PRAVNI ASPEKTI *FACT-CHECKINGA* U EUROPSKOJ UNIJI I HRVATSKOJ

Priručnik o zakonodavnom okviru za rad provjeravatelja točnosti informacija



Financira Europska unija NextGenerationEU

TOČNO tako

AGENCIJA ZA ELEKTRONIČKE MEDIJE

Nakladnik: **Agencija za elektroničke medije**
www.aem.hr

Naslov: Pravni aspekti fact-checkinga u Europkoj uniji i Hrvatskoj
Autori: dr.sc. Hrvoje Lisičar, dr.sc. Marko Jurić, dr.sc. Tihomir Katulić, dr.sc. Romana Matanovac Vučković, Perica Norac-Kevo

za nakladnika: Josip Popovac
urednik: Robert Tomljenović
dizajn i prijelom: O,ne radiona d.o.o.
godina izdanja: 2025., rujan



Priručnik je nastao u okviru edukacijskog programa za neovisne provjeravatelje točnosti informacija, u sklopu projekta „Uspostava sustava provjere točnosti informacija“, a u organizaciji Agencije za elektroničke medije i Pravnog fakulteta Sveučilišta u Zagrebu. Projekt „Uspostava sustava provjere točnosti informacija“ financira se iz Mehanizma za oporavak i otpornost Europske unije, u okviru mjere iz Nacionalnog plana oporavka i otpornosti. Nositelji mjere su Agencija za elektroničke medije i Ministarstvo kulture i medija, a cilj joj je jačanje otpornosti društva na dezinformacije kroz smanjenje količine dezinformacija u javnom prostoru, jačanje informacijske pouzdanosti i sigurnosti kod konzumiranja medijskih sadržaja i korištenja društvenih mreža te poticanje kvalitete novinarstva i vjerodostojnog izvještavanja.

ISBN zapis je dostupan u računalnome katalogu Nacionalne i sveučilišne knjižnice u Zagrebu pod brojem ISBN 978-953-8583-10-0

SADRŽAJ

Modul 1.
Temeljna ljudska prava (sloboda izražavanja i pravo na privatnost) u kontekstu provjere točnosti informacija i sustava javne objave podataka 4
1. Uvodno o slobodi izražavanja 4
2. Balansiranje prava na privatnost i prava na zaštitu osobnih podataka s pravom na informiranje i slobodom izražavanja – uloga fact-checking organizacija 6
3. Razgraničenje prava na privatnost i prava na zaštitu osobnih podataka 7
4. Europski i nacionalni pravni okvir 7
5. Obrada osobnih podataka u kontekstu novinarstva i provjere točnosti informacija (čl. 85. Opće uredbe o zaštiti podataka) 9
6. Zaključak 10

Modul 2.
Pravo na pristup informacijama 11
1. Uvod 11
2. Zakon o medijima 11
3. Zakon o pravu na pristup informacijama 12
4. Opća uredba o zaštiti podataka 19
5. Zaključak 20

Modul 3.
Fact-checking, privatnost i zaštita osobnih podataka – između javnog interesa i zaštite temeljnih prava 21
1. Uvod 21
2. Pregled načela zaštite osobnih podataka važnih za novinarstvo i fact-checking 22
3. Primjenjive pravne osnove za obradu podataka u medijskom izvještavanju i fact-checkingu 24
4. Rukovanje i upotreba osobnih podataka prilikom fact-checking provjera 26
5. Zaključak 29

Modul 4.
Zaštita autorskog i srodnih prava u kontekstu borbe protiv dezinformacija 31
1. Uvod 31
2. Zakonodavni okvir 31
3. Temeljni pojmovi autorskog i srodnih prava 33
4. Ograničenja i iznimke autorskog i srodnih prava 35
5. Kolektivno ostvarivanje prava 37
6. Umjetna inteligencija i autorsko pravo 39
7. Zaključak 40

Modul 5.
Regulacija digitalnih usluga, medijska regulacija i aktivnosti međunarodnih organizacija u borbi protiv dezinformacija 41
1. Uvodno o zakonodavnom okviru 41
2. Akt o digitalnim uslugama 42
3. Europski akt o slobodi medija 49
4. Direktiva o audiovizualnim medijskim uslugama 51
5. Smjernice Vijeća Europe 52
6. Zaključak 53

Modul 6.
Odgovornost za štetu - u predmetima za naknadu štete zbog povrede prava osobnosti objavljenom informacijom u medijima kroz sudsku praksu 55
1. Uvod 55
2. Zakonodavni okvir 56
3. Građanskopravna zaštita privatnosti 59
4. Izjave o činjenicama i vrijednosni sudovi 66
5. Zaključak 66

Popis korištene literature 67

Modul 1.

Temeljna ljudska prava (sloboda izražavanja i pravo na privatnost) u kontekstu provjere točnosti informacija i sustava javne objave podataka

Prof. dr. sc. Hrvoje Lisičar
Izv. prof. dr. sc. Marko Jurić
Izv. prof. dr. sc. Tihomir Katulić
Pravni fakultet Sveučilišta u Zagrebu

1. Uvodno o slobodi izražavanja

Sloboda izražavanja predstavlja temeljno ljudsko pravo koje je zajamčeno brojnim međunarodnim aktima i Ustavom RH, a čija je zaštita suočena s brojnim izazovima u današnjem informacijskom društvu. Tako prema Općoj deklaraciji o ljudskim pravima u članku 19. svatko ima pravo na slobodu mišljenja i izražavanja što uključuje slobodu zadržavanja mišljenja bez uplitanja i slobodu traženja, primanja i širenja informacija i ideja putem bilo kojeg medija i bez obzira na granice. Prema članku 10. Europske konvencije o ljudskim pravima svatko ima pravo na slobodu izražavanja što uključuje: slobodu mišljenja i izražavanja, slobodu primanja i prenošenja informacija i ideja uz određena ograničenja. Ta ograničenja podrazumijevaju da sloboda izražavanja može podlijegati takvim formalnostima, uvjetima, ograničenjima ili sankcijama koje su predviđene zakonom i koje su neophodne u demokratskom društvu u interesu nacionalne sigurnosti, teritorijalnog integriteta ili javne sigurnosti, sprječavanja nereda ili zločina, zaštite zdravlja i morala, ugleda ili prava drugih, sprječavanja širenja povjerljivih informacija ili u interesu očuvanja autoriteta i nepristranosti sudstva, što se sumarno može svesti na tri temeljna standarda za ograničenje a to su zakonitost, legitimni cilj te nužnost i proporcionalnost. Na sličan način o slobodi izražavanja govori i Povelja EU-a o temeljnim pravima u članku 11. stavku 1 koji svima jamči slobodu izražavanja što uključuje slobodu zadržavanja mišljenja, slobodu primanja i prenošenja informacija i ideja bez uplitanja javnih vlasti i neovisno o granicama te u stavku 2 istog članka uključuje i obvezu poštivanja slobode i pluralizma medija. Konačno, Ustav RH u članku 38. jamči slobodu mišljenja i izražavanja misli pri čemu sloboda izražavanja misli osobito obuhvaća: slobodu tiska i drugih sredstava priopćavanja, slobodu govora i javnog nastupa, slobodno osnivanje svih ustanova javnog priopćavanja, te se jamči pravo na pristup informacijama koje posjeduju tijela javne vlasti s time da ograničenja prava na pristup informacijama moraju biti razmjerna naravi potrebe za ograničenjem u svakom pojedinom slučaju te nužna u slobodnom i demokratskom društvu.
Kada se suštinski promotre sve navedene definicije kojima se sloboda izražavanja kao te-

meljno ljudsko pravo želi zaštititi jasno se može zaključiti da one sadrže dvije temeljne komponente – aktivnu i pasivnu komponentu. Aktivna komponenta podrazumijeva aktivno prakticiranje zajamčenog prava kao što je pravo na slobodu izražavanja, pravo na slobodu govora, pravo na slobodu javnog nastupa te pravo na iznošenje mišljenja, dok pasivna komponenta podrazumijeva pravo na primanje ideja, izričaja i informacija, pravo čuti, pravo znati i pravo na pristup medijima. Uz navedene aktivnu i pasivnu komponentu, slobodu izražavanja možemo promatrati i u kontekstu eksterne i interne komponente, pri čemu eksterna komponenta uključuje pravo na slobodu izražavanja i slobodno iznošenje vlastitog mišljenja a interna komponenta slobodu mišljenja, pravo na formiranje vlastitog mišljenja i prava povezana s pravom na zaštitu privatnost.

Kada se sloboda izražavanja promatra u kontekstu dezinformacija bitno je istaknuti da navedeno pravo jamči iznošenja svih vrsta informacija i ideja, uključujući one koje mogu šokirati, uvrijediti ili uznemiriti bez obzira na istinitost sadržaja. Prema međunarodnom pravu, osobe imaju pravo izražavati neutemeljena mišljenja i izjave ili svoje pravo koristiti u svrhu parodije ili satire. S toga je izrazito važno za provjeravatelje informacija voditi računa da li se radi o takvim slučajevima ili se radi o iznošenju činjeničnih tvrdnji. Također, u kontekstu borbe protiv dezinformacija bitno je istaknuti da je za slobodu izražavanja od ključne važnost i slobodan protok informacija. Time se nameće pozitivna obveza državi da aktivno čini dostupnim javnosti informacije od javnog interesa, pluralne i raznolike izvore informacija, uključujući i slobodu medija.

Ako se sloboda izražavanja promatra kroz različite teorije postoje brojni teorijski pristupi koji opravdavaju zaštitu slobode izražavanja[1]. Teorije slušača tvrde da ograničavanje govora ne poštuje autonomiju građana i njihovu sposobnost donošenja vlastitih sudova. Država čini nepravdu svojim građanima odlučujući što mogu, a što ne mogu čuti, tretirajući ih kao nesposobne za samostalno razmišljanje. Autonomija slušatelja je ključna: građani bi trebali imati slobodu pristupa različitim gledištima i sami odlučivati, umjesto da država kontrolira tok ideja. Poštivanje autonomije slušača (primatelja informacija) odnosi se ne samo na slobodu govora već i na promoviranje okruženja koje omogućuje primanje različitih informacija iz različitih izvora (Cohen). Ova teorija podržava načela poput neutralnosti sadržaja i gledišta, tvrdeći da država ne bi trebala ograničavati govor na temelju vlastitih poruka ili stajališta. Teorije govornika zastupaju stajalište da sloboda govora ima važnu ulogu u našem razvoju i ostvarivanju osobne autonomije. Kod čovjeka postoji „izražajni interes" u iznošenju pogleda o životu, pravdi, identitetu te drugim aspektima „istine" kako je svaki pojedinac vidi (Cohen) te uključuje potrebu za dijeljenjem mišljenja sa drugima. Također, govor ima razvojnu komponentu. Ako je sloboda govora opravdana važnošću naših interesa da se izrazimo, to opravdava i negativne dužnosti tj. suzdržavanja od ometanja govornika bez odgovarajućeg opravdanja. Kao i kod teorije slušatelja, argumenti protiv uvođenja granica slobodi izražavanja koje se temelje na sadržaju i stajalištu pojedinca, predstavljaju oblik diskriminacije. Teorije demokracije ističu važnost slobode izražavanja za demokraciju (Heyman; Sunstein; Weinstein). Sloboda govora na instrumentalnom nivou promiče demokraciju te je konstitutivni element demokratskih društava u kojima prema Rawls-u „ ograničiti ili potisnuti slobodu političkog govora…uvijek podrazumijeva barem djelomičnu suspenziju demokracije". Sloboda govora i demokracija dijele istu temeljnu vrijednost – autonomiju (Baker), pri čemu demokracija ima posebnu ulogu u teoriji slobode govora, npr. da politič-

[1] Vidi: Stanford Encyclopedia of Philosophy, Freedom of Speech, Siječanj 19, 2024 https://plato.stanford.edu/entries/freedom-speech/ (21.1.2025)

ki govor zaslužuje posebnu zaštitu (Barendt). Teorije mišljenja obuhvaćaju slobodu komunikacije i slobodu mišljenja, koji se, iako logički različiti, međusobno nadopunjuju te su međusobno ovisni (Shiffrin). Sloboda govora ključna je za razvoj, funkcioniranje i djelovanje mislioca zato jer često moramo eksternalizirati naše ideje kako bismo ih precizno artikulirali i procijenili njihovu vrijednost. Također, ljudi razrađuju ono što misle uglavnom razgovarajući o tome s drugima. Iskrena komunikacija nam omogućuje dijeliti potrebe, emocije, namjere, uvjerenja, ambicije, želje, fantazije, razočarenja i osude. Teorije tolerancije promatraju slobodu govora kao važnu komponentu razvoja našeg karaktera kao liberalnih građana, pomažući nam ukrotiti naše neliberalne porive (Bollinger). Sloboda govora nam pomaže prakticirati opći etos tolerancije na način koji učvršćuje naša liberalna uvjerenja. Navedena teorija osuđuje cenzuru kojoj je cilj zaštititi publiku od izloženosti pogrešnim pogledima. U srži ove teorije nalazi se teza da je najviši moral države odgovornost da osigura društvene uvjete koji služe razvoju i održanju samopoštovanja kao i poštivanje građana, neovisno o njihovim stavovima. Instrumentalne teorije govore da slobodu govora štitimo prvenstveno zato jer bi državi bilo daleko lakše ušutkati svoje političke protivnike i provoditi nepravednu politiku (Epstein). Inzistira se na načelu da su odluke onih kojima je povjerena velika moć podvrgnute javnoj raspravi i nadzoru, čime sloboda izražavanja postaje svojevrsni instrument kontrole državne vlasti. Konačno, teorije skepticizma slobodu izražavanja promatraju kao „posebno" pravo (Kendrick). Pri tome izraz "posebno pravo" općenito zahtijeva da ono bude potpuno različito od ostalih prava i djelatnosti te da uživa vrlo visok stupanj zaštite. Da bi se opravdala sloboda govora kao posebno pravo, ono mora služiti nekim posebnim vrijednostima ili interesu. Zajamčena sloboda govora mora biti čvrsta u onome što želi zaštiti, tako da je samo posebno uvjerljivo opravdanje može nadjačati, dok istovremeno nije potrebno štititi štetni govor ili izričaj kako bi se slobodu izražavanja moglo nazvati pravom.

U kontekstu teoretskih razmatranja o slobodi izražavanja nameće se pitanje kada i zašto ograničenja slobode izražavanja mogu biti opravdana? Iako je uobičajeno o slobodi izražavanja govoriti kao apsolutnom pravu, to nije uvijek slučaj (kao što je to jasno navedeno i u članku 10. EKLJP-a). Stoga slobodu izražavanja možemo promatrati kroz tri temeljne kategorije - izražavanje (govor) koje nije zaštićeno (prijetnje), izražavanje koje je pokriveno pravom ali nije zaštićeno (oglašavanje) te izražavanje koje je pokriveno i zaštićeno u što spada većina ljudske komunikacije. Osim navedenih ograničenja svakako je potrebno uzeti u obzir i druga interna ograničenja slobode izražavanja kao što su kleveta, govor mržnje, poticanje na nasilje, sadržaj koji krši neke moralne standarde i slično te eksterna ograničenja kao što su zaštita privatnosti, autorska prava ili javna sigurnost.

2. Balansiranje prava na privatnost i prava na zaštitu osobnih podataka s pravom na informiranje i slobodom izražavanja – uloga *fact-checking* organizacija

Pravo na privatnost te pravo na zaštitu osobnih podataka često su suprotstavljena pravu javnosti na informiranje i pravu na slobodno izražavanje. Digitalna tehnologija i mediji olakšali su prikupljanje i objavu osobnih podataka u digitalnom okruženju, što proširuje i podiže pitanje granica zaštite privatnosti nasuprot interesu javnosti da bude informirana.

Fact-checking organizacije koje provjeravaju točnost informacija u javnom prostoru, nalaze se kao posrednici između ovih suprotstavljenih prava – one djeluju u javnom interesu razotkrivanja neistina, ali su pritom dužne voditi računa o dostojanstvu i privatnosti pojedinaca o kojima se izvještava. Ni pravo na privatnost ni pravo na zaštitu podataka s jedne strane, kao niti pravo na slobodu izražavanja i pravo na informiranje nisu apsolutna prava, već pravni

poredak predviđa mehanizme za njihovo međusobno usklađivanje. U nastavku se analizira teorijsko razgraničenje tih prava, relevantni europski i nacionalni pravni okvir, sudska praksa, te posebnosti obrade osobnih podataka u novinarstvu i provjeri točnosti informacija, uz osvrt na etiku i odgovornost *fact-checkera*.

3. Razgraničenje prava na privatnost i prava na zaštitu osobnih podataka

Iako su konceptualno povezani, pravo na privatnost i pravo na zaštitu osobnih podataka zasebna su prava. Pravo na privatnost u širem smislu podrazumijeva pravo na poštovanje privatnog i obiteljskog života te opću zabranu miješanja u osobnu sferu pojedinca, osim kada javni interes može opravdati takvo miješanje. Zaštićeni su različiti aspekti privatnosti – od intime obiteljskog života, preko časti i ugleda, do nepovredivosti doma i komunikacija. S druge strane, pravo na zaštitu osobnih podataka uspostavlja sustav pravila i kontrola kojim se pojedincima osigurava zaštita prilikom svake obrade njihovih osobnih podataka. Drugim riječima, zaštita podataka usredotočena je na informacijsku privatnost, tj. na to kako se podaci prikupljaju, obrađuju i koriste.

Postoji razlika između privatnog života pojedinca i njegovog javnog ili profesionalnog života. Tako, primjerice, informacije o obnašanju javne dužnosti neke osobe mogu biti osobni podaci, ali nisu nužno dio njezine privatnosti jer se tiču njegove javne uloge. Pravo na privatnost štiti pojedinca od pretjeranog zadiranja u njegov osobni život, dok pravo na zaštitu podataka osigurava da se *svaka* obrada osobnih podataka provodi zakonito, transparentno i pošteno uz odgovarajuće mjere zaštite.

4. Europski i nacionalni pravni okvir

Europska konvencija o ljudskim pravima jamči pravo na privatnost u članku 8., a slobodu izražavanja u članku 10. Članak 8. EKLJP propisuje da *"svatko ima pravo na poštovanje svog privatnog i obiteljskog života, doma i dopisivanja"*, uz zabranu miješanja javne vlasti u to pravo osim ako je to predviđeno zakonom i nužno u demokratskom društvu radi legitimnih ciljeva (npr. radi zaštite sigurnosti, javnog reda, zdravlja ili zaštite prava i sloboda drugih). S druge strane, čl. 10. Konvencije jamči slobodu izražavanja, koja obuhvaća slobodu mišljenja te primanja i širenja informacija bez miješanja vlasti. No, ostvarivanje tih sloboda nosi *"dužnosti i odgovornosti"* pa se može podvrgnuti ograničenjima propisanim zakonom nužnim, primjerice, radi zaštite ugleda ili prava drugih. Dakle, već EKLJP u svojim tekstom predviđa mogućnost ograničenja slobode medija radi zaštite nečije privatnosti ili ugleda, kao i obratno, ograničenje privatnosti radi drugih javnih interesa.

Povelja EU o temeljnim pravima („Povelja EU") također štiti ista prava. Prvo, u čl. 7. propisano je da *„svatko ima pravo na poštovanje svojeg privatnog i obiteljskog života, doma i komuniciranja"*. Nadalje, čl. 8. Povelje sadrži samostalno temeljno pravo na zaštitu osobnih podataka, koje je odvojeno od prava na zaštitu privatnog života. Prema čl. 8:

„1. Svatko ima pravo na zaštitu osobnih podataka koji se na njega ili nju odnose.

2. Takvi podaci moraju se obrađivati pošteno, u utvrđene svrhe i na temelju suglasnosti osobe o kojoj je riječ, ili na nekoj drugoj legitimnoj osnovi utvrđenoj zakonom. Svatko ima pravo na pristup prikupljenim podacima koji se na njega ili nju odnose i pravo na njihovo ispravljanje.

3. Poštovanje tih pravila podliježe nadzoru neovisnog tijela".

Konačno, čl. 10. Povelje određuje da *„svatko ima pravo na slobodu izražavanja. To pravo uklju-*

čuje slobodu mišljenja te primanja i širenja informacija i ideja bez miješanja tijela javne vlasti i bez obzira na granice". Također, u stavku 2. navodi se da se poštuju sloboda i pluralizam medija.

Na razini nacionalnog prava, Ustav Republike Hrvatske u članku 35. jamči *"...štovanje i pravnu zaštitu osobnog i obiteljskog života, dostojanstva, ugleda i časti"* svakog čovjeka. Time je ustavno zaštićena šira sfera privatnosti pojedinca, uključujući njegovu čast i dostojanstvo. Osim opće privatnosti, Ustav RH posebno u čl. 37. jamči *"...sigurnost i tajnost osobnih podataka"* te određuje da se, bez privole ispitanika, osobni podaci mogu prikupljati i obrađivati samo pod uvjetima predviđenim zakonom. To znači da je već na najvišoj razini propisano da svako postupanje s osobnim podacima mora imati zakonsku osnovu ili privolu osobe, čime je uspostavljen temelj domaćeg okvira zaštite podataka. Istovremeno, Ustav u čl. 38. štiti slobodu izražavanja i slobodu medija, zabranjuje cenzuru te afirmira pravo novinara na slobodno izvještavanje i pristup informacijama. Ustav također eksplicitno propisuje i *pravo na ispravak* kroz odredbu kojom se *"...jamči ... pravo na ispravak svakomu komu je javnom viješću povrijeđeno Ustavom utvrđeno pravo"*. Ova odredba utjelovljuje mehanizam zaštite pojedinaca od netočnih ili štetnih medijskih navoda, a od izravne je važnosti za rad i odgovornost *fact-checking* organizacija.

Kako je prethodno rečeno, prava na privatnost, zaštitu osobnih podataka i slobodu izražavanja iz EKLJP, Povelje EU i Ustava nisu apsolutna. Ona se mogu ograničiti, pod uvjetom da su ispunjene pretpostavke propisane tim propisima.

Temeljno načelo iz Ustava RH (čl. 16.) je da se slobode i prava mogu ograničiti zakonom da bi se zaštitila sloboda i prava drugih ljudi te pravni poredak, javni moral i zdravlje. Nadalje, isti članak propisuje da „svako ograničenje slobode ili prava mora biti razmjerno naravi potrebe za ograničenjem u svakom pojedinom slučaju."

Slična je situacija i s pravom na poštivanje privatnog života iz čl. 8. EKLJP. Prema drugom stavku iz toga članka, javna vlast se može miješati u ostvarivanje prava ako su kumulativno zadovoljena tri uvjeta: (1) da je ograničenje u skladu sa zakonom (pravom, *in accordance with the law*), (2) da ono služi nekom legitimnom cilju te (3) da je nužno u demokratskom društvu.

Ograničenje je u skladu sa zakonom ako (a) u domaćem pravu postoji pravna osnova (izvor prava) koja omogućava miješanje u pravo iz čl. 8., ako je (b) taj izvor prava dostupan osobi čiji se privatni život ograničava, ako je (c) domaće pravo predvidljivo, u smislu da pojedinci mogu u razumnoj mjeri predvidjeti pravne posljedice vlastitog ponašanja, te (d) ako postoji pravno sredstvo protiv arbitrarnog miješanja u pravo koje se štiti.

Drugi uvjet je da ograničenje služi legitimnom cilju. EKLJP sadrži zatvorenu listu ciljeva zbog kojih se može ograničavati pravo na privatnost: (1) državna sigurnost, (2) javni red i mir, (3) gospodarska dobrobit zemlje, (4) sprečavanja nereda ili zločina (5) zaštita zdravlja ili morala te (6) zaštita prava i sloboda drugih. Slično je uređeno i za pravo na slobodu izražavanja.

