Oni su informacije i podatci koji imaju dokaznu vrijednost i mogu se koristiti u sudskom postupku, a pohranjeni su ili se prenose putem elektroničkih uređaja.[51]

Elektronički dokaz je svaki elektronički zapis koji je nastao na računalu ili

48 Tako KEĆA, R. – STAROVIĆ, B., *Građansko procesno pravo*, Novi Sad, 2004., str. 277.

49 Usp. PRLJA, D.- RELJANOVIĆ, M. – IVANOVIĆ, Z., *Internet pravo*, Institut za uporedno pravo, Beograd, 2012., str. 145.

50 Vidi PRLJA, D.- RELJANOVIĆ, M. – IVANOVIĆ, Z., *Internet pravo*, Institut za uporedno pravo, Beograd, 2012., str. 145.

51 Tako BANOVIĆ, B., *Kompjuterski kriminalitet i zaštita ličnosti*, Bezbednost, god. 1., 2003., str. 36.

sličnom uređaju, od strane čovjeka ili je automatski generiran, a koji može služiti u dokaznom postupku pred sudom ili drugim državnim tijelima.[52] To je svaka (binarna) informacija u digitalnom obliku koja ima dokazujuću vrijednost i koja je generirana, obrađivana, pohranjena ili prenesena u digitalnom obliku,[53] i koji služi kao sredstvo uvjeravanja u vjerodostojnost neke isprave.[54] Elektroničkom dokumentu ne može se osporiti valjanost ili dokazna snaga samo zato jer je sačinjen u elektroničkom obliku. Elektronički dokazi predstavljaju kombinaciju različitih informacija poput teksta, slike, audio i videosnimke i sl.[55]

Pravni propisi mogu se primijeniti na elektronički dokaz zahvaljujući interpretativnom načelu analogne primjene normi, što je posebno bitno zbog činjenice što za takvu vrstu dokaza ne postoje posebne norme.[56]

ZPP ne definira ni pojam "(elektronički) dokument".[57] Međutim, iz sudske prakse europskih i nacionalnih sudova dade se zaključiti da taj pojam uključuje fotografije, dijagrame, karte, fotografski film, magnetofonske vrpce, diskove, računalne baze podataka i sl. U tom smislu pojam elektroničkog (digitalnog) dokaza uključuje kompjutorski pohranjene i generirane dokazne informacije i podatke, digitalizirane audio i video signale, podatke s digitalnog mobilnog telefona, podatke s digitalnih faks uređaja i podatke s drugih digitalnih uređaja.[58] Kao dokaz u sudskom postupku može se upotrijebiti i ispisani tekst koji je generiralo samo računalo ili ga je samo arhiviralo (tzv. rukopis osobe u elektroničkoj formi), tekst obrađen procesorima za elektroničku poštu, zapisi iz aktivnosni diskutirajućih skupina (foruma i blogova) i virtualnih soba za razgovor ("*chat-rooms"*), zapisi provajdera koji se tiču identifikacije korisnika (internet protokoli), telefonski zapisi, zapisi govornih automata i sl.[59] Elektronički

52 *Scientific Working Group on Digital Evidence (SWGDE), Digital Evidence: Standards and Principles*, Forensic Science Communications, vol. 2, 2/2000, str. 1.

53 Vidi PISARIĆ, M., *Elektronski zapisi kao dikazi u krivičnom postupku*, Zbornik radova Pravnog fakulteta u Novom Sadu, vol. 43., 2009., br. 2., str. 521.; PETROVIĆ, D. L., *Digitalni dokazi*, rad na savjetovanju ZITEH 2004., podatak na stranici https://singipedia.singidunum.ac.rs/izdanje/40058-digitalni-dokazi, str. 2.

54 Tako *Dopustivost elektroničkog dokaza pred sudom: Suzbijanje visokotehnološkog kriminala – I. dio*, Odvjetnik, 5-6/2007., str. 39.

55 Usp. PROTRKA, N., *Računalni podaci kao elektronički (digitalni) dokazi*, Policija i sigurnost, god. 20., 2011., broj 1, str. 2.

56 Vidi *Dopustivost elektroničkog dokaza pred sudom: Suzbijanje visokotehnološkog kriminala – I. dio*, Odvjetnik, 5-6/2007., str. 41.

57 Elektronički dokument bilo je koji elektronički medijski sadržaj (osim računalnih programa i sistemskih datoteka) koji je namijenjen korištenju u elektroničkom ili pisanom obliku (*Elektronički dokument*, https://hr.wikipedia.org/wiki/Elektroni%C4%8Dki_dokument), napravljen, odnosno generiran na računalu, koji nema svojstva elektroničke isprave (*Uredba o uredskom poslovanju*, "Narodne novine" broj 7/2009, čl. 4. razdjel 4.), a predstavlja elektronički oblik papirnatog dokumenta. (*Osnovni pojmovi, OptimIT*, http://www.optimit.hr/hr/edi/-/asset_publisher/6a93Ij7DSOHe/content/osnovni-pojmovi).

58 Tako KER, O., *Digital evidence and new criminal procedure*, "Columbia law review", vol. 105, 2005., No. 1, p. 283., podatak kod PISARIĆ, M., *Elektronski zapisi kao dikazi u krivičnom postupku*, Zbornik radova Pravnog fakulteta u Novom Sadu, vol. 43., 2009., br. 2, str. 522.