Konačno, treći uvjet koji proizlazi iz čl. 8 st. 2. EKLJP je da je ograničenje nužno u demokratskom društvu, što znači da za njim mora postojati „prijeka društvena potreba". Test nužnosti u demokratskom društvu s obzirom na postojanje prijeke društvene potrebe je sasvim sigurno najkompleksnije pitanje o kojem je potrebno odlučiti kada se utvrđuje je li neko ograničenje prava u skladu s EKLJP. U svojoj praksi ESLJP koristi veći broj kriterija temeljem kojih se odlučuje je li neko ograničenje nužno u demokratskom društvu. Mnogi od tih kriterija su uneseni u nacionalna zakonodavstva država članica EKLJP.

Primjerice, u slučaju izvještavanja medija o privatnom životu pojedinca Zakon o medijima sadrži temeljno pravilo prema kojemu svatko ima pravo na privatnost; to pravo imaju i

osobe koje obavljaju javnu službu ili dužnost, osim u slučajevima koji su vezani uz tu službu / dužnost. Nadalje, propisuje se da osoba koja svojim izjavama, ponašanjem i drugim djelima u vezi s osobnim ili obiteljskim životom sama privlači pozornost javnosti ne može zahtijevati istu razinu zaštite privatnosti kao drugi građani.

Ograničenja iz Povelje EU u bitnome slijede strukturu sličnu onoj iz EKLJP (uz nekoliko razlika koje izlaze izvan okvira ovog rada). Sumirajući, kad se ograničava neko od temeljnih prava, potrebno je da budu ispunjeni sljedeći zahtjevi:

1. Ograničenje prava mora biti propisano zakonom odnosno pravno uređeno. Pri tome, traži se da norma bude dovoljno precizna i jasna. Posljedično, bilo koje ograničenje prethodno spomenutih prava neće biti valjano ako se ne temelji na jasnom i predvidivom izvoru iz nacionalnog prava (ili prava EU).
2. Ograničenje mora slijediti legitimni cilj. Legitimni ciljevi su izrijekom navedeni u spomenutim propisima (v. čl. 8. i 10. EKLJP, čl. 7., 8. i 10. Povelje EU, i čl. 16. Ustava RH).
3. Ograničenje mora biti nužno u demokratskom društvu.

EKLJP, Povelja EU i Ustav RH ovime postavljaju jasna ograničenja državama u pogledu mogućnosti zadiranja u temeljna prava građana na privatnost, zaštitu osobnih podataka i slobodu izražavanja. Ova načela štite građane od samovolje vlasti i zahtijevaju da države vode računa o ravnoteži između javnog interesa i zaštite pojedinca.

Opća uredba o zaštiti podataka (GDPR), u primjeni u cijeloj EU pa tako i u Hrvatskoj, daje konkretniji okvir za zaštitu osobnih podataka. GDPR potvrđuje da zaštita podataka nije neograničeno pravo te da se treba ostvariti u ravnoteži s drugim pravima, uključujući slobodu izražavanja i informiranja. Posebno je relevantan članak 85. GDPR-a, koji traži od država članica da zakonom usklade pravo na zaštitu osobnih podataka s pravom na slobodu izražavanja i informiranja, uključujući obradu u novinarske svrhe, što u praksi znači da države trebaju propisati *izuzeća ili odstupanja* od pojedinih odredbi GDPR-a za obradu osobnih podataka u novinarstvu, kada je to nužno da bi se očuvala sloboda medija.

U skladu s tom odredbom, sektorski medijski propisi predviđaju odstupanja za novinarske obrade podataka, a recital (uvodna izjava) 153 Opće uredbe naglašava važnost slobode izražavanja u demokratskom društvu te potrebu širokog tumačenja pojmova poput "novinarstva". U hrvatskom pravu, ključni poseban propis je Zakon o medijima, koji u čl. 3. jamči slobodu medija i prava javnosti na informaciju, ali također zahtijeva poštivanje ljudske osobnosti, privatnosti i dostojanstva pri objavi informacija. Zakon o medijima propisuje da se sloboda medija može ograničiti samo ako je to nužno radi zaštite, primjerice, ugleda ili prava drugih (čl. 3. st. 3.), a u čl. 7. st. 3. ugrađuje načelo da osoba koja sama privlači pozornost javnosti u vezi sa svojim privatnim životom *"ne može zahtijevati istu razinu zaštite privatnosti kao drugi građani"*. Nadalje, čl. 8. tog Zakona glasi da *nema povrede prava na privatnost ako glede određene informacije prevladava opravdani javni interes nad zaštitom privatnosti*. Ove odredbe medijskog zakonodavstva operacionaliziraju ravnotežu: novinari (i posredno *fact-checkeri*) smiju obrađivati i objaviti osobne podatke bez privole ako postoji pravna osnova u zakonu i preteže javni interes, uz obvezu istovremenog uvažavanja dostojanstva osobe.

5. Obrada osobnih podataka u kontekstu novinarstva i provjere točnosti informacija (čl. 85. Opće uredbe o zaštiti podataka)

Opća uredba o zaštiti podataka u članku 85. prepoznaje novinarstvo i srodne djelatnosti (akademsko, umjetničko i književno izražavanje) kao područja gdje treba osigurati posebne iznimke od strogih pravila zaštite podataka kako bi se očuvala sloboda informiranja. Ovo se

često naziva "novinarska iznimka" odnosno *"journalist exception"*. U praksi, to znači da novinari i medijske organizacije smiju obrađivati osobne podatke (prikupljati, objavljivati ih itd.) u mjeri nužnoj za obavljanje svojeg informativnog zadatka, *bez privole pojedinca ili drugih uobičajenih pravnih osnova*, pod uvjetom da poštuju profesionalne standarde i da je obrada opravdana pravom na objavu informacije. Države članice detaljnije uređuju tu iznimku – u Hrvatskoj, kao što je spomenuto, Zakon o medijima i medijski kodeksi postavljaju kriterije i granice. Bitno je naglasiti da čak i u okviru novinarske iznimke nisu suspendirana sva pravila zaštite osobnih podataka. Primjerice, novinari su oslobođeni od pojedinih obveza poput informiranja ispitanika, ograničenja svrhe ili prava ispitanika na brisanje, ali ne smiju povrijediti neka temeljna načela obrade. Uredba ne dopušta izuzeća od načela da obrada mora biti zakonita, poštena i transparentna prema pojedincu (čl. 5. st.1(a)), što znači da se ni u novinarskom radu ne smije pribjegavati nezakonitim metodama prikupljanja podataka, obmanjivanju ispitanika i sl. Također, načelo točnosti podataka ostaje relevantno – novinari imaju etičku i pravnu dužnost iznositi provjerene i istinite informacije, što je upravo područje djelovanja *fact-checkera*.

Fact-checking organizacije u suštini obavljaju novinarsku funkciju provjere tvrdnji i objave točnih informacija. One su često dio medijskih kuća ili surađuju s medijima, te se na njih primjenjuju ista pravila o novinarskim iznimkama u pogledu zaštite podataka. Članak 85. Uredbe odnosi se i na obradu u svrhe *"provjere točnosti informacija"* ako je cilj javno informiranje. Iako Uredba izričito ne spominje *fact-checkere*, zakonodavstvo i praksa ih svrstavaju u aktere od javnog interesa na području informiranja, stoga uživaju slične slobode kao i novinari u korištenju osobnih podataka kada razotkrivaju dezinformacije. Naravno, te slobode dolaze s odgovornošću jer *fact-checkeri* trebaju procijeniti je li svaki osobni podatak koji objavljuju doista nužan za razumijevanje i kontekst tvrdnje koju provjeravaju. Primjerice, ako se provjerava istinitost tvrdnje političara, objava njegovog imena, funkcije i citata je opravdana, no objavljivanje njegove adrese ili osobnih obiteljskih prilika obično ne bi bilo potrebno niti opravdano.

Dodatno, nacionalni propisi poput Zakona o elektroničkim medijima i smjernice tijela kao što je Agencija za zaštitu osobnih podataka ili Agencija odnosno Vijeće za elektroničke medije mogu sadržavati upute o tome kako se Uredba primjenjuje na medijske objave. U primjeni uvijek ostaje onaj završni test proporcionalnosti: je li određena objava ili zadiranje u nečiju privatnost nužna da bi se ostvarilo pravo javnosti da bude informirana o nekom pitanju? U tom smislu, *fact-checking* organizacije moraju stalno balansirati između različitih prava i interesa kao čuvari istine u javnom prostoru, ali ne smiju same postati izvor povrede nečijih prava bez pravnog temelja.

6. Zaključak

Balansiranje međusobno suprotstavljenih prava kao što su prava na privatnosti i zaštite osobnih podataka s jedne strane te prava na informiranje i slobodu izražavanja s druge strane jedan je od trajnih izazova modernog pravnog poretka, osobito u digitalnom medijskom okruženju. Pravo na privatnost i podatke ne smije se instrumentalizirati za ušutkavanje opravdanih novinarskih istraživanja od javnog interesa (primjer za to je neuspjeli pokušaj političara da se pozivanjem na GDPR ukloni neugodan članak), ali ni sloboda medija ne smije postati izgovor za senzacionalizam koji povređuje intimu pojedinaca bez stvarne potrebe. *Fact-checking* organizacije pri tome imaju posebnu ulogu - osigurati ravnotežu, istodobno jačati slobodu izražavanja (šireći točne informacije i ispravljajući laži) i štititi pojedince od štetnih neistina. Praksa pokazuje da je moguće odgovorno koristiti povlašteni položaj novinarske iznimke uz poštivanje načela minimizacije, razmjernosti i prava na odgovor. Ta prava služe javnosti, a da se pritom ne umanjuje dostojanstvo osobe.

Modul 2.

Pravo na pristup informacijama

Izv. prof. dr. sc. Marko Jurić
Pravni fakultet Sveučilišta u Zagrebu

1. Uvod

U ovom poglavlju razmatraju se temeljni pravni mehanizmi putem kojih je u hrvatskom pravnom sustavu moguće pribavljati informacije od javnog sektora. Pravo na pristup informacijama predstavlja jedno od ključnih jamstava transparentnosti rada tijela javne vlasti, ali i učinkovite kontrole od strane javnosti. U kontekstu demokratskog društva, pristup informacijama nije samo tehničko pitanje dostupnosti dokumenata, već duboko povezano s pravima građana, slobodom medija i zaštitom privatnosti.

Analiza obuhvaća tri međusobno povezana izvora pravne regulacije: Zakon o medijima, Zakon o pravu na pristup informacijama te Opću uredbu o zaštiti podataka (GDPR). Svaki od tih propisa uređuje različite aspekte pristupa i korištenja informacija – od uloge medija u informiranju javnosti, preko institucionaliziranih procedura za pristup službenim podacima, do ograničenja temeljenih na zaštiti osobnih podataka. Pored ovih, u pravu RH postoje i drugi posebni propisi koji uređuju dostupnost informacija u pojedinim usko definiranim područjima, koji se ovdje međutim ne analiziraju.

Cilj ovog poglavlja je u sažetom obliku prikazati pravne mehanizme koji stoje na raspolaganju novinarima, udrugama i građanima pri ostvarivanju prava na informacije, kao i ograničenja koja proizlaze iz pravne zaštite suprotstavljenih interesa.

2. Zakon o medijima

Zakon o medijima[1] propisuje neka osnovna pravila o dostupnosti javnih informacija u svom čl. 6. Aktivno ovlašteni na traženje informacija su novinari[2]. Prema čl. 6. st. 1., obveza davanja informacija odnosi se na:

- tijela izvršne, zakonodavne i sudbene vlasti
- tijela jedinica lokalne i područne (regionalne) samouprave
- ostale pravne i fizičke osobe koje obavljaju javnu službu i/ili dužnost.

Gore navedeni obveznici dužni su davati točne, potpune i pravovremene informacije o pitanjima iz svog djelokruga. Na ovom mjestu, bitno je istaknuti da pojam „informacije“ nije definiran u Zakonu o medijima. U tom smislu, može se opravdano tvrditi da je značenje „informacije“ u Zakonu o medijima šire od onoga iz Zakona o pravu na pristup informacijama, gdje se informacijom smatra podatak koji je na bilo koji način materijaliziran (primjerice u obliku dokumenta ili zapisa). Stoga se na temelju čl. 6. Zakona o medijima mogu tražiti „i pojaš-

[1] Zakon o medijima, NN 59/04, 84/11, 81/13, 114/22.

[2] Zakon o medijima u čl. 2 definira „novinara“ kao fizičku osobu „koja se bavi prikupljanjem, obradom, oblikovanjem ili razvrstavanjem informacija za objavu putem medija, te je zaposlena kod nakladnika na temelju ugovora o radu ili obavlja novinarsku djelatnost kao samostalno zanimanje, u skladu sa zakonom“.

njenja pojedinog pitanja, stajališta tijela i sl."[3] U tom smislu, ako novinar želi dobiti informaciju koja nije materijalizirana, jedino pravno sredstvo koje mu stoji na raspolaganju je čl. 6. Zakona o medijima. S druge strane, kad su potrebne informacije koje su materijalizirane u nekom obliku, prikladnije pravno sredstvo je vjerojatno Zakon o pravu na pristup informacijama (o tome više dalje u tekstu).

U provedbenom smislu, čelnici tijela odnosno pravnih osoba koje su obveznici davanja informacija temeljem Zakona o medijima dužni su urediti način davanja informacija te odrediti osobu koja osigurava dostupnost informacija. U praksi se često događa da se ista osoba odredi kao nadležna za davanje informacija po Zakonu o medijima i Zakonu o pravu na pristup informacijama pri čemu Zakon o medijima ne propisuje strogi rok za postupanje po zahtjevu, nego samo navodi da se informacija mora dati „u primjerenom roku".

Iznimke od obveze davanja informacija propisane su u čl. 6. st. 5. Zakona o medijima. Prema ovoj odredbi, davanje informacija može biti uskraćeno u dva slučaja. Prvo, ako su tražene informacije na propisan način određene kao državna ili vojna tajna, ili drugo, ako bi njihovo objavljivanje predstavljalo povredu tajnosti osobnih podataka sukladno zakonu. U drugom slučaju (zaštita osobnih podataka), iznimka se ne primjenjuje ako bi se objavom informacija moglo spriječiti izvršenje težega kaznenog djela ili spriječiti neposredna opasnost za život ljudi i njihovu imovinu. Ako tijelo odbije davanje informacije zbog nekog od gore navedenih razloga, dužno je, na pisani zahtjev podnositelja, u pisanom obliku obrazložiti razloge i to u roku od tri dana od dana zaprimanja takvog zahtjeva.

U slučaju da je davanje informacije uskraćeno, novinar ima pravo podnijeti tužbu zbog nezakonite radnje nadležnom sudu, o kojoj se odlučuje u hitnom postupku. Utvrdi li se da ne postoji razlog za uskratu informacije propisan Zakonom o medijima, sud će naložiti davanje tražene informacije.

3. Zakon o pravu na pristup informacijama

Zakon o pravu na pristup informacijama (dalje: ZPPI)[4] temeljni je propis u Republici Hrvatskoj za omogućavanje pristupa javnim informacijama. To čini na način da uređuje tri temeljna mehanizma za omogućavanje transparentnosti:

1. određene mjere proaktivne transparentnosti (mjere koje se poduzimaju bez posebnog zahtjeva)
2. pristup informacijama na zahtjev i
3. ponovnu uporabu informacija.
   Provođenje zakona kontrolira neovisno tijelo – Povjerenik za informiranje (https://pristupinfo.hr/).[5]

3.1. Polje primjene ZPPI-a

Zakon o pravu na pristup informacijama ima iznimno široko, ali ipak ne neograničeno djelovanje. ZPPI se primjenjuje u odnosu na (1) informacije, koje se nalaze u posjedu (2) tijela javne vlasti.

U pogledu pojma „informacije", sukladno definiciji iz čl. 5. ZPPI-a riječ je o „svakom podatku koji posjeduje tijelo javne vlasti u obliku dokumenta, zapisa, dosjea, registra, neovisno o načinu na koji je prikazan (napisani, nacrtani, tiskani, snimljeni, magnetni, optički, elektronički ili neki drugi zapis), koji je tijelo izradilo samo ili u suradnji s drugim tijelima ili dobilo od druge osobe, a nastao je u okviru djelokruga ili u vezi

[3] Rajko, Alen, Odnos sudova i medija (iz perspektive informacijskog upravnog prava, Zbornik radova 10. savjetovanja Novosti u upravnom pravu i upravnosudskoj praksi. Zagreb: Organizator, 2022. str. 326.

[4] Zakon o pravu na pristup informacijama, NN 25/13, 85/15, 69/22.

[5] V. čl. 35.-40. ZPPI-a.

s organizacijom i radom tijela javne vlasti". Informacija u smislu ZPPI-a mora biti materijalizirana.[6] Temeljem ZPPI-a nije moguće postići da tijelo javne vlasti stvori novu informaciju – ZPPI se odnosi samo na informacije koje u trenutku podnošenja zahtjeva postoje i to u materijaliziranom obliku. U tom dijelu ZPPI dakle ima uže djelovanje od Zakona o medijima, koji omogućava da se traže i informacije koje nisu materijalizirane.

Drugi kriterij za primjenu ZPPI-a jest da je informacija u posjedu „tijela javne vlasti". Prema čl. 5. st. 3. ZPPI-a, tijela javne vlasti su:

- tijela državne uprave,
- druga državna tijela,
- jedinice lokalne i područne (regionalne) samouprave,
- pravne osobe i druga tijela koja imaju javne ovlasti,
- pravne osobe čiji je osnivač Republika Hrvatska ili jedinica lokalne ili područne (regionalne) samouprave,
- pravne osobe koje obavljaju javnu službu,
- pravne osobe koje se temeljem posebnog propisa financiraju pretežito ili u cijelosti iz državnog proračuna ili iz proračuna jedinica lokalne i područne (regionalne) samouprave odnosno iz javnih sredstava (nameta, davanja, i sl.),
- trgovačka društva u kojima Republika Hrvatska i jedinice lokalne i područne (regionalne) samouprave imaju zasebno ili zajedno većinsko vlasništvo.

Najjednostavniji način za provjeriti je li neko tijelo obveznik ZPPI-a jest putem stranica Povjerenika za informiranje, gdje je moguće pronaći ažuran popis svih tijela javne vlasti (u trenutku pisanja ovog rada njih 5813), zajedno s adresama, adresama mrežnih stranica i kontakt podacima službenika za informiranje.

Usporedi li se popis obveznika ZPPI-a s onima na koji se primjenjuje čl. 6. Zakona o medijima, uočava se da ZPPI pokriva širi krug subjekata (primjerice, pravne osobe koje se financiraju iz javnih sredstava ili trgovačka društva u većinskom vlasništvu RH ili jedinica lokalne/područne samouprave. U praksi Povjerenika za informiranje moguće je pronaći veći broj odluka u kojima su se zahtjevi temeljem ZPPI-a s uspjehom postavljali protiv tijela iz navedenih kategorija.[7]

Konačno, određene informacije izuzete su iz polja primjene ZPPI-a, makar su njihovi posjednici tijela javne vlasti i unatoč tome što je riječ o „informaciji" u smislu tog zakona. Sukladno čl. 1. ZPPI-a, njegove odredbe ne primjenjuju se na:

- stranke u sudskim, upravnim i drugim na zakonu utemeljenim postupcima, kojima je dostupnost informacija iz tih postupaka utvrđena propisom.[8] U pravu RH postoji već broj zakona i drugih pravnih izvora koji pojedinim subjektima omogućavaju dostupnost informacija u kontekstu određenih postupaka. Primjerice, stranke i druge osobe koje za to imaju pravni interes imaju mogućnost obavijestiti se o tijeku upravnog postupka, razgledati spis i kopirati određene akte iz spisa temeljem čl. 84. Zakona o općem upravnom postupku.[9] Slična mogućnosti postoji i u parničnom[10] te kaznenom[11] postupku.
- na informacije za koje postoji obveza čuvanja tajnosti, sukladno zakonu koji uređuje sigurnosno-obavještajni sustav Republike Hrvatske.[12] Obveze o kojima je riječ uređene su Zakonom o sigurnosno-obavještajnom

[6] Povjerenik za informiranje, Pravo na pristup informacijama: Vodič za medije i udruge (dostupno na https://pristupinfo.hr/wp-content/uploads/2018/10/esf-vodic_web.pdf?x45242), str. 6.

[7] Odluke dostupne odgovarajućim filtiranjem na stranici https://tom.pristupinfo.hr/pregledfilter1.php.

[8] ZPPI čl. 1. st. 3.

[9] Zakon o općem upravnom postupku, NN 47/09, 110/21.

[10] V. čl. 150. Zakona o parničnom postupku, SL SFRJ Službeni list SFRJ br. 4/1977, 36/1977, 36/1980, 6/1980, 69/1982, 43/1982, 58/1984, 74/1987, 57/1989, 20/1990, 27/1990, 35/1991, NN 53/1991, 91/1992, 112/1999, 129/2000, 88/2001, 117/2003, 88/2005, 2/2007, 96/2008, 84/2008, 123/2008, 57/2011, 25/2013, 89/2014, 70/2019, 80/2022, 114/2022, 155/2023.

[11] V. čl. 184. Zakona o kaznenom postupku, NN 152/2008, 76/2009, 80/2011, 91/2012, 143/2012, 56/2013, 145/2013, 152/2014, 70/2017, 126/2019, 126/2019, 80/2022, 36/2024, 72/2025.

[12] ZPPI čl. 1. st. 4.

sustavu Republike Hrvatske[13] te se odnose na informacije koje predstavljaju klasificirane informacije čiji su vlasnici međunarodne organizacije ili druge države, te klasificirane informacije tijela javne vlasti koje nastaju ili se razmjenjuju u okviru suradnje s međunarodnim organizacijama ili drugim državama.[14]

3.2. Proaktivna transparentnost

Prvi način kako se prema Zakonu o pravu na pristup informacijama proaktivno osigurava transparentnost rada tijela javne vlasti je putem obveznog objavljivanja informacija. Sukladno čl. 10., tijela javne vlasti dužna su na svojim **mrežnim stranicama** u strojno čitljivom obliku objavljivati informacije iz zakonom propisanih kategorija, kao što su opći akti i odluke kojima se utječe na interese korisnika, godišnje planove, programe, strategije, izvješća o radu, podatke o financiranju, dodjelama sredstva, sponzorstvima, natječajima i sl.[15]

Nadalje, temeljem čl. 10.a postoji obveza dostavljanja određenih dokumenata **u Središnji katalog službenih dokumenata Republike Hrvatske**. Ta obveza odnosi se na (1) opće akte i odluke koje donose, kojima se utječe na interese korisnika, s razlozima za njihovo donošenje, i (2) godišnje planove, programe, strategije, upute, izvješća o radu, financijska izvješća i druge odgovarajuće dokumente koji se odnose na područje rada tijela javne vlasti. Navedena obveza pokriva nešto uži krug obveznika nego definicija „tijela javne vlasti".[16] Središnji katalog službenih dokumenata dostupan je na https://sredisnjikatalogrh.gov.hr/sredisnji-katalog/pravni-propisi.

Također, tijela državne uprave, druga državna tijela, jedinice lokalne i područne (regionalne) samouprave i pravne osobe s javnim ovlastima dužni su provoditi savjetovanja s javnošću pri donošenju:

- zakona,
- podzakonskih propisa,
- općih akata odnosno drugih strateških ili planskih dokumenta kad se njima utječe na interese građana i pravnih osoba.

Kad savjetovanja provode državna tijela ona se obavljaju putem središnjeg državnog internetskog portala za savjetovanja s javnošću, a kad to čine drugi obveznici mogu to raditi i putem svoje internetske stranice.[17]

Konačno, u čl. 12. ZPPI-a propisano je da su tijela javne vlasti obvezna informirati javnost i o dnevnom redu zasjedanja/sjednica njihovih službenih tijela, mogućnostima neposrednog uvida u njihov rad, i broju osoba kojima se može osigurati neposredan uvid (prisustvo).

3.3. Davanje informacija na zahtjev

Kako je prethodno objašnjeno, tijela javne vlasti dužna su proaktivno poduzeti određene mjere u smislu proaktivne transparentnosti, odnosno učiniti određene informacije dostupnima na zakonom propisane načine i kad to nitko ne traži. Pored toga, ona su obveznici jedne iznimno široke mjere, a to je da daju informacije koje imaju u svom posjedu na zahtjev korisnika. Drugim riječima, načelno svaka informacija koja nije javno objavljena također može biti otkrivena, ako to netko traži.

Koncept informacije koja se može tražiti je objašnjen iznad (3.1.). U bitnome, riječ je o bilo kojem podatku koji je materijaliziran odnosno pohranjen u obliku zapisa, dokumenta, dosjea, registra i slično, neovisno o tome kojom tehnologijom je to učinjeno.

[13] Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, NN 79/2006, 105/2006.
[14] ZPPI čl. 1. st. 5.
[15] Za puni popis v. čl. 10. st. 1. ZPPI-a.
[16] ZPPI, čl. 10.a st. 1.
[17] V. čl. 11. ZPPI-a.

U kontekstu Zakona o pravu na pristup informacijama osobu koja zahtijeva davanje informacije naziva se „korisnik". Pojam korisnika definiran je iznimno široko i uključuje svaku domaću ili stranu fizičku i pravnu osobu. Drugim riječima, iz navedenog jasno slijedi da informaciju od tijela javne vlasti može tražiti bilo tko.

U pogledu načina traženja informacije, ZPPI propisuje da se zahtjev može postaviti u usmenom ili pisanom obliku.[18] Ključno je da podnositelj zahtjeva nije dužan navoditi razloge zbog kojih traži informaciju, niti je dužan pozvati se na primjenu ZPPI-a.[19] Iz navedenog jasno slijedi da je pravo na pristup informacijama, ovdje u smislu prava na dobivanje informacije na zahtjev, iznimno široko formulirano. Ono međutim ipak nije neograničeno.

Prvo, u čl. 18. st. 5. ZPPI-a propisano je da se ne smatra „zahtjevom za pristup informacijama traženje uvida u cjelokupni spis predmeta, objašnjenja ili uputa vezanih uz ostvarivanje nekog prava ili izvršavanje obveze, izrade analize ili tumačenja nekog propisa, kao ni stvaranje nove informacije".

Drugo, ZPPI predviđa određeni broj iznimki od prava na pristup informacijama, koje izazivaju različite učinke.

Za početak, čl. 15. st. 1. ZPPI-a propisuje da će tijela javne vlasti ograničiti pristup informacijama koje se tiču svih postupaka koje vode nadležna tijela u prethodnom i kaznenom postupku za vrijeme trajanja tih postupaka. Ova iznimka ne odnosi se samo na one slučajeve kad se informacija traži od tijela koja vode prethodne odnosno kaznene postupke. U praksi Povjerenika za informiranje je tako moguće pronaći odluke u kojima su se i druga tijela, primjerice javno visoko učilište, s uspjehom mogla pozvati na činjenicu da je riječ o informaciji koja je dio dokumentacije u pogledu koje se vode izvidi od strane državnog odvjetništva.[20] Ako se utvrdi da je riječ o informaciji koja je tiče prethodnog ili kaznenog postupka, tijelo javne vlasti koje primi zahtjev mora ga odbiti.

Nadalje, čl. 15. st. 2. ZPPI-a sadrži određeni broj dodatnih iznimki. Kako je tamo propisano, „tijela javne vlasti mogu ograničiti pristup informaciji:

1) ako je informacija klasificirana stupnjem tajnosti, sukladno zakonu kojim se uređuje tajnost podataka;
2) ako je informacija poslovna ili profesionalna tajna, sukladno zakonu;
3) ako je informacija porezna tajna, sukladno zakonu;
4) ako je informacija zaštićena propisima kojima se uređuje područje zaštite osobnih podataka;
5) ako je informacija zaštićena propisima kojima se uređuje pravo intelektualnog vlasništva, osim u slučaju izričitoga pisanog pristanka nositelja prava;
6) ako je pristup informaciji ograničen sukladno međunarodnim ugovorima ili se radi o informaciji nastaloj u postupku sklapanja ili pristupanja međunarodnim ugovorima ili pregovora s drugim državama ili međunarodnim organizacijama, do završetka postupka, ili se radi o informaciji nastaloj u području održavanja diplomatskih odnosa;
7) u ostalim slučajevima utvrđenim zakonom."

Prva od gore navedenih iznimki odnosi se na informacije **klasificirane stupnjem tajnosti**.[21] Propis koji uređuje klasifikacije tajnih informacija je Zakon o tajnosti podataka.[22] Sukladno čl. 4 ovog zakona, stupnjevi tajnosti klasificiranih podataka su (1) vrlo tajno, (2) tajno, (3) povjerljivo i (4) ograničeno. Ovim stupnjevima tajnosti mogu se klasificirati „podaci iz djelokruga državnih tijela u području obrane, sigurno-

[18] V. čl. 18. st. 1. ZPPI-a.
[19] V. čl. 18. st. 4. ZPPI-a.
[20] Primjerice: rješenje klasa UP/II-008-07/24-01/287, broj 401-01/06-24-5, od 12. rujna 2024.
[21] Detaljno o ovoj iznimci v. u Smjernicama za provedbu Zakona o pravu na pristup informacijama: Pristup informacijama i klasificiranim podacima, 2024, dostupno na https://pristupinfo.hr/wp-content/uploads/2025/01/Smjernica-pristup-informacijama-i-klasificiranim-podacima.pdf?x45242
[22] Zakon o tajnosti podataka, NN 79/2007, 86/2012.

sno-obavještajnog sustava, vanjskih poslova, javne sigurnosti, kaznenog postupka te znanosti, tehnologije, javnih financija i gospodarstva ukoliko su podaci od sigurnosnog interesa za Republiku Hrvatsku".[23] Ovo je bitno ograničenje, jer nisu sva tijela javne vlasti koja su obveznici ZPPI-a ovlaštena klasificirati podatke stupnjem tajnosti.[24] Podatak klasificira tijelo u okviru čijeg djelovanja je podatak nastao, a koje se naziva „vlasnik podataka".

Također, sukladno čl. 2. Zakona o tajnosti podataka, klasificirani podatak je i onaj „kojeg je Republici Hrvatskoj tako označenog predala druga država, međunarodna organizacija ili institucija s kojom Republika Hrvatska surađuje". Ovo je bitno jer, ako je riječ o zahtjevu za pristupom informaciji iz ove kategorije, ZPPI se neće primjenjivati.[25]

Kad primi zahtjev za pristupom informaciji koja je klasificirana stupnjem tajnosti (a nije međunarodna informacija), tijelo javne vlasti mora provjeriti je li ono vlasnik informacije. Ako nije, dužno je ustupiti zahtjev vlasniku informacije. Drugim riječima, ako tijelo javne vlasti ima u posjedu klasificirani podatak, ali nije njegov vlasnik u smislu Zakona o tajnosti podataka, dužno je ustupiti zahtjev vlasniku.[26]

Činjenica da je informacija klasificirana stupnjem tajnosti nije apsolutna smetnja za njeno otkrivanje temeljem ZPPI-a (osim ako je riječ o međunarodnim informacijama, kako je objašnjeno gore). Prvo, ako informacija sadrži neklasificirane dijelove, oni se moraju otkriti (osim ako se u pogledu njih ne primjenjuje neko drugo ograničenje).[27]

Jednom kad se zahtjev nalazi kod vlasnika informacije, bilo da je izvorno upućen tom tijelu, bilo da mu je ustupljen, vlasnik informacije dužan je pribaviti mišljenje Ureda Vijeća za nacionalnu sigurnost i nakon toga provesti test razmjernosti i javnog interesa. U praksi Povjerenika za informiranje, kao i u sudskoj praksi, je prihvaćeno da sam Povjerenik nema ovlast preispitivati da li je informacija pravilno klasificirana, niti predložiti njenu deklasifikaciju.[28]

Druga iznimka predviđena Zakonom o pravu na pristup informacijama jest ako je informacija **poslovna ili profesionalna tajna**. Institut poslovne tajne reguliran je Zakonom o zaštiti tajnosti podataka.[29] Sukladno ovom zakonu, poslovna tajna su podaci koji su „kao poslovna tajna određeni zakonom, drugim propisom ili općim aktom trgovačkog društva, ustanove ili druge pravne osobe, a koji predstavljaju proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada te druge podatke zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za njezine gospodarske interese".[30] Iz navedenog jasno slijedi da su dva temeljna uvjeta za postojanje poslovne tajne:

1. da je ona određena zakonom, propisom ili općim aktom, i
2. da štiti podatak koji predstavlja proizvodnu tajnu, rezultate istraživačkog ili konstrukcijskog rada, ili druge podatke zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za njezine gospodarske interese.

Osobito je bitno da je Zakonom o zaštiti tajnosti podataka propisano da se općim aktom „ne

[23] Zakon o tajnosti podataka, čl. 5.

[24] Primjerice, kako objašnjava Povjerenik, „Ministarstvo unutarnjih poslova je ovlašteno klasificirati podatke s određenim stupnjem tajnosti za razliku od dječjeg vrtića koji nije ovlašten klasificirati podatke". Vidi Smjernice za provedbu Zakona o pravu na pristup informacijama: Pristup informacijama i klasificiranim podacima, 2024, dostupno na https://pristupinfo.hr/wp-content/uploads/2025/01/Smjernica-pristup-informacijama-i-klasificiranim-podacima.pdf?x45242, str. 3.

[25] ZPPI, čl. 1. st. 5.

[26] V. čl. 21. st. 2. ZPPI-a: „Ako tijelo javne vlasti zaprimi zahtjev za pristup informaciji iz članka 15. stavka 2. točke 1. ovog Zakona, a nije njezin vlasnik, dužno je bez odgode, a najkasnije u roku od osam dana od zaprimanja zahtjeva, ustupiti zahtjev vlasniku informacije, o čemu će obavijestiti podnositelja."

[27] V. čl. 15. st. 5. ZPPI-a: „Ako tražena informacija sadrži i podatak koji podliježe ograničenju iz stavaka 2. i 3. ovoga članka, preostali dijelovi informacije učinit će se dostupnim."

[28] Vidi primjerice odluku u predmetu klasa UP/II-008-07/23-01/184, broj: 401-01/04-23-3, od 20. travnja 2023.

[29] Zakon o zaštiti tajnosti podataka, NN 108/1996, 79/2007.

[30] Zakon o zaštiti tajnosti podataka, čl. 19. st. 1.

može odrediti da se svi podaci koji se odnose na poslovanje pravne osobe smatraju poslovnom tajnom niti se poslovnom tajnom mogu odrediti podaci čije priopćavanje nije razložno protivno interesima te pravne osobe".[31]

Drugi pravni izvor koji uređuje institut poslovne tajne je Zakon o zaštiti neobjavljenih informacija s tržišnom vrijednosti.[32] Sukladno ovom zakonu, poslovna tajna su informacije koje ispunjavaju sljedeće uvjete:

a) tajne su jer nisu, u svojoj ukupnosti ili u točnoj strukturi i sklopu svojih sastavnih dijelova, općenito poznate ili lako dostupne osobama iz krugova koji se obično bave predmetnom vrstom informacija
b) imaju tržišnu (komercijalnu) vrijednost zbog toga što su tajne
c) u odnosu na njih osoba koja te informacije zakonito kontrolira poduzela je u tim okolnostima razumne korake kako bi sačuvala njihovu tajnost."

U praksi, tijela javne vlasti se često pozivaju na institut poslovne tajne kako bi opravdala odbijanje pristupa određenim informacijama, makar za to ne postoje opravdani razlozi.[33]

U pogledu profesionalne tajne, polazna odredba je čl. 27. Zakona o zaštiti tajnosti informacija, koji propisuje da „profesionalnu tajnu predstavljaju podaci o osobnom ili obiteljskom životu stranaka koje saznaju svećenici, odvjetnici, zdravstveni i socijalni djelatnici, i druge službene osobe u obavljanju svog poziva". Iz predmetne definicije proizlazi da profesionalnu tajnu mogu uživati samo pripadnici posebnog kruga osoba koje obavljaju određen poziv odnosno zanimanje. Radi se dakle o slučajevima u kojima obavljanje poziva zahtijeva povećani stupanj povjerenja bez kojega bi i sama opstojnost poziva bila dovedena u pitanje. U pravu Republike Hrvatske postoje posebni propisi koji uređuju profesionalne tajne pojedinih profesija, primjerice odvjetničke,[34] javnobilježničk,[35] bankarske,[36] itd. U kontekstu ZPPI-a, činjenica da se traži pristup informaciji koja uključuje profesionalnu tajnu ima učinak relativne iznimke, na koju se primjenjuje test razmjernost i javnog interesa (vidi dolje).

Jedna od relativnih iznimki prema ZPPI-u je i ako je ako je informacija **porezna tajna**. Sadržaj i opseg čuvanja porezne tajne uređeni su Općim poreznim zakonom, koji u čl. 8. propisuje, između ostalog, da je „porezno tijelo dužno … kao poreznu tajnu čuvati sve podatke koje porezni obveznik iznosi u poreznom postupku te sve druge podatke u vezi s poreznim postupkom kojima raspolaže, kao i podatke koje razmjenjuje s drugim državama u poreznim stvarima".[37] U kontekstu ZPPI-a, činjenica da se traži pristup informaciji koja uključuje poreznu tajnu ima učinak relativne iznimke, na koju se primjenjuje test razmjernost i javnog interesa (vidi dolje).

---

[31] Zakon o zaštiti tajnosti podataka, čl. 19. st. 2.

[32] Zakon o zaštiti neobjavljenih informacija s tržišnom vrijednosti, NN 30/2018.

[33] Vidi o tome praksu Povjerenika na https://tom.pristupinfo.hr/. Isto i u Smjernicama za provedbu Zakona o pravu na pristup informacijama: Pristup informacijama i poslovnoj tajni, 2024, dostupno na https://pristupinfo.hr/wp-content/uploads/2025/01/Smjernice-poslovna-tajna.pdf?x45242

[34] V. čl. 13. Zakona o odvjetništvu (NN 9/1994, 117/2008, 50/2009, 75/2009, 18/2011, 126/2021): „(1) Odvjetnik je dužan, sukladno zakonu, čuvati kao odvjetničku tajnu sve što mu je stranka povjerila ili što je u zastupanju stranke na drugi način saznao.
(2) Odvjetničku tajnu dužne su čuvati i druge osobe koje rade ili su radile u odvjetničkom uredu."

[35] V. čl. 37. Zakona o javnom bilježništvu (NN 78/1993, 29/1994, 162/1998, 16/2007, 75/2009, 120/2016, 57/2022): „(1) Javni bilježnik je dužan čuvati kao tajnu ono za što je saznao u obavljanju svoje službe, osim ako iz zakona, volje stranaka ili sadržaja pravnog posla ne proizlazi što drugo. …"

[36] V. čl. 156. Zakona o kreditnim institucijama (NN 59/2013, 19/2015, 102/2015, 15/2018, 70/2019, 47/2020, 146/2020, 151/2022, 145/2024): „(1) Bankovna tajna su svi podaci, činjenice i okolnosti koje je kreditna institucija saznala na osnovi pružanja usluga klijentima i u obavljanju poslova s pojedinačnim klijentom. Kreditna institucija dužna je čuvati bankovnu tajnu.
(2) U smislu ovoga Zakona klijentom kreditne institucije smatra se svaka osoba koja je zatražila ili primila bankovnu i/ili financijsku uslugu od kreditne institucije."

[37] Kao iznimka, „ne smatra poreznom tajnom:
1. podatak o datumu upisa u sustav poreza na dodanu vrijednost ili ispisa iz sustava poreza na dodanu vrijednost
2. podatak o poreznim obveznicima koji su davali lažne podatke s namjerom umanjenja svoje ili tuđe obveze poreza na dodanu vrijednost (kružne prijevare poreza na dodanu vrijednost) ako je to utvrđeno u porezno-pravnom postupku". V. čl. 8. Općeg poreznog zakona (NN 115/2016, 106/2018, 121/2019, 32/2020, 42/2020, 114/2022, 152/2024).

Konačno, značajna iznimka u kontekstu prava na pristup informacijama jesu **osobni podaci**. Naime, prema čl. 15. st. 2. ZPPI-a, tijela javne vlasti mogu ograničiti pristup informaciji ako je ona zaštićena propisima kojima se uređuje područje zaštite osobnih podataka. Propis koji definira pojam osobnog podatka, kao i sadržaj i doseg njihove zaštite, je Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka).[38] Prema čl. 4. st. 1. ove Uredbe, osobni podaci su „svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi („ispitanik"); pojedinac čiji se identitet može utvrditi jest osoba koja se može identificirati izravno ili neizravno, osobito uz pomoć identifikatora kao što su ime, identifikacijski broj, podaci o lokaciji, mrežni identifikator ili uz pomoć jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca". Riječ je samo na prvi pogled o jednostavnoj definiciji. Iz citirane odredbe čl. 4. točke 1. Opće uredbe o zaštiti podataka slijedi da postoje četiri konstitutivna elementa definicije osobnog podatka koja uvijek kumulativno moraju postajati. Riječ je o:

- bilo kojem podatku ili informaciji,
- koji se odnosi
- na pojedinca
- čiji identitet je utvrđen ili se može utvrditi.[39]

Pitanje je li neka informacija osobni podatak ili ne nije nužno jednostavno kako se na prvi pogled čini, i oko ovoga postoji detaljna praksa Suda Europske unije.[40] U kontekstu ZPPI-a, činjenica da se traži pristup informaciji koja uključuje osobne podatke ima učinak relativne iznimke, na koju se primjenjuje test razmjernost i javnog interesa (vidi dolje).

Nadalje, čl. 15. st. 2. t. 5. ZPPI propisuje da tijela javne vlasti mogu ograničiti pristup informaciji koja je zaštićena propisima kojima se uređuje **pravo intelektualnog vlasništva**, osim u slučaju izričitoga pisanog pristanka nositelja prava. Tipična ovakva situacija je kad se traži pristup djelu koje je zaštićeno temeljem Zakona o autorskom pravu i srodnim pravima,[41] makar u obzir mogu doći i druga prava intelektualnog vlasništva.

Konačno, ZPPI predviđa još nekoliko iznimki, koje se u praksi nešto rjeđe susreću:

- ako je pristup informaciji ograničen sukladno međunarodnim ugovorima ili se radi o informaciji nastaloj u postupku sklapanja ili pristupanja međunarodnim ugovorima ili pregovora s drugim državama ili međunarodnim organizacijama, do završetka postupka, ili se radi o informaciji nastaloj u području održavanja diplomatskih odnosa (ZPPI čl. 15. st. 2. t. 6).
- ako bi objavljivanje informacije onemogućilo učinkovito, neovisno i nepristrano vođenje sudskog, upravnog ili drugog pravno uređenog postupka, izvršenje sudske odluke ili kazne (ZPPI čl. 15. st. 3. t. 1).
- ako bi objavljivanje informacije onemogućilo rad tijela koja obavljaju upravni nadzor, inspekcijski nadzor, odnosno nadzor zakonitosti (ZPPI čl. 15. st. 3. t. 2).
- ako je informacija u postupku izrade unutar jednog ili među više tijela javne vlasti, a njezino bi objavljivanje prije dovršetka izrade cjelovite i konačne informacije moglo ozbiljno narušiti proces njezine izrade (ZPPI čl. 15. st. 4. t. 1).
- ako je informacija nastala u postupku usuglašavanja pri donošenju propisa i drugih akata te u razmjeni stavova i mišljenja unutar jednog ili među više tijela javne vlasti, a njezino bi objavljivanje moglo dovesti do pogrešnog tumačenja sadržaja informacije, ugroziti proces donošenja propisa i akata ili slobodu davanja mišljenja i izražavanja stavova (ZPPI čl. 15. st. 4. t. 2).

[38] SL L 119, 4.5.2016, p. 1–88.
[39] O ovome vidi detaljno u Jurić, Katulić, Lisičar, Zaštita osobnih podataka: prvi dio, Zagreb, 2025.
[40] Vidi iznimno koristan vodič na dpcuria.eu.
[41] Zakon o autorskom pravu i srodnim pravima, NN 111/2021.

U svim prethodno navedenim slučajevima, tijelo javne vlasti od kojeg se traži informacija dužno je provesti **test razmjernosti i javnog interesa**. Riječ je o procjeni razmjernosti između razloga za omogućavanje pristupa informaciji i razloga za ograničenje, koji dovodi do omogućavanje pristupa informaciji ako prevladava javni interes.[42] Sukladno čl. 16. st. 2. ZPPI-a, „kod provođenja testa razmjernosti i javnog interesa tijelo javne vlasti dužno je utvrditi da li se pristup informaciji može ograničiti radi zaštite nekog od zaštićenih interesa iz članka 15. stavka 2., 3. i 4. ovog Zakona, da li bi omogućavanjem pristupa traženoj informaciji u svakom pojedinom slučaju taj interes bio ozbiljno povrijeđen te da li prevladava potreba zaštite prava na ograničenje ili javni interes. Ako prevladava javni interes u odnosu na štetu po zaštićene interese, informacija će se učiniti dostupnom".[43]

3.4. Ponovna uporaba informacija

Ponovna uporaba informacija specifično je pravo iz Zakona o pravu na pristup informacijama, koje ima za cilj osigurati otvorenost podataka javne uprave. Prema tom zakonu, ponovna uporaba „znači uporabu informacija tijela javne vlasti od strane fizičkih ili pravnih osoba, u komercijalnu ili nekomercijalnu svrhu različitu od izvorne svrhe za koju su informacije nastale, a koja se ostvaruje u okviru zakonom ili drugim propisom određenog djelokruga ili posla koji se uobičajeno smatra javnim poslom. Razmjena informacija između tijela javne vlasti radi obavljanja poslova iz njihova djelokruga ne predstavlja ponovnu uporabu".[44]

Ponovna uporaba informacija tipično se osigurava objavljivanjem u elektroničkom obliku, u strojno čitljivom, pristupačnom i otvorenom formatu, u skladu s otvorenim standardima. U RH, Portal otvorenih podataka[45] predstavlja podatkovni čvor koji služi za prikupljanje, kategorizaciju i distribuciju otvorenih podataka javnog sektora. U trenutku pisanja ovog rada Portal omogućava pristup gotovo tri tisuće otvorenih skupova podataka.[46] Temeljem ovih podataka razvijene su od strane korisnika i određene računalne aplikacije.[47]

4. Opća uredba o zaštiti podataka

Opća uredba o zaštiti podataka primjenjuje se na zaštitu osobnih podataka kao osobnog prava svake fizičke osobe. U tom smislu, ona se ne čini pretjerano relevantnom za pitanje pristupa podacima od strane javnog i privatnog sektora. Međutim, potrebno je obratiti pažnju na njen čl. 15, koji uređuje pravo ispitanika na pristup. Sukladno ovom članku, svaka fizička osoba ima pravo dobiti od voditelja obrade:

1. potvrdu obrađuju li se osobni podaci koji se odnose na njega ili nju, i
2. ako se obrađuju, pristup osobnim podacima i određenim informacijama o obradi, i
3. kopiju osobnih podataka.