59 Usp. NIKOLIĆ, V., *Otkrivanje i praćenje kompjuterskog kriminala*, Bezbednost, Beograd, vol. 46., 2004., broj 2., str. 273.

dokaz kao generički pojam obuhvaća analogni dokaz (primjerice, audio trake, gramofonske/vinilne ploče, fotografski film, telefonski poziv i sl.) i digitalni dokaz (sve što je kreirano ili se čuva u kompjutoru, što je napravljeno na način koji predviđa internet, CD, DVD, MP3, MP4, digitalni signal i sl.).[60]

Elektronički dokazi se u tom smislu ne razlikuju prema svojoj svrsi, pa samim time ni prema načinu izvođenja i upotrebe u različitim postupcima, od ostalih dokaza. Pravila koja važe za ostale, uvjetno nazvane "obične" dokaze, primjenjuju se shodno i na elektroničke dokaze. Treba, ipak, imati na umu da postojeća pravila i metode prikupljanja dokaza nisu u potpunosti primjenjiva kod (svih) dokaza u elektroničkom obliku. Elektronički dokazi se ipak razlikuju od klasičnih dokaznih sredstava po nekoliko karakteristika koje su posljedica njihove prirode. Ponajprije zbog toga što oni nastaju u prostoru elektroničkih komunikacija i elektroničkih podataka.[61] Za razliku od ostalih, elektronički dokazi prolaze dvostruku provjeru u sudskom postupku – provjeru njihove izrade, pohrane, prijenosa, čuvanja, vjerodostojnosti i nepromjenjivosti s jedne strane (arg. Zakon o elektroničkoj ispravi, čl. 12. st. 2.), a s druge ocjenu njihove dokazne snage.

Prednosti elektroničkog dokaza u odnosu na obične, tradicionalne dokaze su: objektivnost, točnost, pouzdanost, vjerodostojnost, dostupnost, održivost, trajnost i neutralnost informacije; jednostavnost i brzina prikupljanja i korištenja te vrste dokaza; smanjenje troškova dostave i dr. Nedostatci su: nedostatak sredstava provjere autentičnosti, nedovoljno poznavanje postupka obrade podataka i tumačenja postupovnog prava u tom pogledu, jednostavnost kojom se tim dokazima može manipulirati, nepoznavanje načina očuvanja i ispravnog pohranjivanja elektroničkog dokaza, nedostatak primjerenih i sustavnih zakonskih propisa, oskudnost sudske prakse, nedostatak tehničke infrastrukture u pravosudnim tijelima, nužnost specifičnih znanja i sl. [62]

4.2. Prikupljanje podataka i procjena elektroničkih dokaza

Prikupljanje podataka i dokaza najosjetljiviji je korak u području računalnog kriminaliteta i obavlja se putem računalne forenzičke analize. Eventualne pogreške u ovom stupnju mogu značiti nepovratan gubitak dokaza, bilo zbog njihova oštećenja ili zbog gubitka njihove vjerodostojnosti zbog neprimjerenih metoda prikupljanja. Zbog toga je potrebno pažljivo isplanirati postupak prikupljanja dokaza, s posebnim naglaskom na ranjive dokaze, te koristiti odgovarajuće programske alate.

Prije prikupljanja elektroničkih dokaza potrebno je izvršiti temeljitu procjenu danog slučaja i na temelju toga odrediti smjer daljnjeg djelovanja. U okvir takve

60 Vidi MASON, S., *International electronic evidence*, British Institute of International and Comparative Law, 2008., str. 35., podatak kod PALAČKOVIĆ, D., *E – dokument i E- isprava – Legislativa i mogućnost primene u parničnom postupku*, Pravni život, Beograd, godina LX, knjiga 549, 2011., br. 11., str. 787.

61 Tako RELJA, D.- RELJANOVIĆ, M. – IVANOVIĆ, Z., *Internet pravo*, Institut za uporedno pravo, Beograd, 2012., str. 145.

62 U tom smislu kod *Dopustivost elektroničkog dokaza pred sudom: Suzbijanje visokotehnološkog kriminala – I. dio*, Odvjetnik, 5-6/2007., str. 44.

procjene ulaze nalog za pretraživanje, detalji slučaja, vrsta ispitivanog sklopovlja i programske podrške, potencijalni dokazi koje se traži te uvjeti njihova prikupljanja. Nepohranjivanjem elektroničkih dokaza istražitelji se dovode u opasnost od gubitka istih te nemogućnosti nastavka daljnjeg procesa RFA.[63] Stoga je u razgovoru s voditeljem istrage potrebno razmotriti: primjenu ostalih forenzičkih postupaka nad dokazima (DNA analiza, prikupljanje otisaka prstiju, traženje tragova mehaničke obrade i sl.); važnost opreme pronađene uz računalo (npr. kreditne kartice, skeneri, pisači ili digitalne kamere); ostale smjerove istrage npr. traženje podataka od pružatelja internet usluga, pronalaženje udaljenih spremišta podataka ili poruka elektroničke pošte); vrstu potencijalnih dokaza (fotografije, tablice, dokumenti, baze podataka, financijski podatci); ostale informacije vezane uz slučaj (korisnička imena, zaporke, računi elektroničke pošte, mrežne postavke, dnevnički zapisi) koje je možda moguće dobiti u razgovoru s administratorima, korisnicima ili zaposlenicima, te razinu informatičkog znanja korisnika čije se djelovanje ispituje. Po dolasku na mjesto potencijalnog zločina potrebno je utvrditi: broj i vrste računala; prisutnost računalne mreže; vrstu i količinu medija za pohranu podataka te dokumentirati gdje su pronađeni; postojanje udaljenih spremišta podataka i/ili udaljenih računala; korištene komercijalne programske pakete; o kojim se operacijskim sustavima radi; te intervjuirati sistemske administratore i korisnike. Skladištenju pronađenih dokaza potrebno je osigurati njihovu zaštitu od elektromagnetskih smetnji. Stalni izvori napajanja mogu biti potrebni ako se radi o uređajima s baterijskim napajanjem.[64]

4.3. Ranjivost (elektroničkih) dokaza

Elektronički dokazi su mnogo ranjiviji od konvencionalnih fizičkih dokaza i zbog toga je pri rukovanju potrebno se pridržavati određenih smjernica kako ih se ne bi uništilo ili oštetilo. Prvi korak u traženju dokaza na računalu često je njegovo gašenje i transport u laboratorij radi provođenja temeljite analize. Svi podatci nastali tijekom rada računala, koji nisu pohranjeni na tvrdi disk, time su nepovratno izgubljeni. Ostavljanje računala uključenim ipak ne jamči očuvanje dokaza. Ako je računalo povezano na računalnu mrežu, napadač može s udaljene lokacije izbrisati dnevničke zapise ili, neovisno o vezi na mrežu, programirati njihovo automatsko brisanje. Jednako tako, dobronamjeran korisnik radom na računalu može nesvjesno uzrokovati prepisivanje dokaza. Uništenje nije jedina opasnost koja prijeti digitalnim dokazima. Nestručnim rukovanjem oni mogu biti oštećeni i tako obezvrijeđeni u potencijalnom sudskom postupku. To se najčešće događa zbog neinformiranosti korisnika koji, nakon što su uočili zločin, pokušavaju otkriti što se točno dogodilo te tako utječu na sustav.