Pravo na pristup osobnim podacima ima u dijelu uže, ali u dijelu bitno šire djelovanje od ZPPI-a. Ono je uže u smislu da se ne odnosi na „informaciju" kako je definirana ZPPI-em, nego na „osobni podatak", a koji je u bitnome podatak koji se odnosi na pojedinu fizičku osobu. U tom smislu, temeljem Opće uredbe o zaštiti podataka svatko može tražiti pristup svojim osobnim podacima, i njihovu kopiju. Nije moguće tražiti osobne podatke drugih osoba. Međutim, koncept osobnog podatka prema Općoj uredbi je iznimno širok, i uključuje sve informacije koje se „odnose" na dotičnu fizičku osobu. Prema tekstu uredbe, osobni podatak je podatak koji se

[42] ZPPI čl. 5. st. 7.
[43] O ovome vidi detaljno u Smjernicama za provedbu Zakona o pravu na pristup informacijama: Test razmjernosti i javnog interesa, dostupno na https://www.pristupinfo.hr/wp-content/uploads/2018/10/Smjernice-Test-razmjernosti-i-javnog-interesa-1.pdf.
[44] ZPPI, čl. 5. st. 6.
[45] Dostupan na data.gov.hr
[46] https://data.gov.hr/ckan/hr/dataset
[47] https://data.gov.hr/aplikacije?dataUsage=APPLICATION

„odnosi na pojedinca“ (neku konkretnu fizičku osobu). Drugim riječima, između podatka i pojedinca (osobe) mora postojati određena veza. U praksi, informacija se odnosi na osobu ako je ona s tom osobom povezana temeljem svog sadržaja, svrhe obrade ili rezultata obrade.[48] Primjenom ovih kriterija moguće je doći do ishoda u kojem se veoma širok krug informacija može povezati s pojedinom fizičkom osobom. Ako se u tome uspije, onda se pravo na pristup podatku, kao i pravo na dobivanje kopije, može koristiti prema bilo kojem voditelju obrade, što uključuje ne samo tijela javne vlasti nego i privatnopravne subjekte. Jedino ograničenje je da pravo na dobivanje kopije (ali ne i pravo na pristup) ne smije negativno utjecati na prava i slobode drugih. Konačno, bitno je za naglasiti da se prva kopija podataka mora dati bez naknade.[49]

5. Zaključak

Temeljni pravni izvor za pristup informacijama u Republici Hrvatskoj je Zakon o pravu na pristup informacijama. Njegovom primjenom moguće je, uz određene iznimke, načelno osigurati pristup bilo kojoj informaciji koja je u posjedu tijela javne vlasti. Zakon o medijima će poslužiti kao korisno sredstvo kad se traži informacija koja nije materijalizirana, odnosno ne ispunjava uvjete za „informaciju“ temeljem ZPPI-a. Opća uredba o zaštiti podataka ima usko djelovanje jer se odnosi samo na mogućnost pribavljanja osobnih podataka podnositelja zahtjeva, ali u tom dijelu djeluje iznimno široko, jer otvara mogućnost dobivanja podataka i od privatnopravnih subjekata.

[48] O ovome vidi detaljno u Jurić, Katulić, Lisičar, Zaštita osobnih podataka: prvi dio, Zagreb, 2025.

[49] V. čl. 12. st. 5. Opće uredbe o zaštiti podataka.

Fact-checking, privatnost i zaštita osobnih podataka – između javnog interesa i zaštite temeljnih prava

Izv. prof. dr. sc. Tihomir Katulić
Pravni fakultet Sveučilišta u Zagrebu

1. Uvod

Neovisni *fact-checkeri* i novinarske nevladine organizacije u Europskoj uniji djeluju na razmeđu istraživačkog novinarstva od javnog interesa i zaštite osobnih podataka kao temeljnog prava prepoznatog Poveljom o temeljnim pravima.[1]

Fact-checkeri ispituju tvrdnje, koje često uključuju osobne podatke, kako bi podržali transparentnost, točnost i odgovornost u javnom diskursu. Pritom su dužni pridržavati se strogih zahtjeva koje uspostavlja europski sustav zaštite osobnih podataka uređen već široko poznatom Općom uredbom o zaštiti podataka (*General Data Protection Regulation*, GDPR[2]), istovremeno čuvajući temeljno pravo na slobodu informiranja i izražavanja. Ova obveza može predstavljati značajne praktične izazove i poteškoće budući da novinari trebaju pristup informacijama i mogućnost objavljivanja u javnom interesu, ali pojedinci (*ispitanici*) čiji se osobni podaci objavljuju (*obrađuju*) posjeduju široku i snažnu zaštitu prava na privatnost i prava na zaštitu podataka koja se ne mogu zanemariti.[3] U praksi to znači da je nužno ostvariti balans između transparentnosti i povjerljivosti, istinitog i potpunog izvještavanja i zaštite privatnosti i osobnih podataka.

Aktivnosti nadzornih tijela i novinarskih organizacija širom EU pokazuju koliko je važno imati jasne smjernice o balansiranju ovih često suprotstavljenih interesa. Tako primjerice britanski Kodeks ponašanja o zaštiti podataka u novinarstvu koji je pripremio Ured povjerenika za informiranje (ICO) detaljno propisuje kako novinarske grupe mogu slijediti zakon o zaštiti podataka kada se bave novinarstvom.[4] Pitanje ostvarivanja ovog balansa predmet je znanstvenog i stručnog interesa, pa su se problemi s kojima se europski *fact-checkeri* suočavaju u stvarnom svijetu istraživali na području nekoliko EU država članica kao što su Španjolska, Francuska, Portugal i Italija. Studija je pokazala da te grupe podržavaju visoke standarde otvorenosti i odgovornosti iako gotovo uvijek u praksi imaju male timove s ograničenim resur-

[1] Povelja Europske unije o temeljnim pravima, dostupna na: https://eur-lex.europa.eu/HR/legal-content/summary/charter-of-fundamental-rights-of-the-european-union.html

[2] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka, OUZP)

[3] v. čl. 4. OUZP.

[4] ICO Data Protection and Journalism Code of Practice 2023, dostupan na adresi: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-and-journalism-code-of-practice/journalism-code/

sima, no koje ipak u pravilu uspijevaju osobama koje su predmet novinarskog interesa osigurati "pravo na odgovor" i uključiti javnost u svoj rad što pokazuje da im je stalo do poštenja i poštivanja temeljnih prava.

Također, ista studija govorila je o "teškoćama u pristupu javnim informacijama" i drugim velikim problemima s kojima se moraju nositi *fact-checkeri*, poput nedostatka potrebnih financijskih i ljudskih resursa za sve potrebne kontrole i procese te pritiskom konkurencije.[5]

Neki od tih problema povezani su s pitanjima privatnosti na indirektan način, npr. javni službenici možda neće dijeliti informacije jer su zabrinuti za osobne podatke ili će malim timovima biti teško osigurati pomoć stručnjaka za pitanja pravne usklađenosti. Pravni stručnjaci ukazuju na razvoj novi aspekata prava na zaštitu podataka poput *"prava na zaborav"* (pravo na brisanje[6]) i što to znači za čuvanje internetskih informacija u javnoj digitalnoj sferi.

Budući da internetske arhive dugo ostaju aktivne, čak i ispravno izvještavanje može dugoročno naštetiti imidžu medijske organizacije. Zbog toga se medijski profesionalci i *fact-checkeri* podjednako pitaju kako uravnotežiti trajnu dostupnost osobnih podataka na internetu s pravima na zaštitu privatnosti i osobnih podataka. Europski sudovi počeli su se baviti tim problemima, podržavajući ideju da osobne informacije koje su zastarjele ili više nisu relevantne ponekad trebaju ostati privatne.

Cilj ovog poglavlja je pružiti pregled postupaka i mjera zaštite podataka posebno osmišljenih za osobe koje provjeravaju činjenice i neovisne novinarske organizacije na području Europske unije, počevši s prikazom osnovnih načela zaštite osobnih podataka prema Općoj uredbi o zaštiti podataka iz perspektive relevantnosti za novinarski poziv. Pokušat ćemo dati konkretne odgovore i savjete koji vode odgovornom upravljanju osobnim podacima u postupcima provjere činjenica, osiguravanju točnosti i nepristranosti, adekvatnom ispunjavanju zahtjeva i osiguranju prava ispitanika (s posebnim naglaskom na pravo na brisanje odnosno zahtjeve za brisanjem osobnih podataka) i usklađivanje slobode izražavanja s pitanjima zaštite osobnih podataka odnosno privatnosti.

2. Pregled načela zaštite osobnih podataka važnih za novinarstvo i *fact-checking*

Članak 5. Opće uredbe o zaštiti podataka (OUZP) uređuje osnovna načela zaštite osobnih podataka koja su obvezna za sve voditelje i izvršitelje obrade, odnosno organizacije, pravne osobe i pojedince koji uređuju način i sredstva obrade osobnih podataka. Drugim riječima, sve organizacije koje obrađuju osobne podatke na području Europske unije, pa tako i organizacije *fact-checkera* dužne su poštivati ova osnovna načela zaštite osobnih podataka, uz neka ograničenja o kojima će biti riječ kasnije u ovom prikazu.

Načela zaštite osobnih podataka čine osnovu za obradu osobnih podataka na siguran, zakonit i povjerljiv način, i od presudne su važnosti za novinarski poziv.

2.1. Načelo zakonitosti, poštenosti i transparentnosti

Prema Općoj uredbi o zaštiti podataka, osobni podaci trebaju se obrađivati u skladu sa zakonom (na temelju odgovarajuće pravne osnove), a njima se treba upravljati pošteno i transparentno prema pojedincu čiji se podaci obrađuju.

U praksi, zakonitost zahtijeva da osobe koje provjeravaju činjenice posjeduju čvrstu pravnu osnovu za prikupljanje ili korištenje osobnih podataka, kao što je pristanak, legitimni interes ili javni interes u novinarstvu.

---

[5] Moreno-Gil, V., Ramon-Vegas, X., & Mauri-Ríos, M. "Bringing journalism back to its roots: examining fact-checking practices, methods, and challenges in the Mediterranean context.", *Profesional De La información, 31*(2). 2022. https://doi.org/10.3145/epi.2022.mar.15

[6] v. čl. 16. OUZP.

Poštenost u ovom kontekstu označava izbjegavanje korištenja činjenica na načine koji nepravedno dovode u nepovoljan položaj osobe, uzimajući u obzir njihova legitimna očekivanja.

Transparentnost obično zahtijeva obavještavanje pojedinaca o korištenju njihovih podataka. U standardnim situacijama, OUZP zahtijeva izdavanje eksplicitnih upozorenja o privatnosti u kojima se navodi svrha obrade osobnih podataka, trajanje njihove obrade i zadržavanja i organizacije, subjekti odnosno strane kojima će se podaci prenositi odnosno otkrivati. Ako se podaci dobivaju izravno od pojedinca, potrebno ga je u tom trenutku obavijestiti o obradi podataka, a takva obavijest se treba i dostaviti u razumnom vremenskom roku ako su informacije dobivene iz drugih izvora, izuzimajući zakonske iznimke kada je obavijest neizvediva, zahtijeva pretjeran napor ili bi značajno ometala svrhu – objektivno novinarsko odnosno medijsko izvještavanje o temi od javnog interesa.

Za osobe koje provjeravaju činjenice, ovo se načelo može ublažiti novinarskim izuzećem dopuštajući određenu povjerljivost u istragama, iako zahtjev transparentnosti i dalje zagovara maksimalnu otvorenost s publikom i ispitanicima, u skladu s novinarskom etikom odgovornosti.

2.2. Načelo ograničenja svrhe

Načelo ograničenja svrhe kaže da bi se podaci trebali obrađivati u određenu izričitu i legitimnu svrhu, i ne bi se trebali dalje obrađivati na način koji ne bi bio sukladan takvim svrhama.

Kako *fact-checkeri* u pravilu obrađuju osobne podatke poput javnih dokumenata, izjava, tvrdnji ili istražuju informacije povezane s izvorom tvrdnji u svrhu potvrde javno iznesenih podataka i informiranja javnosti, tada oni odnosno njihove organizacije ne bi smjeli koristiti osobne podatke u neke druge svrhe koje nisu povezane s prirodom njihovih aktivnosti. Primjerice, NGO koji obavlja poslove *fact-checkera* i prikuplja osobne podatke određenog ispitanika u svrhu ispitivanja točnosti iznesenih tvrdnji ne bi smio tako prikupljene podatke koristiti u svrhu marketinga, zatim s provjerom tvrdnji nepovezanog istraživanja bez dodatne pravne osnove, primjerice privole ispitanika.

Ukoliko bi se pokazala potreba za nekom novom upotrebom podataka, ispitanika bi se o takvoj upotrebi, u slučaju postojanja primjenjive pravne osnove, trebalo unaprijed obavijestiti.

2.3. Načelo smanjenja količine podataka (minimizacije)

Načelo smanjenja količine podataka zahtjeva od voditelja obrade da treba prikupljati i koristiti samo osobne podatke koji su bitni za navedeni novinarski cilj. Kriterij prikupljanja samo nužnih podataka bitan je u novinarstvu iz etičkih ali i iz pravnih razloga. *Fact-checkeri* bi trebali razmotriti npr. je li potrebno identificirati privatnu osobu u svom izvješću ili bi opis bio prikladan, je li moguće potvrditi zahtjev s manje invazivnim podacima.

Na primjer, ako razotkrivate lažnu glasinu koja je nastala na malom osobnom blogu, možda neće biti potrebno razotkriti puni identitet blogera – fokus može biti na ispravljanju sadržaja odnosno netočne informacije. Pridržavanje načela minimizacije podataka također znači sigurno brisanje osobnih podataka nakon što više nisu potrebni za provjeru činjenica ili daljnje radnje.

2.4. Načelo točnosti

Prema Općoj uredbi o zaštiti podataka (OUZP), voditelji obrade dužni su osigurati da osobni podaci budu točni i, ako je potrebno, ažurirani. Za novinare i osobe koje provjeravaju činjenice, točnost je profesionalni, kao i zakonski standard i zahtjev. Svi osobni podaci koje objavljuju (imena, citati, atribucije itd.) trebaju biti točni i ne smiju dovoditi u zabludu.

2.5. Ograničenje pohrane

Osobni podaci trebaju se čuvati u obliku koji može identificirati ispitanika samo onoliko dugo koliko je potrebno za prikupljene svrhe.

Za *fact-checkere*, to znači da ne bi trebali zadržavati neobrađene podatke ili dokumente koji sadrže osobne podatke na neodređeno vrijeme "za svaki slučaj", posebno ako nisu relevantni za budući rad.

U praksi, novinarski arhivi (objavljeni sadržaji) mogu se držati online neograničeno dugo zbog svoje vrijednosti kao povijesni zapis s obzirom na to da Opća uredba prepoznaje arhiviranje u javnom interesu kao zakonom dozvoljeno ograničenje prava na zaštitu osobnih podataka.

Ipak, popratni materijali (bilješke, popisi kontakata itd.) koji sadrže osobne podatke možda se neće trebati čuvati nakon što je dovršen novinski prilog. Izrazito je važno definirati razdoblja zadržavanja koja odgovarajuće važu s jedne strane medijske odnosno uredničke zahtjeve i potrebe i s druge strane pravo ispitanika na privatnost.

2.6. Cjelovitost i povjerljivost

Voditelji obrade dužni su odabrati, sukladno percipiranim rizicima od povrede osobnih podataka, odgovarajuće sigurnosne tehničke ili organizacijske mjere. Takve mjere potrebne su kako bi se zaštitilo osobne podatke od neovlaštenog pristupa, izmjene ili gubitka.

Provjera činjenica često uključuje osjetljive informacije – od komunikacije zviždača do osjetljivih osobnih navoda – kojima je potrebna snažna zaštita. Novinari imaju ustaljenu praksu snažne zaštite svojih izvora (u digitalnom kontekstu to bi značili i npr. korištenje sigurnih komunikacijskih alata i drugih metoda koje olakšavaju zaštitu identiteta). Usklađenost ovdje znači korištenje jakih kontrola pristupa svim bazama osobnih podataka, šifriranje datoteka ili komunikacije kada je to prikladno i obuku članova tima novinske ili *fact-checking* organizacije o povjerljivosti.

Povreda osobnih podataka ne samo da riskira štetu pojedincima (i ugledu medija), već prema OUZP također može dovesti do odgovornosti organizacije izuzev ako je upotreba osobnih podataka nužna u svrhu koja je prepoznata kao neko od ograničenja prava na zaštitu osobnih podataka. Na primjer, ako osoba koja provjerava činjenice sastavi proračunsku tablicu tvrdnji i izvora koja uključuje osobne podatke, ta bi datoteka trebala biti zaštićena lozinkom i dijeliti je unutar svog suradničkog tima samo ako je za aktivnost organizacije potrebno podijeliti te podatke.

2.7. Pouzdanost (odgovornosti)

Načelo pouzdanosti znači da organizacije trebaju biti u stanju dokazati usklađenost sa svim gore navedenim načelima. U praksi bi čak i male nevladine organizacije koje provjeravaju činjenice trebale dokumentirati svoje postupke zaštite podataka i donošenje odluka u mjeri u kojoj je to proporcionalno rizicima od povrede osobnih podataka.

Naravno, veće medijske organizacije (ili one koje se bave obradama višeg rizika) imati će formalnije ustrojene organizacijske odjele i dodijeljene odgovornosti za usklađenost –uključujući poziciju službenika za zaštitu podataka (DPO) ako su za to ispunjeni kriteriji za obvezu imenovanja prema čl. 37 OUZP.

Iako mnoge svakodnevne novinarske aktivnosti predstavljaju nizak rizik, određene istrage (npr. one koje uključuju tajni nadzor ili velike skupove osobnih podataka) mogu zahtijevati procjenu učinka na zaštitu podataka (DPIA) za procjenu i ublažavanje rizika.

3. Primjenjive pravne osnove za obradu podataka u medijskom izvještavanju i *fact-checkingu*

Temeljem navedenih načela, osobito načela zakonitosti, Opća uredbe o zaštiti podataka zahtijeva da svaka obrada osobnih podataka ima zakonsku osnovu prema članku 6. Uredbe. Za obradu u vezi s novinarstvom najčešće su pri-

mjenjive dvije osnove – legitimni interes voditelja obrade i javni interes.

Fact-checkeri se često mogu pouzdati u svoj legitimni interes traženja istinitih informacija i informiranja javnosti, u odnosu na prava pojedinca. Ova osnova zahtijeva test ravnoteže odnosno test legitimnog interesa. S obzirom na veliki javni interes, osobito za istraživačko novinarstvo, balans se često naginje u korist obrade, posebno za informacije o političarima i drugim javnim osobama ili pitanjima od javnog značaja. OUZP u uvodnoj izjavi 47 navodi da obrada osobnih podataka koja je striktno neophodna za slobodu izražavanja može predstavljati legitiman interes. Međutim, legitimni interes je neprimjenjiv ako ga nadjačaju interesi nositelja podataka (npr. objavljivanje osobnih podataka koji su vrlo osjetljivi i sumnjive vrijednosti za javni interes moglo bi pasti na testu legitimnog interesa).

U nekim slučajevima, novinarstvo javnih medijskih organizacija ili subjekata koje financira država može se smatrati zadatkom koji se obavlja u javnom interesu. Čak i privatni *fact-checkeri* mogu se pozvati na "javni interes" ako nacionalni zakon izričito priznaje novinarstvo kao zadatak od javnog interesa. Neke države članice Unije zakonski su izričito prepoznale novinarstvo kao aktivnost čije obrade predstavljaju obrade od javnog interesa. U praksi, međutim, većina neovisnih nevladinih organizacija koristi se legitimnim interesom kao zakonskom osnovom za obradu osobnih podataka, budući da nisu tijela javne vlasti.

Što se mogućnosti korištenja privole kao pravne osnove tiče, novinari obično ne mogu ili ne traže privolu od osoba o kojima pišu, osobito u istraživačkom kontekstu. OUZP detaljno uređuje pravila pod kojim se traži i bilježi privola, a javna osoba realno ne može odbiti pristanak za provjeru činjenica o svojoj javnoj izjavi. Stoga je privola obično rezervirana za aktivnosti kao što je intervjuiranje privatne osobe za priču (uz suglasnost za korištenje njezinih podataka u toj priči) ili za upravljanje listama slanja obavijesti pretplatnicima i sličnim obradama, a ne za osnovno prikupljanje vijesti.

Preostaje osvrnuti se na okolnosti obrade tzv. posebnih kategorija osobnih podataka uređenih čl. 9 OUZP. Ako su osobni podaci koji se obrađuju neki od podataka iz posebnih kategorija (osjetljivi osobni podaci kao što su zdravstveni podaci, politička ili vjerska uvjerenja itd.) i kao takvi uključeni u provjeru činjenica, potreban je dodatni uvjet kako bi se zaobišla načelna zabrana obrade takvih podataka koje je uređena prema članku 9 OUZP. Članak 9. stavak 2. točka g. Uredbe dopušta obradu takvih podataka ako je to "potrebno zbog značajnog javnog interesa, na temelju prava Unije ili države članice" - a mnoge države članice deklariraju novinarstvo kao značajan javni interes. Štoviše, članak 9. stavak 2. točka e. dopušta korištenje osobnih podataka koje je pojedinac očigledno sam javno objavio. Mnoge provjere činjenica uključuju tvrdnje koje su pojedinci javno iznijeli npr. javna izjava političara o njihovom zdravlju ili vjeri može se ponoviti bez povrede Uredbe jer je osoba sama objavila tu informaciju.

Nacionalni propisi ponekad izričito dopuštaju novinarima da obrađuju osjetljive podatke kada su potrebni za izvještavanje, podložno odgovarajućim zaštitnim mjerama. Tako primjerice britanski zakon predviđa da novinari mogu rukovati osjetljivim osobnim podacima za potrebe novinarstva ukoliko vjeruju da je objavljivanje u javnom interesu. Italija, na sličan način, putem svog kodeksa ponašanja novinara dopušta obradu osjetljivih podataka u izvještavanju pod uvjetom da zadovoljavaju testove bitnosti i javnog interesa.

Fact-checkeri bi stoga trebali biti svjesni svojih nacionalnih odredbi, ali općenito se mogu osloniti na iznimke od javnog interesa za osjetljive podatke – na primjer, razotkrivanje lažne tvrdnje o zdravstvenom stanju osobe bilo bi dopušteno ako je relevantno za javni diskurs, iako kod zdravstvenih podataka obično preteže interesi ispitanika nad javnim interesom.

Načela zaštite osobnih podataka sadržana u čl. 5 Opće uredbe, kao i pravne osnove iz čl. 6 kao ostvarenje načela zakonitosti predstavljaju zakonski okvir za odgovornu upotrebu osobnih podataka. Novinari i *fact-checkeri* slobodni su prikupiti ono što im je potrebno za navedenu novinarsku svrhu pod uvjetom da tako osobne podatke čuvaju na sigurnom, jamče njihovu povjerljivost i točnost te ih zadržavaju ne dulje nego što je potrebno.

4. Rukovanje i upotreba osobnih podataka prilikom *fact-checking* provjera

Fact-checkeri se rutinski bave osobnim podacima, bilo da se radi o identitetu javne osobe koja iznosi tvrdnju, pojedinostima o ljudima koji se spominju u priči ili informacijama prikupljenim od pojedinaca kako bi potvrdili činjenicu.

Primjeri upotrebe osobnih podataka mogu uključivati i imena i profile korisnika društvenih medija koji su pokrenuli viralne glasine, kontakt informacije i izjave stručnjaka ili očevidaca koji komentiraju nečije navode, biografske podatke o obrazovanju, financijama ili drugim okolnostima od značaja za život politički istaknute javne osobe ili eventualno osjetljive podatke poput nečijeg zdravstvenog stanja ili kaznenog dosjea ako su relevantni za tvrdnju koja se ispituje.

Naravno, i multimedijski sadržaji kao što su fotografije ili videosnimke mogu predstavljati osobne podatke ako se pojedinci mogu identificirati. Stoga osobe koje provjeravaju činjenice moraju većinu svog istraživačkog materijala tretirati kao osobne podatke čija je upotreba regulirana Općom uredbom o zaštiti podataka i drugim primjenjivim propisima.

4.1. Pošteno i zakonito prikupljanje podataka

Prilikom prikupljanja podataka, *fact-checkeri* koji provjeravaju medijske navode trebaju uzeti u obzir metodu prikupljanja podataka i njihov izvor. Ako podaci dolaze izravno od osobe (na primjer, traženje komentara ili dokaza od nekoga), ta osoba općenito može pretpostaviti da će novinari ili *fact-checkeri* njezine podatke koristiti u okviru prikaza aktivnosti o provjeri točnosti informacija, što u određenoj mjeri zadovoljava zahtjeve transparentnosti odnosno informiranja ispitanika o obradi podataka.

Ako se podaci prikupljaju neizravno – recimo putem online pretraživanja, baza podataka ili drugih izvora, a ne direktno od ispitanika – standardi Opće uredbe zahtijevaju informiranje ispitanika prema odredbama čl. 14. OUZP. Međutim, kao što je navedeno, novinarstvo se može pozvati na iznimke od zahtjeva informiranja ako je informiranje subjekta neizvedivo ili bi ugrozilo javni interes odnosno novinarsku istragu. Tako naprimjer, ako se istražuje potencijalno lažnu tvrdnju o nekom državnom dužnosniku ili direktoru velike tvrtke koja kotira na burzi, unaprijed upozoriti osobu koja je predmet istrage da se prikupljaju podaci o njemu moglo bi ugroziti istragu ili dovesti do pritiska na izvore. Novinarsko izuzeće od zaštite osobnih podataka dopušta uskraćivanje obavijesti u sličnim situacijama, uz naravno pošteno i objektivno razmatranje situacija u kojima bi se novinari ili *fact-checkeri* mogli pozvati na tu vrstu zaštite.

Legitimni interes osobe / organizacije koja provjerava činjenice vezane uz osobne podatke često služi kao primarna pravna osnova za obradu podataka. To obuhvaća aktivnosti poput pretraživanja javnih zapisa o osobi ili spremanja kopije sumnjive objave na društvenoj mreži za analizu. Legitimni interes je u biti interes tiska i javnosti da se otkrije istina – težak posao u suvremenim demokratskim društvima. U balansiranju s privatnošću pojedinca, kontekst je presudan - javne osobe imaju smanjena očekivanja privatnosti u pogledu svojih javnih izjava, tako da oni koji provjeravaju činjenice mogu slobodnije koristiti i preispitivati njihove podatke (kao što je citiranje i pomno ispitivanje riječi političara).

Pojedinci koji nisu javne osobe, privatne osobe, imaju veća očekivanja u pogledu zaštite osobnih podataka odnosno privatnosti. Ako su i njihovi podaci predmet interesa novinara ili *fact-checkera*, osobe koje provjeravaju činjenice mogu pokušati anonimizirati ili minimizirati identifikacijske detalje kako bi smanjile štetu za prava i slobode pojedinaca. Na primjer, ako se širi lažna tvrdnja koja uključuje privatnog građanina (recimo pogrešno pripisan citat ili osobna anegdota koja je postala viralna), osoba koja provjerava činjenice može ispraviti neistinu bez otkrivanja potpunog identiteta ili osobnog života osobe, osim ako je taj detalj ključan za razotkrivanje tvrdnje. Ovaj pristup usklađen je s načelom zakonitosti, poštenosti i transparentnosti i pomaže u zadovoljavanju "nužnog" segmenta testa legitimnog interesa - koristite samo onoliko osobnih podataka koliko je potrebno da biste rekli istinu.

U slučajevima kada je pristanak prikladan, osoba koja provjerava činjenice treba ga jasno pribaviti i dokumentirati. To se može primijeniti kada se radi o nejavnoj osobi koja dobrovoljno daje informacije za provjeru činjenica (npr. pojedinac se javi kako bi ispravio lažne glasine o sebi – mogao bi pristati da bude citiran u članku). Privola prema Općoj uredbi o zaštiti podataka treba biti jasna, nedvosmislena, granularna, konkretna i informirana, tako da bi osoba trebala razumjeti da će biti citirana ili da će se njezini podaci koristiti u objavljenoj provjeri činjenica. Međutim, kao što je navedeno, privola je rijetko glavno uporište za novinarsku obradu zbog mogućnosti odbijanja ili povlačenja privole i posljedica koje to može imati za takve aktivnosti.

Dobra praksa provjere činjenica uključuje i minimizaciju podataka. *Fact-checkeri* trebaju biti usredotočeni na dokaze relevantne za tvrdnju koju ispituju, a ne na prikupljanje, obradu i zadržavanje nepotrebnih osobnih podataka. Time što obrađuju samo nužne podatke, smanjuju i rizik od potencijalne povrede osobnih podataka. Pretpostavimo da je za provjeru tvrdnje o obrazovanju javnog dužnosnika potrebno potvrditi koje diplome posjeduje. Osoba koja provjerava činjenice može dobiti kopiju životopisa dužnosnika ili evidenciju bivših studenata. Taj bi dokument slučajno mogao sadržavati dodatne osobne podatke (kućnu adresu, datum rođenja itd.). Minimiziranje podataka znači da osoba koja provjerava činjenice treba izdvojiti samo potrebne informacije (diploma i ustanova) i izbjegavati obradu, prenošenje, otkrivanje ili drugo objavljivanje ostalih podataka u svom posjedu.

Ako dokument ili skup podataka sadrži osjetljive osobne podatke (npr. zdravstvene dijagnoze, sindikalno članstvo, vjerska ili politička mišljenja), osoba koja provjerava činjenice treba još jednom provjeriti je li njihova upotreba neophodna i zakonski dopuštena. Mnoge lažne tvrdnje u javnoj sferi zadiru u osjetljiva područja (npr. dezinformacije o zdravstvenom stanju osobe ili vjerskoj pripadnosti). Novinari mogu obrađivati takve podatke ako su relevantni za ispravljanje neistine u javnom interesu, ali trebaju biti posebno oprezni. Nacionalne novinarske smjernice često savjetuju suzdržavanje od isticanja osjetljivih aspekata nečijeg života osim ako nisu izravno relevantni za javni interes priče.

Nadalje, ključni aspekt rukovanja osobnim podacima novinara je zaštita novinarskih izvora – osoba koje novinarima dojavljuju relevantne informacije. Ako privatna osoba pruži informacije za razotkrivanje lažne tvrdnje (primjerice, insajder koji zna istinu iza lažne izjave), osoba koja provjerava činjenice ima profesionalnu dužnost čuvati tajnost identiteta tog izvora ako bi to netko od nje to zatražio.

Šire gledano, sigurno rukovanje znači korištenje šifrirane (kriptirane) komunikacije ili usluga sigurnog prijenosa za osjetljive podatke (kako bi se spriječilo presretanje osobnih podataka) i pohranjivanje bilješki ili izvornih kontakt informacija u sigurnim sustavima.[7]

[7] Tako primjerice i često spominjani kodeks britanskog ICO nanovo ističe važnost sigurnosnih mjera – organizacije koje se bave novinarskim aktivnostima trebaju provoditi tehničke i organizacijske mjere kao i svi drugi voditelji obrade.

4.2. Osiguranje točnosti i odgovornosti (pouzdanosti) u javno objavljenim provjerama podataka

Za *fact-checkere* točnost podataka je profesionalni imperativ, suština njihovog poziva, no točnost podataka je i pravni zahtjev prema propisima o zaštiti osobnih podataka. U novinarskoj etici, objavljivanje netočnih informacija je propust koji šteti vjerodostojnosti no prema odredbama Opće uredbe o zaštiti podataka, objavljivanje netočnih osobnih podataka može povrijediti prava ispitanika. Ponekad su ti ciljevi usporedni i ispunjenje jednog vodi prema ispunjenu drugog – temeljitost i pažljivost u postupku provjere činjenica dovodi do ispravka netočnosti koje se objavljuju o pojedincima, no ishod ne treba uvijek biti takav. U praksi se može dogoditi da se nove informacije pojave tijekom vremena, nove činjenice koje se mogu pojaviti nakon objave, ispitanik tj. osoba koja je predmet navoda o kojima se piše u novinskom tekstu može osporiti zaključke. U okviru svoji aktivnosti novinari i *fact-checkeri* konzultiraju brojne izvore i prolaze različite kontrole kvalitete sadržaja prije objave. U većim novinskim organizacijama više razina uredništva kontrolira točnost, objektivnost i poštenje sadržaja prije objave, što pozitivno utječe na smanjenje šanse za povredu osobnih podataka.

Prema načelu točnosti iz čl. 5. OUZP, voditelj obrade treba poduzeti razumne korake kako bi se osigurala točnost podataka. U kontekstu novinarstva, razumni koraci bili bi provjera identiteta, imena osoba o kojima se piše, provjeravanje ispravnosti navoda kroz snimke ili transkripte intervjua, provjere navoda iz dokumenata kroz druge izvore i davanje mogućnosti osobi o kojoj se piše. Čak i kad je riječ o prilozima nižeg profila, relativno uobičajenim, svakodnevnim vijestima, novinari i *fact-checkeri* trebaju moći dokazati što su i kako su djelovali da prepoznaju i smanje rizike od povrede, bilo kroz vođenje bilješki o tome kako su činjenice provjeravane do postupaka koji dokazuju integritet i odgovorno uređivanje priloga, što je presudno u slučaju da se njihov integritet naknadno dovede u pitanje.

Ponekad će se, unatoč svim naporima, ipak dogoditi greške, bilo da je ime ili titula osobe krivo navedena, ili se neki citat pripisuje pogrešnoj osobi, ili isplivaju nove okolnosti, činjenice, dokazi nakon objave koji mijenjaju zaključak. Suvremeni propisi iz područja zaštite osobnih podataka bez rezerve uređuju da pojedinci imaju pravo na ispravak netočnih osobnih podataka. Tako i OUZP u čl. 16 uređuje pravo na ispravak ili pravo na brisanje podataka. Analognu ulogu u novinarstvu imaju "ispravci", pa će svi nakladnici, ali i *fact-checkeri* i mediji imati politiku ispravljanja netočnih navoda, a neki će biti i potpisnici kodeksa Međunarodne mreže za provjeru činjenica koji zahtijeva brzo ispravljanje pogrešaka.[8] Sa stajališta zaštite podataka, ako netko spomenut u provjeri činjenica kontaktira organizaciju kako bi ukazao na netočnost o sebi, voditelj obrade dužan je odgovoriti i, ako je tvrdnja potvrđena, učiniti odgovarajuće ispravke. Treba napomenuti, *fact-checkeri* nisu dužni ispravljati prošlost – ako je podatak bio ispravan u vrijeme objave, tada ne postoji obveza ispravljanja starog sadržaja odnosno ponovnog popravljanja starih objavljenih materijala kako se podaci mijenjaju u realnom vremenu – primjerice svaki put kad netko promijeni posao, obrazovanjem stekne novu titulu ili bude imenovan na novu dužnost – *fact-checkeri* imaju obvezu provjere podatka u kontekstu i vremenu objave.

Nadalje, *fact-checking* često služi očuvanju društvenih povijesnih zapisa o temama od javnog interesa. Uklanjanje ili izmjena takvih zapisa može otežati ispunjenje te svrhe što je protivno vrlo snažnom javnom interesu da se zapisi o izvještavanju i novostima zadrže u in-

[8] IFCN Code of Principles, dostupan na stranicama IFCN https://ifcncodeofprinciples.poynter.org. Kodeks načela namijenjen je organizacijama koje redovito objavljuju izvješća o točnosti izjava javnih osoba, javnih institucija i drugih tvrdnji od interesa za društvo. Kodeks je rezultat konzultacija među fact-checkerima iz cijelog svijeta i nudi načela kojima trebaju težiti u svom svakodnevnom radu.

tegralnom obliku kako bi društvo imalo pristup podacima o prošlim događajima – primjerice, javne osobe, osobito dužnosnici i političari mogu promijeniti (i često mijenjanju) mišljenje, pa bi zapisi trebali reflektirati takve promjene – osiguranje točnosti u tom kontekstu je usmjereno na ispravljanje grešaka, a ne na uklanjanje informacija odnosno podataka koji su u prošlosti bili točni.

Kako osigurati višu razinu točnosti i kvalitete provjere podataka?

Fact-checking organizacije mogu povisiti stupanj točnosti podataka uvođenjem kontrola kvalitete koje također služe ispunjavanju načela odgovornosti. Na primjer, mnogi mediji koriste pristup recenzije podataka - jedan istraživač sastavlja nacrt provjere činjenica, dok drugi pregledava izvore i zaključke te bilježi nalaze. Ovo ne samo da poboljšava točnost, već također stvara interni zapis razmatranja koji, ako kasnije dođe do spora (npr. pokretanje sudskog postupka ili drugi pravni rizici), organizacija može pokazati da je poduzela odgovorne korake. Dokumentiranje donošenja odluka (čak i samo kroz e-mail trag komunikacije ili bilješkama za uređivanje) odražava načelo odgovornosti prema čl. 5. st. 2. OUZP – mogućnost dokazivanja kako je ispunjena dužnost poštenog i točnog izvještavanja.

Mehanizmi vanjske odgovornosti također pozitivno utječu na postignutu razinu kvalitete provjerenih činjenica. Oni koji provjeravaju činjenice često objavljuju svoju metodologiju i daju izvore za svaku tvrdnju. Neki imaju praksu uključivanja stručnjaka za određeno područje u pregled sadržaja, učinkovito dodajući dodatni sloj provjere. Osim toga, davanje subjektima prava na odgovor pridonosi točnosti: ako se političar ili javna osoba ne slaže s provjerom činjenica, mogu pružiti protudokaze ili kontekst. Iako to ne obvezuje osobu koja provjerava činjenice da promijeni svoju odluku, osigurava da su sve perspektive uzete u obzir, a ako subjekt iznese valjanu točku, to može dovesti do ispravka ili pojašnjenja prije objave.

Da zaključimo, osiguranje točnosti provjerenih činjenica nije moment, već kontinuirani proces – od provjere prije objavljivanja do ispravaka nakon objavljivanja. Zahtjevi propisa za zaštitu osobnih podataka, primarno načela točnosti, za korištenje točnih podataka u skladu je s novinarskom etikom, a osobe koje provjeravaju činjenice općenito su primjeri u ovom području zbog prirode svog posla. Održavanjem rigoroznih standarda i reagiranjem na legitimne pritužbe, osobe za provjeru činjenica ne samo da se pridržavaju zakona o zaštiti podataka (izbjegavajući potrebu za formalnim nalozima za ispravak), već i jačaju svoju vjerodostojnost i pouzdanost.

5. Zaključak

Iskustva europskih *fact-checking* organizacija pokazuju da Opća uredba o zaštiti podataka zapravo nije prepreka nego koristan okvir koji se prirodno naslanja na etička načela novinarstva.

Kada se načela poštenja, točnosti, podatkovne minimizacije i minimalne intruzivnosti shvate kao produžetak profesionalne odgovornosti, *fact-checkeri* mogu u najvećoj mjeri uskladiti svoju misiju s pravnim zahtjevima zaštite podataka. Komparativna europska praksa u zemljama poput Španjolske, Francuske i Italije vidljivo ukazuje da urednička transparentnost i stalno unapređivanje rada omogućuju brzo i učinkovito uvođenje pravila za zaštitu osobnih podataka bez gubitka vjerodostojnosti ili brzine.

Najveću fleksibilnost donosi „novinarski izuzetak“ iz članka 85. Opće uredbe, koji dopušta odstupanje od pojedinih obveza poput poštivanja nekih aspekata načela zaštite podataka, prava ispitanika, obveza voditelja obrade, obveza prilikom izvoza podataka i drugih Uredbom propisanih obveza kad je to nužno za javni interes. Ključ je, međutim, ovo ograničenje u korist novinarske aktivnosti odnosno prava na slobodu izražavanja i informiranja koristiti selektivno i uz temeljitu argumentaciju - svrha obrade treba

biti novinarska, namjera objave jasna, a javni interes pretežan. Bilježenje takvih odluka stvara obrambeni mehanizam ako uredničke poteze naknadno preispituju nadzorna tijela ili sudovi.

Treba stoga zaključiti kako preciznost i korektnost sadržaja ostaju najbolja preventiva za sukobe oko brisanja ili ispravka podataka. Ako su činjenice provjerene i osobe uključene u priču dobivaju priliku za komentar, prigovori su rijetki i lakše se odbijaju. Kad se ipak pojave, europska praksa naglašava očuvanje arhiva kao povijesnog zapisa, pod uvjetom da su zapisi točni. Takav pristup čuva integritet informacijskog prostora, ali u određenim slučajevima zahtijeva i preispitivanje starijih članaka ako se okolnosti promijene – primjerice, ako je netko neopravdano označen kao izvor dezinformacija i poslije oslobođen krivnje.

Odgovorno balansiranje između privatnosti i javnog interesa stoga počiva na situacijskom prosuđivanju - moćne javne osobe i teme od očite društvene važnosti traže maksimalnu otvorenost, dok osjetljivi osobni podaci anonimnih građana zaslužuju najvišu razinu zaštite. Kako bi takvo prosuđivanje bilo dosljedno, organizacije svih veličina, uključujući i male nevladine organizacije trebaju razviti kulturu privatnosti i zaštite osobnih podataka – makar kroz jednostavan obrazac pitanja pri svakom novom istraživanju i imenovanje osobe koja će pratiti upite o podacima. Vanjski vodiči, akademske studije i sudski presedani stoje im na raspolaganju kao praktični kompas.

Da zaključimo - europski model uređenja *fact-checkinga* pokazuje da zaštita podataka i sloboda medija nisu suprotstavljeni, nego upravo suprotno, dosljedno provođeni imaju međusobno osnažujući utjecaj. Suzbijanje dezinformacija često uključuje ispravljanje lažnih osobnih podataka, dok obveze koje proizlaze iz Opće uredbe potiču urednike da procijene nužnost i razmjernost korištenja podataka, čime se izbjegavaju nepotrebni prodori u osobni prostor i podatke ispitanika koji bi mogli narušiti ugled medija.

Odredbe o ograničenju odgovornosti novinskih organizacija djeluju kao vrsta sigurnosnog ventila koji jamči da sloboda izražavanja neće biti potisnuta birokratskim zahtjevima, ali i postavlja očekivanje odgovorne upotrebe te slobode. Takav uravnotežen pristup omogućuje *fact-checkerima* da i dalje budu „čuvari javnosti“ u digitalnom dobu, osiguravajući rigorozno i na činjenicama utemeljeno izvještavanje uz poštivanje privatnosti i dostojanstva pojedinaca.

Zaštita autorskog i srodnih prava u kontekstu borbe protiv dezinformacija

Prof.dr.sc. Romana Matanovac Vučković
Pravni fakultet Sveučilišta u Zagrebu

1. Uvod

Borba protiv dezinformacija postala je ključan izazov u digitalnom dobu. Novinari, urednici, medijski nakladnici i regulatori u području medija suočavaju se s potrebom da ispravljaju netočne informacije, a istovremeno moraju paziti na prava trećih osoba. Jedan od bitnih pravnih aspekata pritom je poštivanje autorskog i srodnih prava. Čak i *fake news* – lažne ili manipulirane informacije – mogu biti zaštićene autorskim pravom ako ispunjavaju uvjete originalnosti i individualnosti izraza. Primjerice, autorsko pravo može štititi članak koji širi dezinformaciju, digitalno izmijenjenu fotografiju ili video koji sadrži lažan prikaz. Zbog toga stručnjaci postavljaju pitanje, može li se autorskopravna zaštita takvih štetnih sadržaja ograničiti u javnom interesu? U praksi, međutim, autorsko pravo redovno obuhvaća i takve sadržaje, pa ih se prilikom provjere činjenica - *fact-checkinga* i objave ispravaka mora koristiti oprezno i zakonito. Pored autorskog postoji i niz zakonom definiranih i uređenih srodnih prava. Ona su po svojoj naravi slična autorskom, ali imaju različite subjekte i objekte prava, pa i o njima valja voditi računa kod *fact-checkinga*. U medijima su zanimljiva prava organizacija za emitiranje u pogledu njihova signala, prava filmskih producenata u pogledu videograma i prava novinskih nakladnika u pogledu medijskih tiskanih i elektroničkih publikacija. Sve navedeno stvara složen ekosustav autorskih i srodnih prava kojeg treba uklopiti u sustav provjere činjenica.

Ovaj tekst ima za cilj objasniti pravni okvir koji uređuje provjeru informacija i objavu ispravaka u medijima, uz zaštitu autorskog i srodnih prava. Slijedi strukturu relevantnog modula: najprije daje pregled zakonodavnog okvira, zatim obrađuje osnove autorskog i srodnih prava, potom ograničenja i iznimke (situacije kada se autorska djela smiju koristiti bez dozvole i / ili bez plaćanja naknade), nastavlja s kolektivnim ostvarivanjem prava te specifičnim slučajevima autorskih djela u radnom odnosu i po narudžbi, a na kraju razmatra nove izazove koje donosi umjetna inteligencija. Ciljana publika – novinari, urednici, medijski nakladnici i novinski nakladnici te odgovorne osobe i zaposlenici u regulatornim tijelima – dobit će sažeta, edukativna i praktično primjenjiva znanja o tome kako postupati prilikom suzbijanja dezinformacija, uz poštivanje autorskih i srodnih prava.

2. Zakonodavni okvir

Zakon o autorskom pravu i srodnim pravima (NN 111/2021, dalje u tekstu ZAPSP). Kroz postupak provjere činjenica često se koristi tuđi sadržaj (npr. citira se sporni članak ili se prikazuje sporni video), zbog čega je važno razumjeti okvir autorskog prava. U Republici Hrvatskoj temeljni propis je Zakon o autorskom pravu i

srodnim pravima, usklađen s pravnom stečevinom EU. Njime su implementirane, među ostalim, i odredbe Direktive (EU) 2019/790 (tzv. DSM Direktiva) o autorskom pravu na jedinstvenom digitalnom tržištu, koja donosi novine poput novog srodnog prava novinskih nakladnika (o čemu će biti riječi kasnije). Implementirana je i Direktiva 2019/789 (tzv. SatCab 2 Direktiva) koja uređuje prava organizacija za emitiranje u pogledu njihove zaštite kod reemitiranja koje provode operatori reemitiranja (IPTV, DTH i slične tehnologije) kao i kod tzv. pratećih internetskih usluga kao što su TV portali na internetu koji prate redovito emitiranje zemaljskim ili satelitskim signalom.

ZAPSP je sustavan i cjelovit zakon koji propisuje sve u vezi s autorskim i srodnim pravima - što su autorska djela, koji su predmeti srodnih prava, koji sadržaj prava imaju autori i nositelji srodnih prava, koja su ograničenja tih prava – sadržajne i vremenske naravi. Također, uređuje i sustav kolektivnog ostvarivanja prava, autorsko ugovorno pravo, a posebno regulira odnose kad je djelo stvoreno u radnom odnosu ili po narudžbi. Svi ovi segmenti relevantni su za rad medijskih djelatnika.

Europski i međunarodni kontekst. Pored europskih, hrvatsko zakonodavstvo primjenjuje i međunarodne standarde: primjerice, Bernska konvencija postavlja temelje zaštite autorskih djela u cijelome svijetu budući da ima 181 državu potpisnicu. S druge strane, hrvatski ZAPSP usklađen je i s nizom drugih EU direktiva, od koji je za suvremeni kontekst možda najzanimljivija Direktiva 2001/29/EZ (nazivaju ju i InfoSoc Direktivom ili jednostavno Copyright Direktivom).

U području dezinformacija, pravni okvir obuhvaća i nove EU propise poput Akta o digitalnim uslugama (DSA) koji nameće vrlo velikim online platformama obvezu procjene i suzbijanja sistemskih rizika dezinformacija. Iako DSA primarno regulira odgovornost posrednika na internetu, vrijedi spomenuti da se pravila o moderiranju sadržaja i suradnji s provjeravateljima činjenica razvijaju na razini EU te utječu na način širenja (ili suzbijanja) dezinformacija. No, ključna pravna načela zaštite autorskog i srodnih prava ostaju nepromijenjena: čak i u borbi protiv lažnih vijesti, pojedinci, mediji i platforme moraju paziti da ne prekrše nečija autorska ili srodna prava. Naime, autorsko pravo je estetski, umjetnički, činjenično neutralno. Za autorskopravnu zaštitu potrebno je zadovoljiti kriterij originalnosti ili individualnost, a ne kriterij istinitosti ili točnosti. Isto vrijedi i za srodna prava.