Glavne vrste ranjivih dokaza su: prijelazni podatci – oni koji se gube gašenjem računala i tu se ubrajaju aktivne mrežne veze ili aplikacije koje se izvode u radnoj memoriji; ranjivi podatci – iako pohranjeni na tvrdom disku, lako su izmjenjivi (primjer

63 O računalnoj forenzičkoj analizi na fizičkoj memoriji vidi više u BURDACH, M., *Digital forenzics of the physical memory,* Varšava, 2005.

64 Tako i šire CARNET, LS&S, *Osnove računalne forenzičke analize*, str. 6-7.

ovakvih dokaza su vremenske oznake posljednjeg pristupa datoteci ili direktoriju); privremeni podatci – podatci koji su pohranjeni na tvrdom disku, a moguće im je pristupiti samo u određenim vremenskim intervalima (primjer su datoteke kriptiranih datotečnih sustava).[65]

Kako bi se ranjivi dokazi očuvali potrebno ih je što prije pohraniti na siguran medij. Tvrdi disk ispitivanog računala nije prikladan za to jer i sam može sadržavati dokaze koji bi na ovaj način mogli biti uništeni ili oštećeni.[66] Pri pohrani ranjivih dokaza potrebno je koristiti što manje radne memorije kako bi se o čuvao njezin sadržaj. Umetanje tvrdog diska u ispitivano računalo nije prihvatljivo jer zahtijeva njegovo gašenje. Ne preporuča se niti korištenje USB ili *Firewire* prijenosnih medija jer se njihovim spajanjem mijenja stanje ispitivanog sustava. Najbolji način za prikupljanje ranjivih dokaza uporaba je računalne mreže. Kako bi se ispitivano računalo zaštitilo od daljnjih napada i kako bi se prikrila istraga, računalo je po otkriću napada potrebno isključiti s mreže. Njegovim spajanjem na privatno čvorište *(*eng. *hub*) omogućuje se prijenos podataka. Pritom drugo računalo, korišteno za prikupljanje dokaza, treba prilagoditi mrežnim postavkama ispitivanog računala.

Prije svega je potrebno dohvatiti i pohraniti sadržaj radne memorije ispitivanog računala i to u manjim paketima kako bi se izbjeglo prepisivanje ostatka radne memorije. Nakon što je sadržaj radne meorije pohranjen može se pristupiti dohvaćanju ostalih podataka, bez ograničenja na veličinu paketa.[67]

Također, ako su informacije i podatci koji se nalaze na računalu pravno relevantni, a istražitelji znaju što traže, bit će moguće u vrlo kratkom roku dokazati da je dokaz ono što on kaže da jest te da dolazi s lokacije za koju on kaže i da dokaz nije bio mijenjan ili oštećen na bilo koji način. Što se elektroničkih dokaza tiče, ovo može biti vrlo teško jer su elektronički dokazi lako promjenjivi kao što je već ranije istaknuto. Stoga je važno biti promišljen, slijediti ranije navedene korake prikupljanja podataka i elektroničkih dokaza: njihove procjene i zaštite ranjivosti, i nadasve upoznat s tehnologijom koja se istražuje.

5. ELEKTRONIČKE ISPRAVE KAO ELEKRONIČKI DOKAZI U GRAĐANSKOM SUDSKOM POSTUPKU

Iako ZPP ne predviđa razliku između dokaznih sredstava glede njihove dokazne snage, u pravilu su isprave najpouzdanije dokazno sredstvo. ZPP ne daje ni definiciju isprave. Prema stajalištu procesnopravne teorije, isprave su predmeti koji sadrže obavijesti o činjenicama, sastavljene u pisanom obliku. U građanskom postupovnom pravu isprava, kao stvarno dokazno sredstvo, je svaki predmet na kojemu je pismom zabilježena neka misao,[68] odnosno svaki predmet na kojem je znakovima pisma

65 Ibid., CARNET, LS&S, str. 7

66 O postupiku forenzičke analize elektroničkih dokaza i primjerima iz prakse vidi ASHCROFT, J., DANIELS, D. J., HART, S. V., *Forensic Examination of Digital Evidence: A Guide for Law nforcment,* U.S. Department of Justice, 2004.

67 Tako i šire CARNET, LS&S, str. 7-8

68 Tako TRIVA, S. - DIKA, M., *Građansko parnično procesno pravo,* Zagreb, 2004., str. 511.

uneseno neko priopćenje, izjava, misao ili drugi takav podatak,[69] na kojemu je pisanim znacima izražena određena tvrdnja ili iznesena neka činjenica.[70] Tjelesni predmet od kojega je isprava sačinjena osigurava postojanost, trajnost i potpunost onoga što isprava sadrži.[71] Predmeti očevida nisu isprave ako na njima nisu zabilježene misli. Isto značenje imaju i obavijesne stvari poput graničnih znakova, koji sadrže otjelovljenje misli, ali bez upotrebe pisma.[72]

Prema izdavateljima, isprave se dijele na javne i privatne. Kod privatnih isprava na kojima je javno ovjerovljen potpis izdavatelja, značenje javne isprave ima samo ta ovjera (legalizacija). Isprava je autentična ako ju je izdala osoba koja je na njoj označena kao njezin izdavatelj. Ona je lažna ako ne potječe od osobe koja je na njoj označena kao njen izdavatelj.[73] Stranka koja predlaže dokaze ispravom dužna je ispravu individualizirati označavanjem imena izdavatelja, predmeta na koji se ona odnosi, mjesta i datuma sačinjavanja, kao i da uz pripremni podnesak priloži prijepis isprave, a na raspravi pokaže sudu izvornik.[74]