U nastavku ovoga teksta detaljnije se objašnjavaju opisana načela zaštite autorskog i srodnih prava, s ciljem da novinari i urednici te provjeravatelji točnosti – *fact-checkeri* razumiju što smiju, a što ne smiju činiti s tuđim sadržajem dok razotkrivaju neistine.

3. Temeljni pojmovi autorskog i srodnih prava

Autorsko djelo. Autorsko pravo štiti autorska djela – originalne intelektualne tvorevine iz književnog, znanstvenog ili umjetničkog područja, koje su jedinstven rezultat kreativnosti svog stvaratelja. Među autorska djela pripadaju, primjerice, pisani članci, govorna izlaganja, novinarski tekstovi, fotografije, audiovizualni prilozi i računalni programi, pod uvjetom da su originalni i da imaju individualni karakter. Tu je ključno uočiti i naglasiti da ideje, koncepti, činjenice nisu i ne mogu biti zaštićeni autorskim pravom – zaštita se odnosi samo na konkretan izražaj. Drugim riječima, "ideje nisu zaštićene" (što je često naglašeno načelo) – tek kada autor ideju ostvari u formi (npr. napiše članak, snimi fotografiju), nastaje autorsko djelo i pripadajuća zaštita. Također, obična vijest, kao obična činjenica također ne može biti zaštićena autorskim pravom.

Autor. Autorsko pravo po svojoj naravi pripada fizičkoj osobi koja stvori autorsko djelo. Autor je izvorni nositelj autorskog prava, dočim drugi mogu steći prava korištenja na temelju ugovora ili nekog drugog pravnog posla *inter vivos* ili *mortis causa*. Jedini način prenošenja cijelog

autorskog prava događa se na temelju nasljeđivanja, kad autorsko pravo kao cjelina prelazi na nasljednike. Dakle, umjesto i osim fizičke osobe koja je djelo stvorila – nitko drugi ne može biti autor. Druge osobe mogu steći prava iskorištavanja autorskog djela ali se ne mogu smatrati autorima – ni poslodavci, ni naručitelji ni itko drugi. Nasljednici također nisu autori ali stječu nasljeđivanjem cijelo autorsko pravo, onakvo kakvo je pripadalo autoru u trenutku smrti. No, time autor ne prestaje biti autorom naslijeđenog djela.

Autorska moralna prava. Autori uživaju moralna prava. To su, najprije: pravo paterniteta – da budu priznati kao autori, pravo integriteta – zaštita djela od naruženja te pravo na reputaciju – zaštita časti i ugleda autora u kontekstu korištenja djela. Pravo prve objave i pravo opoziva također su moralna prava, ali se ne koriste tako često u svakodnevnoj praksi. Moralnim pravima štite se osobne veze između autora i njegova djela. Moralna prava ne mogu se prenijeti drugim osobama zbog te svoje osobno-pravne naravi, niti se u pogledu moralnih prava mogu za drugog osnovati prava iskorištavanja. S obzirom na to da autorska moralna i autorska imovinska prava čine nedjeljivu i nerazdruživu cjelinu, posljedično autorsko pravo kao cjelina je neprenosivo i kao cjelina traje za života autora i 70 godina nakon njegove smrti.

Autorska imovinska prava. Autor ima također i imovinska isključiva prava, kojima se štite njegovi imovinski interesi u odnosu na djelo. Za razliku od nemogućnosti raspolaganja moralnim pravima, imovinska prava autor može ugovorom ustupiti drugima na način da osnuje prava iskorištavanja – licenciju. Imovinska autorska prava služe prvenstveno komercijalizaciji autorskih djela. Sadržaj imovinskih prava uglavnom je usklađen u cijelome svijetu, a pogotovo u Europskoj uniji. Ta prava uključuju: pravo reproduciranja, pravo distribuiranja, pravo priopćavanja javnosti i pravo prerade.

Pravo umnožavanja (kopiranja) obuhvaća sve načine i oblike umnožavanja djela, u cijelosti, u dijelovima, bilo kojim sredstvima, na bilo kojem mediju, u bilo kojem obliku, neposredno ili posredno.

Pravo distribuiranja podrazumijeva da se original ili kopija djela stavi u promet promjenom vlasništva, što se može dogoditi na temelju kupoprodaje ali i na temelju darovanja. Distribuiraju se, dakle, materijalni primjerci djela.

Pravo priopćavanja javnosti podrazumijeva, s druge strane, korištenje djela u nematerijalnom obliku. Ono obuhvaća, na primjer, javnu izvedbu na koncertu, prikazivanje u kinima, emitiranje i reemitiranje putem televizijskih signala, ali i korištenje na internetu, *streaming* servisima i uslugama na zahtjev (*on-demand*). Priopćavanje javnosti kod kojeg se autorsko djelo čini dostupnim javnosti na način da mu pripadnici javnosti mogu pristupiti s mjesta i u vrijeme koje sami odaberu također je obuhvaćeno isključivim pravom autora. Riječ je o korištenju autorskih djela u internetskim uslugama na zahtjev.

Pravo prerade podrazumijeva bilo kakvu obradu, prijevod, prilagodbu ili drugu preradu ili izmjenu djela.

To da su imovinska prava isključiva znači da se bez autorovog odobrenja (licencije) djelo ne smije koristiti, osim ako je zakonom drukčije propisano, a bit će propisano u obliku zakonskog ograničenja ili iznimke (o čemu će biti riječi u posebnom poglavlju). Za novinare je bitno znati da npr. objavljivanje tuđeg teksta, fotografije ili videopriloga na nekom portalu predstavlja korištenje djela za koje je potrebno prethodno ishoditi dopuštenje i platiti naknadu, osim ako ne postoji neka zakonska iznimka koja to dopušta da se učini bez dopuštenja i / ili bez plaćanja naknade, o čemu više u nastavku.

Ideje vs. izražaj – primjer u praksi: Ako medij želi opovrgnuti lažnu tvrdnju objavljenu u nekom tekstu, smije parafrazirati tu tvrdnju (jer sama činjenica, vijest ili ideja nisu zaštićeni), ali ne i preuzeti čitav tuđi tekst bez dozvole - ako su u pogledu tako objavljenog teksta prava pridržana. O načinu pridržaja prava kasnije,

jer inače postoji iznimka korištenja u svrhu informiranja javnosti. S druge strane, kratki citat tuđeg teksta radi analize ili kritike ili čisto radi citata samog, dopušta se uz određene uvjete To pripada pod iznimke, o čemu također kasnije. Ovo načelo osigurava ravnotežu: istinita informacija od javnog interesa ne smije se "zaključati" autorskim pravom, ali kreativan izraz te informacije pripada autoru.

Srodna prava: zaštita nakladnika, umjetnika izvođača, producenata. Osim autora, i druge kategorije stvaratelja ili investitora u kreativan i kulturan sadržaj imaju prava slična autorskom – takozvana *srodna prava*. Srodna prava štite umjetnike izvođače (npr. glumce, glazbenike za njihove izvedbe), proizvođače fonograma (diskografske kuće u pogledu njihovih snimki), filmske producente (u pogledu videograma tj. snimljenih videosadržaja poput filmova, serija i slično), organizacije za emitiranje (u pogledu signala kojeg emitiraju a koji u sebi nosi autorskim i srodnim pravima zaštićeni sadržaj), ali i – odnedavno – nakladnike novinskih publikacija (izdavače medija) za njihove tiskane i elektroničke publikacije kao cjeline ili u dijelovima, uključujući i male dijelove, osim tzv. *snippeta*.

Srodna prava nastaju, ne zbog originalnosti izraza (kao kod autora), već zbog ulaganja truda, izvedbenog talenta ili financijskih sredstava u stvaranje i/ili diseminiranje sadržaja. Primjerice, televizijska kuća ima srodno pravo na svojem signalu kojeg emitira, i nitko taj signal ne smije reemitirati bez dozvole. Istovremeno, televizijska kuća je i filmski producent u situacijama kad proizvodi vlastite videograme - Nadalje, u medijima je posebno relevantno srodno pravo novinskih nakladnika na izdanjima, bila ona elektronička ili tiskana.

Novo srodno pravo novinskih nakladnika. Ovo pravo uvedeno je DSM Direktivom radi jačanja položaja novinskih nakladnika u digitalnom okružju. Hrvatski ZAPSP ga je implementirao i proširio njegov sadržaj prava u odnosu na minimum. Bit srodnog prava novinskih nakladnika sastoji se u tomu da nakladnici novina i portala imaju isključivo pravo na digitalno umnožavanje i priopćavanje javnosti putem interneta svojih novinskih publikacija. To znači da agregatori vijesti, internetske platforme i drugi pružatelji usluga informacijskog društva moraju ishoditi dozvolu (licenciju) od novinskog nakladnika ako preuzimaju njihove članke ili dijelove članaka online te platiti pripadajuću naknadu, osim ako sam nakladnik ne odluči dati odobrenje bez naknade. Cilj je omogućiti novinskim nakladnicima da ostvare naknadu od npr. preuzimanja vijesti na tražilicama, Google News-u i sl. Srodno pravo nakladnika novinskih publikacija, nije, dakle autorsko pravo i postoji mimo i pored autorskog prava, ali ga ne smije ugrožavati. Drugim riječima, izvršavanja prava novinskih nakladnika ne smije štetiti autorskim pravima novinara, fotoreportera, urednika i drugih autora sadržaja koji se nalazi u publikaciji. Nakladnik stječe svoje srodno pravo zbog investicije u stvaranje publikacije te organizacije i prezentacije sadržaja. Pripada nakladniku izvorno, po samom zakonu, bez potrebe ikakve registracije ili ugovora te ga nakladnik može slobodno izvršavati bez potrebe sklapanja ikakvih dodatnih pravnih poslova – ugovora ili ishođenja licencija. Objekt prava novinskih nakladnika su novinska izdanja, na bilo kojem mediju, uključujući i na papira, npr. dnevne novine, tjedni ili mjesečni magazini, magazini s pretplatom, internetski portali s vijestima i sličnim sadržajima. Dakle, objekt prava su novinska izdanja koja sadrže uglavnom novinarske tekstove, fotografije i videoisječke. Zaštitu uživa cijela publikacija i svaki njen dio, osim u slučajevima kad se publikacija i njeni dijelovi koriste za privatne i nekomercijalne svrhe, kad se stavljaju poveznice (*hyperlinkovi*) i kad se koriste pojedinačne riječi ili vrlo kratki isječci iz publikacija koji nemaju više od nekoliko riječi i koji ne sadrže fotografije ili videosadržaje, pod uvjetom da takvo korištenje ne utječe na djelotvornost isključivih prava nakladnika. Djelotvornost prava će biti ugrožena kad se korištenjem vrlo kratkih isječaka zamjenjuje sama informativna publikacije ili kad se čitatelja odvraća od upućivanja na nju.

Važno je naglasiti i odnos autora (novinara) i nakladnika: zakon propisuje da autori djela uvrštenih u novinsku publikaciju (novinari, fotoreporteri) imaju pravo na odgovarajući udio u naknadi koju nakladnik ostvari od trećih (npr. od Googlea ili drugih platformi) za korištenje njegovih publikacija. Time se želi osigurati da i novinari te fotoreporteri financijski sudjeluju u koristima koje nakladnici ostvare od novog srodnog prava nakladnika novinskih publikacija. U praksi, to znači da ako nakladnik sklopi ugovor s npr. agregatorom vijesti i dobije naknadu, dužan je dio proslijediti autorima čija autorska djela su sadržana u toj publikaciji.

Ostala srodna prava. Pored navedenog, medijskim djelatnicima mogu biti relevantna i druga srodna prava: npr. prava filmskih producenata na umnožavanje, prikazivanje, distribuiranje i činjenje dostupnim javnosti njihovih videograma, prava organizacija za emitiranje (na prijenos njihovog signala, sprječavanje piratskog streaming-a i reemitiranja) i dr. Svi oni utječu na to što se smije reemitirati, snimiti ili objaviti.

Primjerice, ako u emisiji razotkrivanja dezinformacija želite pustiti isječak iz TV programa gdje je izrečena lažna tvrdnja, morate voditi računa o srodnom pravu organizacije za emitiranje na signal kojeg uzimate kao i na pitanje je li televizija ujedno i proizvođač tog videograma, tj. ima li ulogu filmskog producenta pa će tako onda imati i pravo na umnožavanje, na primjer. Često će takva upotreba biti pokrivena konceptom citata ili izvještavanja (kao iznimkom), ali u načelu organizacija za emitiranje ima pravo odobriti ili zabraniti korištenje svojih signala.

Zaključak ovog dijela: Sustav autorskog i srodnih prava je kompleksan, ali se svodi na jasno pravilo – neovlašteno korištenje tuđeg zaštićenog sadržaja nije dopušteno, osim ako postoji iznimka u zakonu ili licencija koju je izdao nositelje prava. Sadržaji provjere činjenica trebaju biti osmišljeni upravo u tim okvirima.

4. Ograničenja i iznimke autorskog i srodnih prava

Autorsko pravo jest apsolutno pravo, po svojoj naravi. Ono je također i isključivo pravo. No, ipak, postoji niz situacija u kojima se autorskim djelom može slobodno koristiti a da se pri tomu autora ne mora pitati za odobrenje niti mu se mora platiti naknada. Postoje zakonski određene iznimke i ograničenja koje dopuštaju korištenje zaštićenih djela bez dozvole autora, u posebnim situacijama od javnog interesa ili uz ograničeni opseg. Ove iznimke ključne su za novinarski rad i općenito rad u medijima, pogotovo kod prenošenja tuđih izjava ili prikaza radi kritike, ispravka ili informiranja javnosti. U drugim jurisdikcijama, poput američke, iznimke i ograničenja autorskog prava označavaju se izrazom *fair use*.

Citat, kritika i osvrt. Hrvatski zakon izričito dopušta doslovno navođenje ulomaka tuđeg autorskog djela (citat) koje je već objavljeno, u svrhu primjerice kritike, polemike, recenzije ili osvrta, u mjeri opravdanoj svrhom i uz obvezno navođenje izvora i autorova imena. To znači da novinar smije citirati dijelove spornog teksta ili govora ili videoisječka koji razotkriva, ako je to potrebno da bi ga kritički analizirao ili dopunio informacijama. Ovo ograničenje je temelj slobode izražavanja – omogućuje javnu raspravu i ispravljanje netočnih navoda korištenjem upravo tih navoda kao dokaza. Pri tome je bitno: citat mora biti razmjeran (ne veći nego što to svrha zahtijeva) i mora se navesti izvor (npr. ime autora i medija odakle je preuzet). Primjer: u faktografskoj analizi lažne vijesti možete prenijeti jednu ili dvije rečenice originalnog članka koje sadrže spornu tvrdnju i zatim ih demantirati; to je zakonito citiranje u svrhu kritike. Ali preuzeti čitav članak i objaviti ga nije citat. Kod preuzimanja cijelih članaka može se razmatrati primjena iznimke korištenja u svrhu informiranja javnosti, o čemu u idućem odjeljku ovoga teksta. No, ako nema mjesta primjenama iznimki i ograničenja od autorskog prava onda prenošenje nije dopušteno bez odobrenja au-

tora. Sve što se ovdje govori za autorska djela, na isti se način primjenjuje i na srodna prava – primjerice na pravo organizacije za emitiranje u pogledu njenog signala ili pravo audiovizualnog producenta u pogledu videograma. I jedno i drugo srodno pravo zanimljivo je, na primjer, kod korištenja u interaktivnim uslugama na internetu.

Izvještavanje o aktualnim događajima. Autorska djela i predmeti srodnih prava mogu se u određenoj mjeri slobodno koristiti u svrhu informiranja javnosti zbog prevladavanja interesa da javnost bude informirana o dnevnim događanjima. U skladu s time, dopušteno je umnožavati i priopćavati javnosti, uključujući i interaktivno činjenje dostupnim javnosti putem interneta, bez odobrenja i bez plaćanja naknade, u opsegu koji je potreban za izvješćivanje javnosti o tekućim događajima, putem tiska, radija, televizije ili na druge načine. Ti „drugi načini" podrazumijevaju, na primjer, prenošenje putem interneta. Tako se radi izvješćivanja javnosti smiju koristiti autorska djela i predmeti srodnih prava koji se pojavljuju kao sastavni dio tekućeg događaja o kojem se javnost izvješćuje, pod uvjetom da se koriste u opsegu koji odgovara svrsi i načinu izvješćivanja o tekućem događaju. Novinar smije, primjerice, u TV prilogu o nekom događaju prikazati isječak predavanja poznatog profesora, glazbene izvedbe na koncertu o kojem izvješćuje ili kadrove mjesta događaja koji uključuju neka zaštićena djela u pozadini, ako je to neizbježno za vijest. Ovo načelo štiti slobodu medija da izvještavaju bez straha od kršenja autorskog i srodnih prava, pod uvjetom da se kreću u opsegu koji je opravdan svrhom izvješćivanja. Pa tako kad izvješćuju o koncertu poznatog glazbenika mogu u okviru priloga pustiti par sekundi njegove glazbene izvedbe ili u podlozi govora cijelo vrijeme koristiti njegovu glazbenu izvedbu ali ne smiju prenijeti veći dio koncerta. U kontekstu borbe protiv dezinformacija, ovo znači da razotkrivanje lažne informacije koja je dio aktualnog događaja (npr. demantiranje viralne fotografije) može uključiti prikaz te fotografije ili navoda s ciljem prenošenja istine, bez odobrenja autora, jer je to dio informiranja javnosti o važnoj temi. Naravno, treba uvijek procijeniti je li prikaz tog djela nužan za vijest i ograničen na potreban opseg.

Nadalje, u okviru iste iznimke o dopuštenom korištenju u svrhu informiranja javnosti posebno je važno naglasiti da je dopušteno umnožavanje, distribuiranja te priopćavanje javnosti uključujući činjenje dostupnim javnosti, objavljenih novinskih članaka i fotografija, radijskih i televizijskih priloga te drugih audiovizualnih snimki o tekućim političkim, gospodarskim ili vjerskim pitanjima, a koji su objavljeni u drugim medijima. Drugim riječima, smije se prenositi tekstove, fotografije i videopriloge iz drugih medija u opsegu koji odgovara svrsi i načinu izvješćivanja. Ipak, ta iznimka propisana radi informiranja javnosti nije bezuvjetna. Naime, takvo prenošenje tuđih novinarskih djela bit će dopušteno samo ako autor izvornog teksta, fotografije ili videopriloga, tj. nakladnik medija koji je to objavio – nije pridržao prava na navedenim sadržajima. Pridržaj prava može se napraviti jednostavnom izjavom koja bi glasila, npr. „sva prava pridržana, uključujući iznimku radi informiranja javnosti". Uvidom u tiskane medije i portale uočava se da nakladnici medija uglavnom pridržavaju sva prava, što daje za zaključiti da nisu otvoreni naspram ovog sadržajnog ograničenja.

Ista iznimka korištenja autorskih djela u svrhu informiranja javnosti može se koristiti kad se prenose tuđi javni politički, vjerski i drugi govori održani u tijelima državne ili lokalne vlasti, vjerskim ustanovama ili prilikom državnih ili vjerskih svečanosti te izvadaka iz javnih predavanja. Ako prava na njima nisu izričito pridržana, smiju se koristiti u opsegu potrebnom za izvješćivanje javnosti na sve načine kao što je prethodno opisano.

Kod ispravka lažnih informacija moguće je koristiti se opisanim iznimkama korištenja u svrhu informiranja javnosti, za autorska djela kao i za predmete srodnih prava.

Još je jednu iznimku od isključivih prava potrebno istaknuti u kontekstu medija – riječ je o popratnom i incidentalnom korištenju. Bez odobrenja autora i drugih nositelja prava i bez plaćanja naknade može se priopćavati javnosti autorska djela i predmete srodnih prava kad se koriste popratno i incidentalno – kao nebitni, uz pravi predmet koji se umnožava, distribuira ili priopćava javnosti. Na primjer, kad je riječ o nekom izvještavanju s događanja a u pozadini svira neka glazba ili se prikazuje neka fotografija ili film. Ta pozadinska glazba, fotografija ili film su u kadru slučajno, incidentalno, popratno, a glavni predmet izvještavanja je nešto drugo.

Opisane iznimke i ograničenja od isključivih autorskih i srodnih prava postoje uglavnom u svim nacionalnim zakonodavstvima država članica Europske unije. U SAD se taj koncept slobodnog korištenja naziva *fair use* doktrinom. Unatoč razlikama, prvenstveno u pitanju kako se do njih dolazi (*fair use* kreira praksa a iznimke i ograničenja su propisani zakonom i harmonizirani na razini Europske unije) – oba koncepta dovode do istog rezultata u kojem se autorskim djelom i predmetima srodnih prava može koristiti bez odobrenja.

Primjena u provjeri činjenica: *Fact-checkeri* mogu legitimno reći da se oslanjaju na iznimku kritike i izvještavanja kad preuzimaju dio spornog sadržaja radi demantija. Na primjer, organizacija koja provjerava točnost objavljenih informacija može u svom izvještaju pokazati *screenshot* dijela internetske stranice s dezinformacijom, a kako bi jasno objasnila što je tu netočno. To se može podvesti pod iznimku citata ali i korištenja u svrhu informiranja javnosti ako u potonjem prava nisu pridržana. U svakom slučaju, bitno je da se pritom navede izvor i da se ne koristi više no što nalaže svrha. Time se sukladno zakonu pokriva upotreba tuđeg materijala u procesu suzbijanja dezinformacija.

Naravno, granice nisu uvijek kristalno jasne pa se preporuča oprez: ako postoji mogućnost da se potrebni efekt postigne bez preuzimanja zaštićenog sadržaja u cijelosti, bolje je koristiti samo dijelove ili opisati sadržaj vlastitim riječima. No, zakonske iznimke i ograničenja autorskog prava su tu upravo da omoguće slobodan tijek informacija kad je to društveno opravdano, uz istodobno očuvanje interesa autora u razumnim granicama.

5. Kolektivno ostvarivanje prava

Velik dio autorskih i srodnih prava u praksi se ostvaruje **kolektivno** – putem organizacija za kolektivno ostvarivanje prava koje djeluju kao posrednici između autora i korisnika djela. Za medijske djelatnike važno je razumjeti kako funkcioniraju, jer se često uz njihovu pomoć pribavljaju potrebne dozvole, primjerice za korištenje glazbe, fotografija ili drugih sadržaja.

Što su organizacije za kolektivno ostvarivanje prava? To su udruženja autora ili nositelja srodnih prava koji im povjeravaju upravljanje određenim pravima – najčešće pravom priopćavanja javnosti glazbenih djela, pravo reemitiranja svih vrsta autorskih djela i predmeta srodnih prava, reprografiju (fotokopiranje) i sl. U Hrvatskoj te organizacije prije započinjanja svojeg djelovanja moraju dobiti odobrenje Državnog zavoda za intelektualno vlasništvo (DZIV) i podliježu njegovom nadzoru. Zakon im često daje poseban status: zakonom propisani monopol za određenu kategoriju nositelja prava i za određenu vrstu prava. To znači da se predmnijeva da jedna organizacija (npr. HDS ZAMP za glazbene autore) zastupa sve autore u toj kategoriji, osim onih koji se izričito isključe (*opt-out*) pisanim putem. Za korisnike (poput TV kuće, radija ili portala) to je vrlo praktično rješenje jer jednim ugovorom s takvom organizacijom mogu dobiti licencu za veliki katalog djela.

Primjer: Televizijska kuća želi u emisiji (ili na portalu) puštati popularnu glazbu. Umjesto da traži dozvolu od svakog skladatelja i izvođača pojedinačno, sklapa ugovor s odgovarajućim organizacijama za kolektivno ostvarivanje prava te tako legalno koristi sva moguća glazbena djela

iz repertoara, uz plaćanje naknade određene u postotku od prihoda. Za razliku od toga, kod individualnog ostvarivanja prava se rješavaju pojedinačno, za svako autorsko djelo ili skupinu određenih autorskih djela pojedinačno. Na primjer, ako portal koristi fotografije agencijskih fotografa, često će preko agencije ili udruženja riješiti prava autora. Takva agencija ili udruženja autora nisu organizacije za kolektivno ostvarivanje prava.