U pravilu je isprava napisana na papiru, ali bi bila valjana ako je napisana i na koži, drvetu, kamenu, metalu, staklu ili na drugom predmetu i materijalu koji mogu trajnije očuvati pisani zapis. Za ocjenu ima li predmet karakter isprave nije bitna ni vrsta pisma i jezika na kojemu se piše, niti je presudno koriste li se uz slova i drugi znakovi (crteži, matematički, geometrijski i drugi znakovi, note i sl.).[75] Za pojam ovog dokaznog sredstva nije bitna ni vrsta znakova (pisana slova, tiskana slova, stenografski znakovi), kao ni sredstva kojima su ti znakovi naneseni na predmet (tinta, olovka, tuš, pisač, pisaći stroj),[76] pa ni to je li sastavljena u svrhu dokazivanja ili nije. Dokazivanje ispravom izvodi se čitanjem isprava, što je vrlo blisko izvođenju dokaza očevidom.[77] Kada se radi o planovima, skicama, graničnim znacima, magnetofonskoj vrpci, gramofonskoj ploči, fotografijama, konvencionalnim znakovima i sl.,[78] primjenjuju se pravila o izvođenju dokaza očevidom, pa postoji mišljenje da bi se to moralo primijeniti i na e-zapis.[79]

Javna isprava jest isprava koju je u propisanom obliku izdalo državno tijelo u granicama svoje nadležnosti te isprava koju je u takvom obliku izdala pravna ili fizička osoba u obavljanju javnog ovlaštenja koje joj je povjereno zakonom ili propisom

69 Vidi KEĆA, R. – STAROVIĆ, B., *Građansko procesno pravo*, Novi Sad, 2004., str. 298.
70 Usp. POZNIĆ, B. – RAKIĆ VODINELIĆ, V., *Građansko procesno pravo*, Beograd, 2010., str. 332.; STANKOVIĆ, G. – RAČIĆ, R., *Građansko procesno pravo, Prva sveska – Parnično procesno pravo*, Podgorica, 2010., str. 421.
71 Vidi STANKOVIĆ, G., *Građansko procesno pravo*, prva sveska – Parnično procesno pravo, Niš, 2010., str. 431.
72 Tako TRIVA, S., *Građansko parnično procesno pravo*, Zagreb, 1986., str. 420.
73 Usp. DIKA-ČIZMIĆ, str. 407-410.
74 Vidi odluku Višeg trgovinskog suda, Pž. - 5227/05 od 23. 1. 2006. godine.
75 Tako KEĆA, R. – STAROVIĆ, B., *Građansko procesno pravo*, Novi Sad, 2004., str. 298.
76 Usp. POZNIĆ, B. – RAKIĆ VODINELIĆ, V., *Građansko procesno pravo*, 15. izmijenjeno i dopunjeno izd., Savremena administracija; Beograd, str. 252.
77 Vidi KEĆA, R. – STAROVIĆ, B., *Građansko procesno pravo*, Novi Sad, 2004., str. 298.
78 Tako TRIVA – DIKA, str. 511.
79 Usp. PALAČKOVIĆ, D., *E – dokument i E- isprava – Legislativa i mogućnost primene u parničnom postupku*, Pravni život, Beograd, godina LX, knjiga 549, 2011., br. 11., str. 771.

utemeljenim na zakonu. Javna isprava dokazuje istinitost onoga što se u njoj potvrđuje ili određuje (ZPP, čl. 230. st. 1.). Istu dokaznu snagu imaju i druge isprave koje su posebnim propisima u pogledu dokazne snage izjednačene s javnim ispravama (ZPP, čl. 230. st. 2).[80] Ako međunarodnim ugovorom nije što drugo određeno, inozemne javne isprave koje su propisno ovjerene imaju, uz uvjet uzajamnosti, istu dokaznu snagu kao i domaće javne isprave (ZPP, čl. 231.). Dopušteno je dokazivati da su u javnoj ispravi neistinito utvrđene činjenice ili da je isprava nepravilno sastavljena (ZPP, čl. 230., st. 3.).

Pojam privatne isprave trebalo bi negativno odrediti kao one isprave koje nisu javne. Uz privatne se isprave ne bi vezivala nikakva presumpcija glede njihove autentičnosti. Ako bi se ona osporila, teret dokaza glede njezine autentičnosti bio bi na onome koji je njome trebao dokazati neku činjenicu. Dokaznu snagu tih isprava glede istinitosti njihova sadržaja sud bi trebao procjeniti po slobodnoj ocjeni dokaza, pa stoga u ZPP-u nema odredaba o presumptivnoj dokaznoj snazi privatnih isprava.[81] Privatnu ispravu, upravo jer se uz nju ne veže presumpcija istinitosti, treba posebno vrednovati u sklopu svih ostalih provedenih dokaza.[82]

U postupcima koji se vode pred tijelima javne vlasti i arbitražama kao dokaz mogu se koristiti i elektroničke isprave (arg. ZEI, čl. 12. st. 1.). Elektronička isprava jednoznačno je povezan cjelovit skup podataka koji su elektronički oblikovani (izrađeni pomoću računala i drugih elektroničkih uređaja), poslani, primljeni ili sačuvani na elektroničkom, magnetnom, optičkom ili drugom mediju, i koji sadrže svojstva kojima se utvrđuje izvor (stvaratelj), vjerodostojnost sadržaja te dokazuje postojanost sadržaja u vremenu. Sadržaj elektroničke isprave uključuje sve oblike pisanog teksta, podatke, slike i crteže, karte, zvuk, glazbu, govor (ZEI, čl. 4. točka 1.). Upravo zato ne može se tvrditi da su elektronička isprava i elektronički dokument istovjetna stvarna dokazna sredstva kao što su to isprave u papirnatom obliku, nego se u slučaju pohrane drugih oblika sadržaja, osim pisanih, moraju primjenjivati pravila o očevidu.[83] Svrha elektroničke isprave jest kreiranje pravno valjanog iskaza volje danog u elektroničkom obliku koji ima određeni sadržaj, a nedvojbeno je da potječe od određene osobe te "dokumantacijskim svojstvom" povezuje sadržaj isprave s formalnim i za pravnu valjanost takve isprave nužnim pratećim elementima.[84]

Stranka je dužna sama podnijeti ispravu na koju se poziva za dokaz svojih navoda (ZPP, čl. 232. st. 1.). ZPP predviđa različita pravila o pribavljanju, odnosno ediciji isprava, u zavisnosti o tomu tko je držatelj isprave. Pravila o ediciji isprava

80 Javnobilježničke isprave su javne isprave. Međutim, izvod iz vjerovnikove kartice dugovanja nije glede dokazne snage izjednačen s javnom ispravom (VSFBiH, Pž-131/97 od 19. 8. 1997. - objavljeno u Biltenu Vrhovnog suda FBiH, broj 2/97).

81 Tako TRIVA-DIKA, str. 515.

82 Odluka OS u Dubrovniku, Gž-435/88. - PSP 45/109. "Pisane potvrde o izvršenim isplatama naknade štete predstavljaju privatne isprave koje sud vrednuje i ocjenjuje zajedno sa svim ostalim provedenim dokazima" (ŽS u Varaždinu, Gž-1248/07-2 od 14. 1. 2008. godine, Domaća i strana sudska praksa, stručni i informativni časopis, godina V, br. 28., str. 92.).

83 Vidi LISIČAR, H., *Mogućnost i uporabe elektroničke isprave i elektroničkih dokumenata u parničnom postupku***,** Zbornik PFZ, vol. 60, (3), 2010., str. 1415.

84 Usp. VOJKOVIĆ, G., *Elektronička isprava*, zbornik radova sa savjetovanja Aktualnosti hrvatskog zakonodavstva i pravne prakse, Godišnjak 13, Organizator, Zagreb, 2006., str. 451.

reguliraju postupak pribavljanja isprava radi dokazivanja pred sudom. Odredbe su različite s obzirom na to da nalazi li se isprava kod stranke koja se na nju poziva, kod njezinog protivnika, ili kod nekoga trećeg.[85] Držimo da se navedena pravila mogu analogno primijeniti i kod edicije elektroničkih isprava.

Elektronicka isprava ima istu pravnu snagu kao i isprava na papiru, ako se njezina uporaba i promet provode u skladu s odredbama Zakona o elektroničkoj ispravi (ZEI, čl. 2.). Unatoč izrijekom propisanoj istovjetnosti i ravnopravnosti elektroničkim isprava s "običnim" (papirnatim) ispravama, iznimno za sve radnje u kojima se zakonom ili drugim propisima izričito traži javnobilježnička ovjera isprava na papiru, ne može se dostavljati elektronička isprava ili njegova preslika na papiru (ZEI, čl. 11.). Upravo zbog toga što ZPP ne daje definiciju isprave kao i zbog toga što u e-regulativi nisu propisani nužni uvjeti koje e-dokument mora ispunjavati da bi bio e-isprava i imao pravnu valjanost kao isprava sačinjena na papiru, ostaje sporno je li e- zapis koji nije otisnut isprava u smislu odredaba ZPP-a.[86]

6. UMJESTO ZAKLJUČKA – VJEŠTAČENJE ELEKTRONIČKIH DOKAZA

Konačni cilj prikupljanja i analize elektroničkih podataka i stvaranja elektroničkih dokaza, jest njihovo prezentiranje u dokaznom postupku. Ono se može ostvariti na više načina, ali je temeljna razlika u tomu provodi li se njihovo veštačenje ili samo ocjena na temelju pregleda istih, kao i jesu li oni pogodni za prezentiranje u papirnatoj formi (tiskani) ili u izvornoj – elektroničkoj formi na računalu ili drugom uređaju.[87] Podnošenje dokaza sudu u elektroničkom obliku, bez obzira na to radi li se o elektroničkoj ispravi ili o elektroničkom dokumentu, ograničeno je ponajprije mogućnošću suda da takve dokaze prihvati i pregleda. Kada je u pitanju elektronička isprava, sud neće moći pregledati njezin sadržaj ako prethodno nije omogućena uporaba infrastrukture javnog ključa. Suprotno, kada je riječ o elektroničkom dokumentu, čak i ako sud ima mogućnost uvida u njegov sadržaj, otvara se pitanje vjerodostojnosti i izvornosti tog sadržaja.[88]

Kod ocjene ispravnosti elektroničke isprave, moraju se uzeti u obzir pojedinosti o njezinoj izradi, pohrani, prijenosu, čuvanju, vjerodostojnosti i nepromjenjivosti (ZEI, čl. 12. st. 2.). Stranke su dužne dokazati autentičnost dokaza koje predlažu, a o načinu na koji će to učiniti odlučuje sud. Ako sud posumnja u autentičnost isprave, može zatražiti da se o tomu očituje tijelo od kojega bi ona trebala potjecati (ZPP, čl. 230. st. 4).

Elektronički dokazi/isprave mogu biti predmetom vještačenja, posebno u pogledu njihove autentičnosti, dokazne snage, istinitosti sadržaja i propisanog oblika. Sud će

85 Tako TRIVA-DIKA, str. 516.

86 Vidi PALAČKOVIĆ, D., *E – dokument i E- isprava – Legislativa i mogućnost primene u parničnom postupku*, "Pravni život", Beograd, godina LX, knjiga 549, 2011., br. 11., str. 778.

87 Usp. PRLJA, D.- RELJANOVI, M. – IVANOVIĆ, Z., *Internet pravo*, Institut za uporedno pravo, Beograd, 2012., str. 149.

88 Tako LISIČAR, H., *Mogućnost i uporabe elektroničke isprave i elektroničkih dokumenata u parničnom postupku***,** Zbornik PFZ, vol. 60, (3), 2010., str. 1415.

izvesti dokaz vještačenjem kad je radi utvrđivanja ili razjašnjenja kakve činjenice potrebno stručno znanje kojim sud ne raspolaže (ZPP, čl. 250.). Pri predlaganju, odnosno određivanju vještaka mora se voditi računa o stručnim kvalifikacijama i kvalitetama onoga tko se imenuje vještakom. Vještaci se određuju, ponajprije, iz reda imenovanih stalnih sudskih vještaka za određenu vrstu vještačenja, ali stranke i sud nisu vezani za listu sudskih vještaka, nego se može po potrebi za vještaka odrediti i drugu osobu.[89] Naime, službenu listu stalnih sudskih vještaka treba shvatiti kao pomoćno sredstvo, podsjetnik, adresar osoba prikladnih za obavljanje vještačenja, i ta lista može imati samo značenje preporuke i sugestije, a ne i obvezatnog izvora.[90] Za određenu vrstu vještačenja sud može odrediti vještake i izvan reda stalnih sudskih vještaka, primjerice ako za određenu vrstu vještačenja nema stalnog sudskog vještaka ili je stalni sudski vještak spriječen ili postoji opasnost od odgađanja.