Kako to pomaže u praksi? Za sam proces provjere činjenica, kolektivno ostvarivanje prava manje je direktno uključeno – jer se *fact-checking* najčešće oslanja na iznimke (citate, informiranje javnosti). No, mediji kao korisnici autorskih djela (npr. ilustracija ili arhivskih snimaka) moraju općenito imati uređena autorska prava, bilo individualno ili kolektivno. Sustav kolektivnog ostvarivanja im olakšava da budu zakonito "pokriveni" za širok raspon repertoara, dok se oni onda mogu fokusirati na kreiranje vlastitog programa.

Autorska djela u radnom odnosu i po narudžbi

U novinarskoj profesiji čest je slučaj da se autorska djela stvaraju u radnom odnosu (npr. novinar piše članak kao zaposlenik medijske kuće) ili po narudžbi (slobodni novinar ili vanjski suradnik piše tekst na zahtjev urednika, uz honorar). Ove situacije specifične su jer uključuju više uključenih strana – autora i poslodavca/naručitelja – pa zakon posebno uređuje komu pripadaju autorska prava u tim okolnostima.

Djela stvorena u radnom odnosu. Prema hrvatskom zakonu autorsko djelo stvoreno u radnom odnosu je djelo koje zaposlenik (autor) stvori izvršavajući svoje radne obveze kod poslodavca. Ako ugovorom o radu ili drugim aktom nije drugačije uređeno, smatra se da je poslodavac stekao sva isključiva imovinska prava na iskorištavanje djela stvorenog u radnom odnosu, u opsegu potrebnom za obavljanje svoje djelatnosti, bez vremenskog i prostornog ograničenja. To praktično znači da novinska kuća ima pravo koristiti članke svog zaposlenog novinara u okviru djelatnosti (objaviti ih u novinama, na portalu, arhivirati, možda prirediti kompilacije i prevoditi) i ta prava ne prestaju ako novinar ode raditi negdje drugdje. Poslodavac se može predstavljati prema trećima kao nositelj tih prava, što otklanja pravnu nesigurnost. Naravno, autor i dalje zadržava moralna prava – njegovo ime treba biti navedeno uz članak, i ima pravo prigovoriti izmjenama koje deformiraju njegov tekst. S druge strane, ako poslodavac želi koristiti djelo izvan okvira svoje redovne djelatnosti, to bi trebalo posebno ugovoriti. Poslodavac prema zakonu ima i dozvolu da: javno objavi djelo, prerađuje ga, dovrši nedovršeno djelo.

Za novinare to znači da najčešće nemaju pravo zasebno komercijalno iskorištavati članke koje su napisali u sklopu redakcijskog posla – npr. ne mogu isti tekst prodati nekom drugom mediju bez dopuštenja poslodavca, jer poslodavac već ima potrebna prava. Moguće je drugačije urediti ugovorom (primjerice da novinar zadržava dio prava za zbirku svojih tekstova), ali to bi moralo biti izričito.

Djela stvorena po narudžbi. Kod autorskih djela stvorenih po narudžbi (koja stvara vanjski suradnik prema dogovoru), sadašnji zakon kaže da se ugovorom o narudžbi uređuju elementi djela, rokovi predaje i dr. Ako ugovorom ili zakonom nije drukčije određeno, autorska imovinska prava na naručenom djelu pripadaju naručitelju, u sadržaju i opsegu koji je potreban za ostvarenje djelatnosti koju obavlja. Za borbu protiv dezinformacija, ovaj aspekt je bitan utoliko što medijske kuće imaju prava objaviti ispravke, analize, pa i eventualne kompilacije ili edukativne materijale koji sadrže radove novinara i fotoreportera koje su naručile.

Primjer: Novinar zaposlen u portalu napiše analizu dezinformacija. Portal ima prava taj članak staviti i na svoje društvene mreže, u svoje newslettere, ili ga kasnije uvrstiti u zbornik, bez da za svaku tu radnju dodatno pita novinara – jer se to sve smatra dijelom njegove djelatnosti

i pokriveno je presumiranim stjecanjem prava na strani poslodavca. Ista prava imat će portal i u pogledu djela koje naručio od vanjskog stručnjaka – npr. studiju o dezinformacijama.

6. Umjetna inteligencija i autorsko pravo

Nagli razvoj umjetne inteligencije (UI) u stvaranju sadržaja postavlja nova pitanja za autorsko pravo. Alati poput ChatGPT (za tekst) ili DALL-E/Midjourney (za slike) mogu generirati tekstove, slike ili video zapise koji nalikuju ljudskim radovima. U kontekstu dezinformacija, UI može biti dvosjekli mač: s jedne strane, može pomoći u otkrivanju lažnih informacija (npr. algoritmi za detekciju manipuliranih slika), a s druge strane, može i sam generirati uvjerljive lažne sadržaje (poput *deepfake* videa ili lažnih članaka). Važno je razumjeti kako pravo gleda na UI generirani sadržaj – tko (ako itko) ima autorska prava i smije li se takav sadržaj slobodno koristiti.

Autorsko djelo i "smrt autora". Tradicionalno, kao što je već istaknuto, autor mora biti ljudska osoba. Autorsko pravo pripada fizičkoj osobi koja stvori djelo. To implicira da djelo nastalo isključivo djelovanjem stroja ili računarskog programa ne može imati autora u pravnom smislu, te stoga ne uživa standardnu autorskopravnu zaštitu. Upravo su to potvrdili i nedavni pravni slučajevi i smjernice: npr., Američki Ured za autorsko pravo izdao je 2023. smjernice da će registrirati samo ona djela u kojima je ljudski autor značajno doprinio, dok će isključivo UI-generirane sadržaje odbiti. U čuvenom slučaju *Thaler v. Perlmutter (2023)*, sud je potvrdio da slike koje je stvorila umjetna inteligencija bez ikakvog ljudskog kreativnog unosa nisu predmet autorskog prava, jer nedostaje ljudska kreativnost. Isto je razumijevanje i u drugim jurisdikcijama. Posljedično, sadržaj koji generira UI (tekst, slika, glazba) – ako zaista nema ljudskog doprinosa – zapravo je javno dobro u smislu autorskog prava; svatko ga može koristiti, mijenjati i distribuirati bez dozvole, jer nema zaštićenog autora. To može biti korisno npr. medijima koji žele koristiti neku UI-generiranu ilustraciju uz članak (ne moraju brinuti o licenci ako je sigurno da je isključivo UI stvaratelj toga materijala). Međutim, granica je zamagljena kada postoji kombinacija: često ljudi koriste UI alate, pa do određene mjere urede ili odaberu rezultat. Pitanje je koliki ljudski doprinos je potreban da bi se korisnik UI alata smatrao autorom. Za sada, jasnog kriterija nema – sudovi će to razmatrati od slučaja do slučaja, ali smjer je da mora postojati kreativna ljudska kontrola nad rezultatom da bi mu se priznala autorskopravna zaštita.

Trening UI i povrede tuđih autorskih i srodnih prava. Drugi aspekt problema umjetne inteligencije sastoji se u tomu da UI modeli uče na ogromnim bazama podataka postojećih djela (tekstova, slika, glazbe) i predmeta srodnih prava. Oni u procesu generiranja mogu posredno umnožavati elemente tih djela. Korisnik koji dobije rezultat kojeg je generirala UI ne može znati sadrži li on dijelove nečijeg zaštićenog rada. U borbi protiv dezinformacija, ako se koristi UI za generiranje lažnih vijesti ili slika, može se dogoditi dvostruki problem: širenje laži i istovremeno povreda autorskog prava originalnog autora, čiji su radovi poslužili kao izvor.

Europsko zakonodavstvo zasad nema posebne odredbe kojima bi se uređivalo pitanje autorstva na rezultatima koji su generirani uz pomoć umjetne inteligencije. Kroz Akt o umjetnoj inteligenciji (UI Act) adresiraju se etička i sigurnosna pitanja, ali se njime ne mijenjaju autorskopravni temelji. Postavlja se jedino obaveza transparentnosti podataka o korištenju autorskih djela i predmeta srodnih prava u treniranju umjetne inteligencije. Dakle, ključna točka u cijeloj priči s umjetnom inteligencijom jest ta da se za autorskopravnu zaštitu nekog generiranog sadržaja zahtijeva da postoji dostatan ljudski faktor. Ako novinar koristi, recimo, ChatGPT kao alat za izradu nacrta članka, on u to unosi svoju kreativnost (postavlja pitanja, uređuje odgovor, usmjerava rad umjetne inteligencije) te se može smatrati autorom konačnog teksta

u mjeri u kojoj je oblikovao taj rezultat. Ali ako netko pokuša prikazati rezultat koji je isključivo nastao generativnom umjetnom inteligencijom kao svoje djelo, ulazi u „sivu zonu" – moralno gledano. S druge strane, pravno gledano, taj rezultat vrlo vjerojatno i nema autorskopravnu zaštitu pa ga bilo tko drugi može slobodno preuzeti.

UI kao alat u novinarstvu. Iz perspektive dezinformacija, UI je koristan alat za analizu podataka i otkrivanje obrazaca. Također, UI sustavi mogu automatski označavati sumnjive tvrdnje ili generirati sažetke složenih činjenica. Pri svemu tomu treba paziti da UI ima pristup samo legalno pribavljenim podacima (npr. ako treniramo model na novinskim člancima, treba imati dozvole nositelja prava ili se osloniti na javno dostupne baze).

7. Zaključak

Borba protiv dezinformacija traži multidisciplinarni pristup u kojem se isprepliću novinarske vještine, tehnološka rješenja, ali i pravni alati. Autorsko i srodna prava možda na prvi pogled djeluju kao ograničenje – nešto što sputava slobodu djelovanja u razotkrivanju neistina. No, zapravo, pravilno poznavanje ovih prava omogućuje sigurnije i učinkovitije djelovanje. Novinar ili urednik koji razumije koje ulomke smije citirati bez traženja dozvole, kako zakon štiti njegov vlastiti autorski rad, te kako pribaviti licence kad su potrebne, moći će s više samopouzdanja objavljivati ispravke i analize.

Pravni okvir pruža i zaštitu legitimnim kreatorima sadržaja – ne smije se zaboraviti da u nastojanju da suzbijemo dezinformacije ne smijemo ugroziti prava onih koji stvaraju kvalitetne, istinite sadržaje. Stoga je poštivanje autorskog i srodnih prava dio šireg etičkog i pravnog standarda profesionalnog novinarstva. Kao što tražimo od drugih da poštuju činjenice, tako i mi moramo poštovati tuđe stvaralaštvo.

U praksi, to znači uvijek:

- navesti izvore informacija i citata (time ispunjavamo i zakonsku obvezu kod iznimke citata i novinarski standard transparentnosti);
- koristiti onoliko koliko je nužno iz tuđeg djela – ništa više;
- provjeriti licence za fotografije, video snimke ili glazbu koja se koristi u prilozima (kroz agencije ili kolektivne organizacije;
- educirati se o novim pravima – npr. o pravu nakladnika novinskih izdanja – koje mogu utjecati na to kako preuzimamo vijesti s drugih portala;
- biti svjestan UI alata – što nam nude i koje rizike nose – i uvijek uključiti ljudsku prosudbu, kako kreativnu tako i pravnu.

Uz takav pristup, pravni aspekti postaju saveznik u borbi protiv dezinformacija. Omogućuju da se istina širi bez nepotrebnih prepreka, a da se pri tom ne krše ničija zakonska prava. Novinari, urednici i regulatori imaju zadatak balansirati slobodu izražavanja i informiranja sa zaštitom intelektualnog vlasništva – a taj balans je upravo ono što demokratsko društvo čini otpornim na laži i manipulacije, uz poštovanje rada svakog pojedinca.

Rezimirajući, poznavanje i primjena tema iz ovog priručnika – od prava na ispravak, preko autorskog prava, iznimaka, kolektivnog sustava, specifičnih ugovornih situacija, do izazova umjetne inteligencije – pruža cjelovit alat novinarima i medijskim stručnjacima da sigurno navigiraju kroz pravne izazove dok predano rade na istini kao krajnjem cilju. U konačnici, i pravo i novinarstvo teže istom idealu: da istinita informacija dođe do javnosti, uz očuvanje reda i pravde u procesu.

Regulacija digitalnih usluga, medijska regulacija i aktivnosti međunarodnih organizacija u borbi protiv dezinformacija

Prof. dr. sc. Hrvoje Lisičar
Pravni fakultet Sveučilišta u Zagrebu

1. Uvodno o zakonodavnom okviru

Zakonodavni okvir koji uređuje pružanje digitalnih i medijskih usluga jedan je od ključnih alata za borbu protiv širenja dezinformacija. Jasno utvrđena pravila za pružanje digitalnih i medijskih usluga smanjuju rizik od njihove zloporabe u svrhu širenja dezinformacija. Njime se ujedno potiče i osnažuje borba protiv nezakonitog i štetnog sadržaja te se olakšava rad neovisnim provjeravateljima informacija. Zbog toga zakonodavni okvir za pružanje digitalnih i medijskih usluga predstavlja temelj za učinkovitu borbu protiv dezinformacija pri čemu se istovremeno mora jamčiti i zaštita temeljnih prava građana.

U tu svrhu Europska unija razvila je sveobuhvatni zakonodavni okvir koji horizontalno utvrđuje obveze za sve pružatelje i sve vrste digitalnih i medijskih usluga. Ključni akti europskog horizontalnog pristupa su: Uredba 2022/2065, poznatija pod nazivom Akt o Digitalnim uslugama[1] (dalje u tekstu: DSA) zajedno sa Kodeksom dobre prakse u suzbijanju dezinformacija koji je uključen u okvir Akta o digitalnim uslugama, Direktiva 2018/1808, skraćenog naziva Direktiva o audiovizualnim medijskim uslugama[2] (dalje u tekstu: AVMSD) te Uredba 2024/1083 tj. Europski akt o slobodi medija[3] (dalje u tekstu: EMFA).

Cilj ovog poglavlja je objasniti doseg zakonodavnog okvira u kontekstu borbe protiv dezinformacija te obraditi specifične odredbe pojedinog zakonodavnog akta koje su relevantne za borbu protiv dezinformacija te sprečavanje širenja nezakonitog i štetnog sadržaja putem digitalnih i medijskih platformi. Poglavlje slijedi strukturu relevantnog modula te se zakonodavni akti obrađuju u skladu s njihovim obuhvatom, od općih pravnih pravila (*lex generalis*) koja se primjenjuju na sve vrste digitalnih usluga i pružatelja, prema specifičnim pravnim pravilima (*lex specialis*) koja su primjenjiva u kontek-

[1] Uredba (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama), SL L 277, 27.10.2022., str. 1–102.

[2] Direktiva (EU) 2018/1808 Europskog parlamenta i Vijeća od 14. studenoga 2018. o izmjeni Direktive 2010/13/EU o koordinaciji određenih odredaba utvrđenih zakonima i drugim propisima u državama članicama o pružanju audiovizualnih medijskih usluga (Direktiva o audiovizualnim medijskim uslugama) u pogledu promjenjivog stanja na tržištu, SL L 303, 28.11.2018., str. 69–92.

[3] Uredba (EU) 2024/1083 Europskog parlamenta i Vijeća od 11. travnja 2024. o uspostavi zajedničkog okvira za medijske usluge na unutarnjem tržištu i izmjeni Direktive 2010/13/EU (Europski akt o slobodi medija), SL L, 2024/1083, 17.4.2024.

stu pružanja specifičnih medijskih i digitalnih usluga. Nadalje, poglavlje se bavi implementacijom akata u zakonodavni okvir Republike Hrvatske te konačno pojedinim relevantnim tekstovima međunarodnih organizacija koji ne pripadaju u zakonodavni okvir za regulaciju digitalnih usluga i elektroničkih medija ali predstavljaju smjernice i dobru praksu u borbi protiv dezinformacija.

2. Akt o digitalnim uslugama

Akt o digitalnim uslugama predstavlja temeljnu reformu europskog pravnog okvira za digitalne usluge, usmjerenu na stvaranje sigurnijeg i transparentnijeg online okruženja. Ovaj regulatorni instrument, koji je u cijelosti u primjeni od veljače 2024., posebno je relevantan za medije i borbu protiv dezinformacija, jer uvodi sustavne mjere za zaštitu slobode izražavanja i suzbijanje nezakonitog sadržaja i dezinformacija. DSA ne samo da modernizira zastarjele odredbe iz Direktive o elektroničkoj trgovini[4] iz 2000. godine, već i direktno utječe na način funkcioniranja društvenih mreža, tražilica i drugih online posrednika koji igraju ključnu ulogu u distribuciji informacija.

2.1. Tumačenje pojedinih važnih pojmova u kontekstu borbe protiv dezinformacija

U svrhu boljeg razumijevanja DSA u kontekstu borbe protiv dezinformacija potrebno je prethodno protumačiti značenje pojedinih pojmova koji su korišteni u DSA a koji su povezani s relevantnim odredbama koje pridonose borbi protiv nezakonitih sadržaja i dezinformacija.

Usluga informacijskog društva Aktom o digitalnim uslugama definirana je kao usluga u članku 1. stavku 1. točki (b) Direktive (EU) 2015/1535 što podrazumijeva svaku uslugu koja se obično pruža uz naknadu, na daljinu, elektroničkim sredstvima te na osobni zahtjev primatelja usluga. Za potrebe ove definicije pojam „na daljinu" znači da se usluga pruža bez da su strane istodobno prisutne, pojam „elektroničkim sredstvima" znači da se usluga na početku šalje i prima na odredištu pomoću elektroničke opreme, za obradu (uključujući digitalnu kompresiju) i pohranu podataka te u potpunosti šalje, prenosi i prima telegrafski, radio vezom, optičkim sredstvima ili ostalim elektromagnetnim sredstvima, te konačno pojam „na osobni zahtjev primatelja usluga" znači da se usluga pruža prijenosom podataka na osobni zahtjev onoga tko uslugu prima.

Posredničke usluge prema DSA definirane su kao usluge informacijskog društva koje mogu biti prijenosnik informacija (npr. telekom kompanije), usluge privremenog smještaja u svrhu učinkovitijeg prijenosa podataka te usluge koje korisnicima omogućavaju smještaj informacija na poslužitelju (npr. cloud servisi ili internetske platforme koje omogućavaju pohranu podataka).

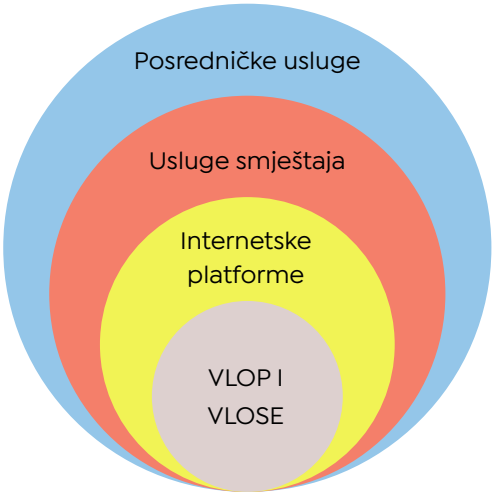
Internetska platforma je usluga informacijskog društva za smještaj informacija na poslužitelju kojom se na zahtjev primatelja usluge informacije pohranjuju i šire u javnosti, osim ako je to sporedna aktivnost koja je isključivo pomoćna značajka druge usluge ili manja funkcionalnost glavne usluge i koja se iz objektivnih i tehničkih razloga ne može koristiti bez te druge usluge te integracija te značajke ili funkcionalnosti u drugu uslugu nije način za izbjegavanje primjene DSA (npr. Instagram, Facebook, Youtube ...). Internetske platforme koje u Europskoj uniji imaju više od 45 milijuna korisnika nazivaju se vrlo velike internetske platforme (VLOP) te su im nametnute dodatne obveze Aktom o digitalnim uslugama jer mogu uzrokovati društvene rizike koji se po opsegu i učinku razlikuju od onih koje uzrokuju manje platforme.

Internetska tražilica je usluga informacijskog društva za posredovanje koja korisnicima omogućuje da unose upite u svrhu pretraživanja, u načelu, svih internetskih stranica ili svih internetskih stranica na određenom jeziku na

[4] Direktiva 2000/31/EZ Europskog parlamenta i Vijeća od 8. lipnja 2000. o određenim pravnim aspektima usluga informacijskog društva na unutarnjem tržištu, posebno elektroničke trgovine (Direktiva o elektroničkoj trgovini) SL L 178, 17.7.2000., str. 1–16.

temelju upita o bilo kojoj temi koji je u obliku ključne riječi, glasovnog zahtjeva, rečenice ili nekog drugog unosa, te vraća rezultate u bilo kojem formatu u kojem se mogu pronaći informacije koje su povezane sa zatraženim sadržajem. (Google Search itd..). Internetske tražilice koje u EU imaju više od 45 milijuna korisnika nazivaju se vrlo velike internetske tražilice (VLOSE) te su im nametnute dodatne obveze DSA-om jer mogu uzrokovati društvene rizike koji se po opsegu i učinku razlikuju od onih koje uzrokuju manje platforme.

Grafički prikaz 1. - Odnos i obuhvat posredničkih usluga



Nezakonit sadržaj podrazumijeva svaku informaciju koja, sama po sebi ili u vezi s određenom aktivnošću, uključujući prodaju proizvoda ili pružanje usluga, nije u skladu s pravom Unije ili pravom bilo koje države članice koje je u skladu s pravom Unije, neovisno o samom sadržaju ili prirodi tog prava (npr. prodaja artikala čiji je promet zakonom zabranjen ili ograničen, dječja pornografija, sadržaj koji potiče terorizam i sl.). Ovdje je bitno istaknuti da DSA utvrđuje samo pravila za otkrivanje, označavanje i uklanjanje nezakonitog sadržaja dok izričito ne navodi što se ima smatrati nezakonitim sadržajem. Nezakonit sadržaj definiran je drugim zakonima na razini EU-a ili na nacionalnim razinama država članica te ako je sadržaj nezakonit samo u određenoj državi članici, u pravilu ga treba ukloniti na području gdje je to nezakonito.

Širenje u javnosti znači stavljanje informacija na raspolaganje potencijalno neograničenom broju trećih strana na zahtjev primatelja usluge koji je dao te informacije.

Sustav za preporučivanje znači potpuno ili djelomično automatiziran sustav kojim se internetska platforma koristi kako bi u svojem internetskom sučelju primateljima usluge predlagala specifične informacije ili kako bi određivala njihov prioritet, među ostalim i na temelju pretrage koju je pokrenuo primatelj usluge ili drukčije određenog relativnog redoslijeda ili važnosti prikazanih informacija (najčešće se radi o sustavima koji su upravljani algoritmima na temelju obrade osobnih podataka korisnika).

Moderiranje sadržaja podrazumijeva aktivnosti, automatizirane ili neautomatizirane, koje poduzimaju pružatelji usluga posredovanja s ciljem, osobito, otkrivanja, identificiranja i suzbijanja nezakonitog sadržaja ili informacija dobivenih od primatelja usluge koje nisu u skladu s njihovim uvjetima poslovanja, uključujući poduzete mjere koje utječu na raspoloživost, vidljivost i dostupnost tog nezakonitog sadržaja ili informacija, kao što su degradacija, demonetizacija, onemogućavanje pristupa tom sadržaju ili njegovo uklanjanje, ili koje utječu na sposobnost primatelja usluge za davanje tih informacija, kao što su zatvaranje ili suspendiranje računa primatelja.