Vještačenje se može povjeriti i stručnoj ustanovi (bolnici, kemijskom laboratoriju, fakultetu i sl.). Ako postoje posebne ustanove za određene vrste vještačenja (vještačenje lažnog novca, rukopisa, daktiloskopsko vještačenje i sl.), takva vještačenja, a osobito složenija, treba povjeravati prvenstveno tim ustanovama (ZPP, čl. 252. st. 2.). Kad je vještačenje povjereno stručnoj ustanovi, ona određuje jednu ili više osoba koje će u njezino ime obaviti vještačenje.[91] Vještačenje sud može povjeriti stručnoj ustanovi posebno ako drži da je potrebno vještačenje toliko teško i složeno da na izradi nalaza i mišljenja treba raditi više stručnjaka i/ili se pri izradi nalaza i mišljenja trebaju koristiti posebna tehnička sredstva i oprema s kojom te ustanove raspolažu.

Sud bi vještačenje elektroničkih dokaza mogao prepustiti sudskom vještaku iz područja informatike, elektronike, elektrotehnike ili komunikacija, koji može sudu na jednostavan način pojasniti komplicirane tehničke sadržaje.[92] Sudski vještak za informacijske tehnologije (IT vještak), mora prethodno utvrditi izvorno stanje informatičkih dokaza te potvrditi da je informatički dokaz nepromijenjen u odnosu na izvorno stanje, što je od ključnog značenja za prihvaćanje dokaza na sudu. Podatak o tomu kako su dokazi pribavljeni, čuvani, prenošeni, zaštićeni od izmjena i kako se s njima manipuliralo, presudan je za donošenje odluke o tomu hoće li oni biti na sudu prihvaćeni ili odbačeni. Elektronički dokazi moraju zadovoljiti i sve druge zahtjeve koji se odnose na ostale sudske dokaze.[93]

LITERATURA

1. ASHCROFT, J., DANIELS, D. J., HART, S. V., Forensic Examination of Digital Evidence: A Guide for Law nforcment, U.S. Department of Justice, 2004.
2. AVIANI, D., *Dokazivanje*, dostupno na http://www.pravst.unist.hr/dokumenti/novosti/

89 Odluka VSH, Rev-1849/80 od 17. veljače 1981. - PSP 19/205.
90 Tako TRIVA-DIKA, str. 530.
91 U tom je smislu odluka VSH u odluci Rev-1001/90, od 11. rujna 1990. - PSP 50/136.
92 Usp. PROTRKA, N., *Računalni podaci kao elektronički (digitalni) dokazi*, Policija i sigurnost, god. 20, 2011., br. 1., str. 8.
93 Tako PETROVIĆ, D. L., *Digitalni dokazi*, rad na savjetovanju ZITEH 2004., podatak na stranici: https://singipedia.singidunum.ac.rs/izdanje/40058-digitalni-dokazi, str. 5.

blog/blog_dodfile_dokazivanje.pdf
3. BAČIĆ, F., Krivično pravo – opći dio, Informator, 1995.
4. BAČIĆ, F., PAVLOVIĆ, Š., Kazneno pravo – Posebni dio, Informator, Zagreb, 2001.
5. BANOVIĆ, B., Kompjuterski kriminalitet i zaštita ličnosti, "Bezbednost", god. 1., 2003.
6. BOBAN, M., Information and communication technologies and the new forms of organized crime in network society, 39th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2016 - Proceedings , 2016., str. 1857-1862
7. BURDACH, M., Digital forenzics of the physical memory, Varšava, 2005.
8. CARNET, LS&S, Osnove računalne forenzičke analize, CCERT-PUBDOC-2006-11-174, 2006., dostupno na http://security.lss.hr/documents/LinkedDocuments/CCERT-PUBDOC-2006-11-174.pdf
9. CASTELLS, M., "Moć identiteta", Svezak I., Golden marketing, Zagreb, 2002.
10. CASTELLS, M., The information age: economy, society and culture, Vol. I: The rise of the network society . Cambridge: Blackwell Publishers, 2000.
11. CERF, V. G., KAHN, R. E., "A protocol for packet network interconnection", IEEE Trans. Comm. Tech., vol. COM-22, V 5, May 1974., str. 627-641
12. CHARLES W. ADAMS, C. W., Spoliation of electronic evidence: sanctions versus advocacy, 18 MICH. TELECOMM. TECH. L. REV. 1 (2011), str. 1, dostupno na http://www.mttlr.org/voleighteen/adams.pdf
13. CHORVAT, T. J., E-Discovery and Electronic Evidence in the Courtroom, "Business Law Today", Vol. 17, No. 1, Sept./Oct. 20.
14. Convention on cybercrime, Conseil de l'Europe, Conseil de l'Europe, 2001. Dostupno na: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm
15. ČIZMIĆ, D., BOBAN, M., ZLATOVIĆ, D., Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost, Sveučilište u Splitu Pravni fakultet, Split, 2016.
16. DERENČINOVIĆ, D., Uvod u kriminologiju i socijalnu patologiju - s osnovama kaznenog prava, Pravni fakultet Sveučilišta u Zagrebu, Zagreb, 2004., str. 223 - 227
17. DIKA, M. - ČIZMIĆ, J., Komentar Zakona o parničnom postupku Federacije Bosne i Hercegovine, Sarajevo, 1999.,
18. DRAGIČEVIĆ, A., DRAGIČEVIĆU, D., Doba kiberkomunizma, Golden marketing, Zagreb, 2003.
19. DRAGIČEVIĆ, D., Novi izazovi kibernetičkog kriminala, Hrvatska pravna revija, br. 7-8, godina V., kolovoz 2005., str.153 - 166
20. DRAGIČEVIĆ, D.: "Kompjutorski kriminalitet i informacijski sustavi", Informator, Zagreb, 1999.
21. EVANS, C., Kompjutorski izazov, Zagreb, 1982.
22. GRBAVAC, V., Informatika, Zagreb, 1995.
23. GRBAVAC, V., PLENKOVIĆ, M., Komunikacijski sustavi na prijelazu u 21. stoljeće, Informatologija, br. 27., 1995., str. 1-5
24. HORVATIĆ, Ž., "Osnove kriminologije", Ministarstvo unutarnjih poslova Republike Hrvatske, Zagreb, 1998.
25. KAZNENI ZAKON, Narodne novine, br. 125, od 07.11.2011., GLAVA DVADESET PETA
26. KEĆA, R. – STAROVIĆ, B., Građansko procesno pravo, Novi Sad, 2004.
27. KER, O., Digital evidence and new criminal procedure, "Columbia law review", vol. 105, 2005., br. 1.
28. KIM J. ANDREASSON, K. J., Cybersecurity: Public Sector Threats and Responses, CRC Press, 2012.
29. LISIČAR, H., Mogućnost i uporabe elektroničke isprave i elektroničkih dokumenata u parničnom postupku, "Zbornik PFZ", vol. 60, (3), 2010.
30. MASON, S., International electronic evidence, British Institute of International and

Comparative Law, 2008.
31. MATIĆ, I., Dokazivanje – pojam dokazivanja, dostupno na http://www.prafak.ni.ac.rs/files/nast_mat/DOKAZIVANJE_39340.pdf
32. MONROE E. PRICE, Free Expression, Globalism, and the New Strategic Communication, Cambridge University Press, 2014.
33. MOSLAVAC, B., Kaznenopravne odrednice autorskog prava, Hrvatska pravna revija, br. 10., god. VIII, listopad 2008., str. 74 - 86
34. NIKOLIĆ, V., Otkrivanje i praćenje kompjuterskog kriminala, Bezbednost, Beograd, vol. 46, 2004., broj 2.
35. NOORDA, C., HANLOSER, S., E-discovery and data privacy: a practical guide, Kluwer Law International, 2010.
36. NOUWT, S., DE VRIES, B. R., PRINS, C., Reasonable expectations of privacy?: eleven country reports on camera surveillance and workplace privacy, Cambridge University Press, 2005.
37. Odluka OS u Dubrovniku, Gž-435/88. - PSP 45/109, ŽS u Varaždinu, Gž-1248/07-2 od 14. 1. 2008. godine, Domaća i strana sudska praksa, stručni i informativni časopis, godina V, broj 28, str. 92
38. Odluka Višeg trgovinskog suda, Pž. - 5227/05 od 23. 1. 2006. godine.
39. Odluka VSH u odluci Rev-1001/90, od 11. rujna 1990. - PSP 50/136.
40. Odluka VSH, Rev-1849/80 od 17. veljače 1981. - PSP 19/205.
41. Odluka VSFBiH, Pž-131/97 od 19. 8. 1997. - objavljeno u Biltenu Vrhovnog suda FBiH, broj 2/97
42. Dopustivost elektroničkog dokaza pred sudom: Suzbijanje visokotehnološkog kriminala – I. dio, Odvjetnik, 5-6/2007.,
43. OPTIMIT, osnovni pojmovi, dostupno na: http://www.optimit.hr/hr/edi/-/asset_publisher/6a93Ij7DSOHe/content/osnovni-pojmovi
44. PALAČKOVIĆ, D., E – dokument i E- isprava – Legislativa i mogućnost primene u parničnom postupku, Pravni život, Beograd, godina LX, knjiga 549, 2011., broj 11,
45. PAVLOVIĆ, Š., Kompjutorska kaznena djela, Kompjuterska kaznena djela – I. dio, Hrvatska pravna revija, br. 4, travanj, 2004., str. 44
46. PETROVIĆ, D. L., Digitalni dokazi, rad na savjetovanju ZITEH 2004., dostupno na: https://singipedia.singidunum.ac.rs/izdanje/40058-digitalni-dokazi
47. PISARIĆ, M., Elektronski zapisi kao dikazi u krivičnom postupku, Zbornik radova Pravnog fakulteta u Novom Sadu, vol. 43., 2009., br. 2, str. 521.;
48. POZNIĆ, B. – RAKIĆ VODINELIĆ, V., Građansko procesno pravo, 15. izmijenjeno i dopunjeno izdanje, Savremena administracija, Beograd, 2010.
49. Preambula Konvencije o kibernetičkom kriminalu, NN MU, br. 9/2002.
50. PRLJA, D.- RELJANOVIĆ, M. – IVANOVIĆ, Z., Internet pravo, Institut za uporedno pravo, Beograd, 2012.
51. PROTRKA, N., Računalni podaci kao elektronički (digitalni) dokazi, Policija i sigurnost, god. 20, 2011., broj 1, str. 1 – 13.
52. Scientific Working Group on Digital Evidence (SWGDE), Digital Evidence: Standards and Principles, Forensic Science Communications, vol. 2, 2/2000.
53. STANKOVIĆ, G. – RAČIĆ, R., Građansko procesno pravo, Prva sveska – Parnično procesno pravo, Podgorica, 2010.
54. STANKOVIĆ, G., Građansko procesno pravo, prva sveska – Parnično procesno pravo, Niš, 2010.
55. ŠEPAROVIĆ, Z., Kriminologija i socijalna patologija, Pravni fakultet Zagreb i dr., 1987.
56. ŠKRTIĆ, D., Implementacija odredbi Konvencije o kibernetičkom kriminalu u hrvatsko Kazneno i Kazneno procesno pravo, 10. SLOVENSKI DNEVI VARSTVOSLOVJA, Varstvoslovje med teorijo in prakso, UM, Fakulteta za varnostne vede, Ljubljana, 4. - 5. junij 2009, Zbornik prispevkov, str. 1 – 12.

57. TOURAINE, A., Qu'est-ce que la democratie?, Fayard, Pariz, 1994.
58. TRIVA, S. – DIKA, M., Građansko parnično procesno pravo, Zagreb, 2004.
59. TRIVA, S., Građansko parnično procesno pravo, Zagreb, 1986., str. 420.
60. TUĐMAN, M., Informacijsko ratište i informacijska znanost, Hrvatska sveučilišna naklada, Zagreb, 2008., str. 263 – 267.
61. TURKALJ, K. Kako se Europska Unija suočila s modernom prijetnjom terorizma? Gdje je tu Hrvatska kao država u procesu pristupanja Europskoj Uniji?, Hrvatska pravna revija, br. 11., godina VII., studeni 2007., str. 1- 16.
62. United Nations International cooperation in combating transnational crime, dostupno na:http://www.uncjin.org/6e.pdf.
63. UREDBA O UREDSKOM POSLOVANJU, Narodne novine broj 7/2009.
64. VOJKOVIĆ, G., Elektronička isprava, zbornik radova sa savjetovanja Aktualnosti hrvatskog zakonodavstva i pravne prakse, Godišnjak 13, Organizator, Zagreb, 2006.
65. WASIK, M., Crime and computer, Clarendon Press, Oxford. 1991.
66. Elektronički dokument, dostupno na stranici: https://hr.wikipedia.org/wiki/Elektroni%C4%8Dki_dokument.
67. ZLATARIĆ, B., Međunarodno krivično pravo, (priredio: Šeparović, Z.), Informator, Zagreb, 1979., str. 33 – 37.
68. ZLATOVIĆ, D., Položaj autorskog prava u informacijskom društvu, Hrvatska pravna revija, br. 3., god. IX., ožujak 2009., str. 35 – 42.

Summary

ELECTRONIC EVIDENCE IN THE JUDICIAL PROCEEDINGS AND COMPUTER FORENSIC ANALYSIS

Today's perspective of the information society is characterized by the terminology of modern dictionaries of globalization including the terms such as convergence, digitization (media, technology and/or telecommunications) and mobility of people or technology. Each word with progress, development, a positive sign of the rise of the information society. On the other hand in a virtual environment traditional evidence in judicial proceedings with the document on paper substrate, are becoming electronic evidence, and their management processes and criteria for admissibility are changing over traditional evidence. The rapid growth of computer data created new opportunities and the growth of new forms of computing, and cyber crime, but also the new ways of proof in court cases, which were unavailable just a few decades.

The authors of this paper describe new trends in the development of the information society and the emergence of electronic evidence, with emphasis on the impact of the development of computer crime on electronic evidence; the concept, legal regulation and probative value of electronic evidence, and in particular of electronic documents; and the issue of electronic evidence expertise and electronic documents in court proceedings.

Keywords: *civil procedure, cyber crime, electronic evidence, information technology.*

Zusammenfassung

ELEKTRONISCHE BEWEISE IM GERICHTSVERFAHREN UND COMPUTERFORENSISCHER ANALYSE

Die heutige Perspektive der Informationsgesellschaft ist geprägt von der Terminologie der modernen Wörterbücher der Globalisierung und schließt die Begriffe wie Konvergenz, Digitalisierung (Medien, Technologie und/oder Telekommunikation) und Mobilität von Menschen oder Technologie ein. Jedes mit den Begriffen wie Fortschritt und Entwicklung verbundene Wort ist ein positives Zeichen für den Aufstieg der Informationsgesellschaft. Auf der anderen Seite, in einem virtuellen Umfeld werden traditionelle Papierbeweise in Gerichtsverfahren in elektronische Beweise umgestellt und ihre Umgangsprozesse und Zulässigkeitskriterien ändern sich in Bezug auf traditionelle Beweise. Das rasante Wachstum von Computerdaten schafft neue Chancen und das Wachstum neuer Formen der Datenverarbeitung und Cyberkriminalität, aber auch neue Beweismethoden in Gerichtsfällen, die nur wenige Jahrzehnte zur Verfügung standen.

Die Autoren dieses Artikels beschreiben neue Trends in der Entwicklung der Informationsgesellschaft und die Entstehung elektronischer Beweise mit Schwerpunkt auf die Auswirkungen der Entwicklung der Cyberkriminalität auf elektronische Beweise; auf das Konzept, die rechtliche Regulierung und die Beweiskraft von elektronischen Beweisen, insbesondere von elektronischen Dokumenten; und auf die Experteinschätzung der elektronischen Beweise und elektronischen Dokumente in Gerichtsverfahren.

***Schlüsselwörter**: Zivilverfahren, Cybertkriminalität, elektronische Beweise, Informationstechnologie.*

Riassunto

LE PROVE ELETTRONICHE NEL PROCEDIMENTO GIUDIZIARIO ED ANALISI INFORMATICA FORENSE

L'odierna società informatica acquisisce la terminologia del vocabolario contemporaneo della globalizzazione, annoverando espressioni quali la convergenza, la digitalizzazione (media, tecnologia e/o telecomunicazione) e la mobilità sia di persone, che di tecnologie. Ciascun termine esprime il progresso, lo sviluppo ed un segnale positivo di crescita della società informatica. Per converso, in un circondario virtuale le prove tradizionali nel procedimento giudiziario da documenti cartacei si trasformano in prove elettroniche: i processi di gestione ed i criteri di ammissibilità risultano mutati rispetto alle prove tradizionali. La rapida crescita di dati informatici ha creato nuove possibilità ed una crescita di nuove forme di criminalità informatica, come anche di quella cibernetica; di qui la comparsa di nuovi mezzi di prova nei procedimenti giudiziari, impraticabili fino a qualche decennio fa.

Gli autori in questo lavoro descrivono le nuove tendenze di sviluppo della società informatica e la comparsa delle prove elettroniche, prestando attenzione all'influenza dell'evoluzione della criminalità informatica sulle prove elettroniche. Ancora, si occupano della nozione, della disciplina giuridica e della forza probatoria delle prove elettroniche ed in particolare degli atti elettronici, come pure della questione delle perizie sulle prove elettroniche e sugli atti elettronici nel procedimento giudiziario.

***Parole chiave:** procedimento giudiziario (civile), criminalità informatica, prove elettroniche, tecnologia informatica.*