Pouzdani prijavitelji su subjekti koji djeluju u okviru svog područja stručnosti u svrhu suzbijanja i prijave objavljenog nezakonitog i lažnog sadržaja putem usluga informacijskog društva, koristeći mehanizme obavješćivanja i djelovanja, a koje pružatelji usluga informacijskog društva moraju implementirati u skladu s DSA-om.

2.2. Obuhvat Akta o digitalnim uslugama (DSA)

Za medije, DSA donosi dvostruku prednost: s jedne strane, štiti autentične izvore od neopravdanog uklanjanja sadržaja kroz stroža pravila o transparentnosti moderiranja sadržaja, a s druge strane nameće platformama obvezu suradnje s provjerenim medijskim izvorima i neovisnim provjeravateljima informacija. DSA obuhvaća i primjenjuje se na digitalne usluge koje se nude korisnicima koji se nalaze u EU-u, bez obzira na mjesto nastana samih pružatelja usluga te ujedno predviđa i višeslojna pravila za posredničke usluge, hosting usluge online platformi, vrlo velike internetske platforme (VLOP) i vrlo velike internetske tražilice (VLOSE). U kontekstu objekta regulacije DSA je usmjeren na posredničke usluge, internetske platforme te internetske tražilice. Temeljni ciljevi DSA su olakšati ponudu prekograničnih digitalnih usluga i stvoriti jedinstvena pravila za unutarnje europsko tržište, učiniti internet i digitalne usluge sigurnijim mjestom na kojem se primjenjuje nacionalno pravo i gdje svatko u EU-u može slobodno ostvarivati svoja temeljna prava, posebice pravo na slobodu izražavanja i informiranja, suzbijanje dezinformacija i govora mržnje uzimajući u obzir način na koji posluju platforme koje mogu svojim djelovanjem naštetiti demokratskim procesima te uspostaviti jednake uvjete za poticanje inovacija, rasta i konkurentnosti, kako na jedinstvenom europskom tržištu tako i globalno. Kako bi se postigli navedeni ciljevi DSA uspostavlja pravna pravila koja se odnose na: odgovornost za pružanje digitalnih usluga; prijavu nezakonitog sadržaja; izvješća o transparentnosti za online platforme; zabranu manipulativnih praksi (*dark patterns*); ograničenja bihevioralnog oglašavanja te iznimke za male i srednje tvrtke koje pružaju digitalne usluge. Kada su u pitanju vrlo velike online platforme i tražilice, DSA nameće obvezu procjene i ublažavanje rizika, uspostavljanje neovisne provjere informacija, uspostavu sustava za preporučivanje sadržaja, vođenje arhive oglašavanja, osiguravanje pristupa podacima za istraživače i organizacije civilnog društva. U smislu teritorijalne nadležnosti za provedbu navedenih obveza DSA uzima u obzir načelo zemlje podrijetla pružatelja usluga, dok je nadležnost za poslovanja VLOP-ova povjerena izravno Komisiji EU-a i njenim tijelima.

U sklopu DSA, borba protiv dezinformacija temelji se na dva stupa: uklanjanju nezakonitog sadržaja (npr. govor mržnje) i suzbijanju "društveno štetnih" obmanjujućih sadržaja koji ne spadaju u kategoriju nezakonitog sadržaja ali ugrožavaju javni raspravu i imaju negativan utjecaj na društvo u cijelosti.[5] Tako DSA uvodi mjere za suzbijanje nezakonitog sadržaja na internetu, uključujući nezakonitu robu i usluge. Nametnuti su novi mehanizmi koji korisnicima omogućuju označavanje nezakonitog sadržaja na mreži i za platforme obvezu suradnje sa specijaliziranim „pouzdanim prijaviteljima" za prepoznavanje i uklanjanje nezakonitog sadržaja. Uvode se nova pravila za praćenje prodavača na internetskim tržištima, kako bi se izgradilo povjerenje i lakše prepoznalo prevarante. Uvedena je nova obveza za internetska tržišta da nasumično provjeravaju postojeće baze podataka jesu li proizvodi ili usluge na njihovim stranicama usklađeni sa zakonodavnim okvirom. Također, uvode se učinkovite zaštitne mjere za korisnike, uključujući mogućnost osporavanja odluke o moderiranju sadržaja temeljene na obveznim informacijama koje platforme sada moraju pružiti korisnicima kada se njihov sadržaj ukloni ili mu se ograniči pristup. Predviđen je i širok raspon mjera transparentnosti za online platforme, uključujući bolje informacije o uvjetima korištenja, kao i transparentnost algoritama koji se koriste za preporučivanje sadržaja ili proizvoda korisnicima. Jedna od značajnih promjena se odnosi i na bolju zaštitu maloljetnika na bilo kojoj platformi koja pruža usluge na području Europske unije. Kada su u pitanju obveze za VLOP i VLOSE one imaju ob-

[5] The Digital Services Act (DSA) and combating disinformation – 10 key takeaways, https://chamber.com/articles/the-digital-services-act-dsa-and-combating-disinformation-10-key-takeaways. (24.3.2025)

vezu spriječiti zlouporabu svojih sustava poduzimanjem radnji temeljenih na riziku, uključujući nadzor putem neovisnih revizija njihovih mjera za upravljanja rizikom. Također, moraju ublažiti rizike kao što su dezinformacije ili izborne manipulacije, cyber nasilje nad ženama ili štetu za maloljetnike na internetu. Ove mjere moraju biti pažljivo usklađene s ograničenjima slobode izražavanja i podliježu neovisnoj reviziji. Uvode se novi mehanizmi odgovora na krizne situacije u slučajevima ozbiljne prijetnje javnom zdravlju i sigurnosti poput pandemije ili rata. Nadalje, uspostavlja se zabrana ciljanog oglašavanja na internetskim platformama profiliranjem djece ili na temelju posebnih kategorije osobnih podataka kao što su etnička pripadnost, politički stavovi ili seksualna orijentacija. U kontekstu borbe protiv dezinformacija moguće je izdvojiti i odredbe koje se odnose na transparentnost za sva oglašavanja na internetskim platformama i reklame tzv. „influencera", zabranu korištenja takozvanih 'tamnih uzoraka' na sučelju online platformi, pozivajući se na zavaravajuće trikove koji manipuliraju korisnicima na izbore koje ne namjeravaju učiniti te nove odredbe koje omogućavaju pristup podacima za istraživače koji se bave ključnim platformama, a kako bi mogli ispitati na koji način platforme funkcioniraju i kako se razvijaju online rizici. U pogledu zaštite prava korisnika DSA korisnicima platformi omogućuje pravo žalbe na usluge i odluke platformi, rješavanje spora izvan suda, žalbe vlastitim nacionalnim tijelima na svom jeziku ili traženje naknade za kršenje prava. Također, reprezentativne organizacije koje predstavljaju korisnike mogu braniti prava korisnika za šire povrede zakona.

Za provedu DSA ključna je uspostava nove jedinstvene strukture nadzora, posebice kada su u pitanju VLOP i VLOSE. Europska komisija primarni je regulator za VLOP i VLOSE, dok su ostale platforme i tražilice pod nadzorom država članica u kojima su uspostavljeni (imaju poslovni nastan). Komisija ima izvršne ovlasti slične onima koje ima u nadzoru i provedbi zakonodavnog okvira za tržišno natjecanje.

Temeljem prethodno iznesenog moguće je posebno izdvojiti najvažnije odredbe DSA koje imaju značajan utjecaj na borbu protiv dezinformacija:

Članak 16. – Mehanizmi obavješćivanja i djelovanja

Sve platforme koje pružaju usluge pohrane sadržaja moraju implementirati jednostavne mehanizme za prijavu sumnjivog sadržaja. Korisnici mogu elektroničkim putem prijaviti sadržaj koji smatraju dezinformacijom, uz obvezu iznošenja detaljnog obrazloženja i točnom lokacijom sadržaja. Platforme su dužne odgovoriti na svaku prijavu te objasniti donesene odluke, što povećava transparentnost procesa.

Članak 22. – Pouzdani prijavitelji

DSA uvodi koncept "pouzdanih prijavitelja" *(trusted flaggers)* – subjekata koji posjeduju stručna znanja u prepoznavanju ilegalnog sadržaja, uključujući koordinirane dezinformacijske kampanje. Nacionalni koordinatori za digitalne usluge (HAKOM u Hrvatskoj) ovlašteni su dodjeljivati ovaj status subjektima koje ispunjavaju kriterije neovisnosti i stručnosti. Primjerice, provjeravatelji činjenica ili medijske kuće mogu postati pouzdani prijavitelji, a platforme su obvezne njihove prijave procesuirati prioritetno i bez odgađanja.

Članak 34. – Procjena rizika

Vrlo velike internetske platforme (VLOP) i vrlo velike internetske tražilice (VLOSE) moraju provoditi godišnje procjene rizika, uključujući rizik od širenja dezinformacija. Ova procjena mora uključivati analizu utjecaja algoritamskih sustava na širenje dezinformacija te evaluaciju mogućeg negativnog djelovanja na izborne procese i sigurnost građana. Primjerice, platforme moraju analizirati kako njihovi sustavi za preporuku sadržaja povećavaju vidljivost obmanjujućih narativa.

Također, pružatelji usluga u svojim uvjetima poslovanja koje moraju javno objaviti, jedno-

stavnim i razumljivim jezikom utvrđuju glavne kriterije koji se upotrebljavaju u njihovim sustavima za preporučivanje, kao i sve opcije za izmjenu tih glavnih kriterija ili utjecanje na njih. To podrazumijeva kriterije koji su najznačajniji za utvrđivanje informacija predloženih primatelju usluge te razloge za relativnu važnost tih kriterija.

Članak 35. – Smanjenje rizika

Komisija u suradnji s koordinatorima za digitalne usluge može izdati smjernice o primjeni stavka 1. u vezi s posebnim rizicima, ponajprije kako bi dala primjere dobre prakse i preporučila moguće mjere, uzimajući u obzir moguće posljedice mjera na temeljna ljudska prava svih uključenih strana koja su utvrđena u Povelji o ljudskim pravima. Nadalje, VLOP moraju prilagoditi svoje algoritme kako bi smanjili širenje dezinformacija. To uključuje smanjenje vidljivosti dezinformacija u korisničkim preporukama i jasno obavještavanje korisnika o kriterijima preporuke. Primjerice, platforme moraju omogućiti korisnicima da deaktiviraju personalizirane preporuke temeljene na profiliranju.

Članak 45. – Kodeksi ponašanja

Temeljem članaka 45. DSA Europska komisija integrirala je Kodeks dobre prakse u suzbijanju dezinformacija u DSA okvir što između ostalo zahtjeva od platformi koje su pristupile Kodeksu da demonetiziraju dezinformacijske kampanje oduzimanjem prihoda od oglašavanja, povećaju transparentnost političkog oglašavanja s jasnim označavanjem izvora financiranja te surađuju s provjeravateljima točnosti informacija i akademskim institucijama u verifikaciji sadržaja.

2.3. Kodeks dobre prakse u suzbijanju dezinformacija

Kodeks dobre prakse u suzbijanju dezinformacija iz 2022. godine (dalje u tekstu: Kodeks) postao je sastavni dio zakonodavnog okvira Akta o digitalnim uslugama (DSA) nakon službene integracije 13. veljače 2025. Kodeks je kreiran kao samoregulativni akt nakon dugoročne suradnje Europske komisije, nacionalnih regulatornih tijela, nevladinih organizacija, istraživača i predstavnika platformi. Temeljni cilj donošenja Kodeksa bio je stvoriti samoregulativni okvir za suzbijanje dezinformacija a koji je u cijelosti prihvaćen od svih dionika (platforme, oglašivači, mediji, korisnici i ostali dionici) koji sudjeluju na tržištu pružanja digitalnih usluga. U veljači 2025. godine Europska komisija i Europski odbor za digitalne usluge službeno su integrirali Kodeks u okvir DSA temeljem članka 45. DSA te je time, sam Kodeks iz samoregulativnog akta, postao svojevrstan regulatorni alat za suzbijanje dezinformacija unutar okvira DSA. Predmetna transformacija iz samoregulacije prema koregulaciji osigurava nadležnim tijelima strožu provedu mjera protiv dezinformacija posebice kada su u pitanju vrlo velike internetske platforme (VLOP) i vrlo velike internetske tražilice (VLOSE).

Kodeks sadrži brojne obveze i specifične mjere kojima se adresira različite oblike dezinformacija dok se istovremeno štiti sloboda izražavanja i promiče transparentnost postupanja. Mjere i obveze sadržane u Kodeksu podijeljene su u četiri osnovne skupine koje su međusobno povezane: demonetizacija, transparentnost u političkom oglašavanju, cjelovitost usluga te osnaživanje korisnika, istraživača i zajednice za provjeru točnosti informacija.

Demonetizacija podrazumijeva da se potpisnici Kodeksa obvezuju demonetizirati sadržaj koji ima svrhu širenja dezinformacija te poboljšati politike i sustave koji određuju prihvatljivost sadržaja za monetizaciju, kontrole za monetizaciju i postavljanje oglasa te podatke za izvješća o točnosti i učinkovitosti kontrola i usluga oko položaja oglasa. U tu svrhu predviđeno je 13 specifičnih mjera od koji su neke: izbjegavanje objavljivanja i prijenosa štetnih dezinformacija kako bi se zaštitio integritet tvrtke koje podržava oglašavanje, poduzimanje smislenih mjera za provedbu i sanaciju kako bi se izbje-

glo postavljanje oglašavanje uz dezinformacijski sadržaj ili na izvorima koji opetovano krše pravila, usvajanje mjera za omogućavanje provjere odredišnih/odredišnih stranica oglasa i podrijetlo postavljanja oglasa. Nadalje, potpisnici Kodeksa se obvezuju spriječiti zlouporabu oglašavanja i sustava za širenje dezinformacija u obliku reklamnih poruka. Također, potpisnici Kodeksa koji su uključeni u kupnju, prodaju i postavljanje digitalnog oglašavanja će razmjenjivati najbolje prakse i jačati suradnju s relevantnim organizacijama aktivnim u lancu vrijednosti online monetizacije, kao što je online plaćanje usluga, platforme za e-trgovinu i relevantne sustave skupnog financiranja/doniranja, s ciljem kako bi povećali učinkovitost nadzora položaja oglasa na vlastitim uslugama. Ostale mjere uključuju korištenje alata za identifikaciju internetskih lokacija i korisničkih profila koji sustavno šire dezinformacije, ograničavanje pristupa alatima koji omogućavaju monetizaciju (kao što su adSense), korištenje "crnih lista" internetskih lokacija koje šire dezinformacije, evaluaciju algoritama za prepoznavanje dezinformacija, uklanjanje lažnih profila koji služe za širenje dezinformacija. Sve navedene mjere imaju za cilj uspostaviti temeljni mehanizam za smanjenje ekonomske održivosti širenja dezinformacija.

Transparentnost u političkom oglašavanju uključuje skupinu mjera koje zajedno s mjerama za demonetizaciju imaju za cilj smanjiti/spriječiti širenje dezinformacija koristeći ciljano reklamiranje i omogućiti građanima bolje razumijevanje namjere političkog oglašavanja. Potpisnici Kodeksa obvezuju se usvojiti zajedničku definiciju političkog oglašavanja ili oglašavanja vezano za važna društvena pitanja. Nadalje, potpisnici Kodeksa obvezuju se da će jasno označiti političke oglase kao plaćeni sadržaj. Ova oznaka mora biti vidljiva korisnicima čak i kada se oglasi dijele ili preusmjeravaju na druge platforme. Potpisnici moraju također primijeniti dosljedan pristup političkom oglašavanju ili oglašavanju o važnim društvenim pitanjima na svojim uslugama što podrazumijeva da u svojim pravilima oglašavanja jasno naznače u kojoj mjeri je takvo oglašavanje dopušteno ili zabranjeno na njihovim uslugama. Svaki politički oglas mora sadržavati potpunu identifikaciju sponzora, uključujući njegovo pravo ime, kontaktne podatke i financijske izvore. Platforme su dužne provjeriti autentičnost ovih podataka prije objave oglasa. Konačno, ovdje možemo još izdvojiti i mjere koje nameću obvezu platformama koje su pristupile Kodeksu a koje se odnose na obvezu uspostave kontaktne točke za nacionalne regulatore, podnošenje kvartalnih izvješća te razvoja alata za provjeru koji omogućavaju korisnicima lako prepoznavanje političkih oglasa.

Kako bi se osigurao integritet usluga u skladu s Kodeksom predviđeno je nekoliko ključnih mjera. To uključuje implementaciju robusnih sustava za moderiranje sadržaja te otkrivanje i uklanjanje dezinformacija. Nadalje, platforme moraju osigurati transparentnost u algoritamskim procesima i praksama moderiranja sadržaja. Platforme se također potiču da uspostave jasne postupke za korisnike za prijavu dezinformacija, davanje pravovremenih odgovora i suradnju s nacionalnim regulatornim tijelima i provjeravateljima informacija. Osim toga, naglasak je na provođenju redovitih procjena rizika kako bi se identificirale ranjivosti i manipulativna ponašanja te sukladno tome primijenile preventivne mjera za ublažavanje negativnih efekata, čime se štiti integritet usluga. Manipulativna ponašanja podrazumijevaju postupke kao što su: stvaranje i korištenje lažnih računa, preuzimanje računa drugih korisnika te amplifikacija vidljivosti sadržaja (dezinformacija) koje pokreću botovi; lažno predstavljanje i zlonamjerni *deep fake* sadržaj; netransparentne plaćene reklamne poruke ili promocija dezinformirajućeg sadržaja od strane influencera; bilo koje ponašanje korisnika usmjereno na umjetno povećanje dosega ili percipirane javne podrške dezinformacijama.

Konačno, kao jednu od ključnih skupina mjera za suzbijanje dezinformacija predviđa se osna-

živanje korisnika, istraživača i zajednice za provjeru točnosti informacija. Potpisnici Kodeksa time se obvezuju da će promicati medijsku pismenost kreirajući alate koji omogućavaju korisnicima kritičko promišljanje u svezi s objavljenim sadržajima, organizirajući kampanje za podizanje svijesti o dezinformacijama, dijeliti kvantitativne informacije relevantne za prikaz učinaka kampanja koje organiziraju ili podržavaju te surađivati sa stručnjacima iz područja medijske pismenosti. Nadalje, u svrhu osnaživanja korisnika, potpisnici se obvezuju implementirati "siguran dizajn" arhitekture usluga koji umanjuje rizik od širenja dezinformacija implementirajući sigurnosne mjere prilikom uspostave njihovih informacijskih sustava i politika njihova korištenja. To, između ostalog uključuje, redovito izvještavanje o implementiranim sustavima za otklanjanja rizika, dostupnim alatima, procedurama, načinu upravljanja sustavima za preporučivanje sadržaja te procjene njihove učinkovitosti. Prilikom kreiranja i nuđenja alata koji korisnicima služe za prepoznavanje dezinformacija potpisnici su dužni raditi na uklanjanju jezičnih barijera te uvođenju funkcionalnosti koji omogućavaju označavanja štetnih, lažnih i/ili pogrešnih informacija. Također, potrebno je uspostaviti transparentan žalbeni mehanizam koji korisnicima omogućava uvid i pokretanje žalbenog postupka u svezi s postupanjem u pogledu sadržaja protiv kojeg je poduzeta neka radnja (uklanjanje korisničkih računa, uklanjanje sadržaja, demonetizacija i slično). Nadalje, predviđene su i mjere za suzbijanje dezinformacija u aplikacijama za slanje poruka kojima se potiče kritičko promišljanje korisnika tih aplikacija te osnaživanje znanstvene i *fact-checking* zajednice koja djeluje prema IFCN Kodeksu.

Uz sve navedene obveze i mjere na koje se potpisnici Kodeksa obvezuju, ovdje je bitno istaknuti da je za pružatelje usluga pristupanje Kodeksu dobrovoljno, ali se u skladu s Uvodnom izjavom 104 DSA, koja navodi da ako pružatelj internetske platforme ili internetske tražilice odbije poziv Komisije na primjenu takvog kodeksa ponašanja bez odgovarajućeg objašnjenja, odbijanje pristupanja kodeksu može se, prema potrebi, uzeti u obzir pri utvrđivanju jesu li internetska platforma ili internetska tražilica povrijedile obveze utvrđene DSA-om. Činjenica da se sudjeluje u određenom kodeksu ponašanja i da se on provodi, sama po sebi ne bi smjela pretpostavljati automatsku usklađenost s DSA. Također, uzimajući u razmatranje i odredbu članka 35 DSA koja govori o razumnim, razmjernim i djelotvornim mjerama za smanjenje rizika za VLOP i VLOSE, te u stavku 1(h) navodi kao jednu od mjera "suradnju s drugim pružateljima internetskih platformi ili internetskih tražilica na temelju kodeksa ponašanja i kriznih protokola iz članka 45 DSA", jasno se može zaključiti da (posebice za VLOP i VLOSE) postoji snažan poticaj pristupanju Kodeksu u svrhu postizanja bolje usklađenosti s DSA i implementacijom mjera za umanjenje sistemskih rizika.

2.4. Provedbeni propis DSA

U travnju 2025 godine, nakon značajnog kašnjenja u Republici Hrvatskoj usvojen je Zakon o provedbi Akta o digitalnim uslugama[6] (dalje u tekstu: ZPDSA). Glavne odrednice ZPDSA su utvrđivanje Koordinatora za digitalne usluge (Hrvatska regulatorna agencija za mrežne djelatnosti) te utvrđivanje nadležnih tijela za izdavanje naloga za djelovanje protiv nezakonitog sadržaja i naloga za davanje informacija pružateljima usluga posredovanja u članku 6. ZPDSA a to su:

1. Državno odvjetništvo i Ministarstvo unutarnjih poslova za nezakoniti sadržaj koji predstavlja kazneno djelo i prekršaj.
2. Agencija za zaštitu osobnih podataka za nezakoniti sadržaj koji predstavlja povredu propisa kojima je uređena zaštita osobnih podataka. (AZOP je također i tijelo nadležno

[6] Zakon o provedbi Uredbe (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama) (Narodne novine br. 67/2025)

za transparentnost sustava za preporučivanje i zaštitu maloljetnika na internetu prema čl. 7. ZPDSA).
3. Carinska uprava Ministarstva financija za nezakoniti sadržaj koji predstavlja povredu prava intelektualnog vlasništva.
4. Državni inspektorat za nezakoniti sadržaj koji predstavlja povredu propisa iz djelokruga inspekcija Državnog inspektorata, u skladu s ovlastima određenim posebnim propisima.
5. Ministarstvo zdravstva za nezakonit sadržaj koji predstavlja povredu iz područja zdravstva, lijekova, medicinskih proizvoda i biomedicine, u skladu s ovlastima određenim posebnim zakonom.
6. Agencija za elektroničke medije za nezakoniti sadržaj koji predstavlja povredu iz područja elektroničkih medija, u skladu s ovlastima određenim posebnim propisima.
7. Druga tijela u skladu s ovlastima određenim posebnim zakonima kojima se uređuje njihov djelokrug

Nalozi koje izdaju gore navedena tijela se izriču na hrvatskom jeziku uz prevođenje elemenata iz članka 9. stavka 2. točaka a) i b) DSA za djelovanje protiv nezakonitog sadržaja te prevođenje elemenata iz članka 10. stavka 2. točaka a) i b) DSA u slučaju naloga za davanje informacija i to na jezik koji je odredio pružatelj usluge posredovanja ili jezik koji je bilateralno naveden. U skladu s DSA, navedene naloge nadležna tijela mogu izdavati ne samo pružateljima usluga posredovanja sa sjedištem u Republici Hrvatskoj, već i pružateljima čiji je poslovni nastan u drugim državama članicama Europske unije, dok o prigovoru protiv izdanih naloga nadležnih tijela u RH odlučuje Općinski prekršajni sud u Zagrebu rješenjem a protiv kojeg se može podnijeti žalba Visokom prekršajnom sudu Republike Hrvatske.

Nadalje, prema ZPDSA korisnici imaju mogućnost podnošenja pritužbe protiv pružatelja usluga posredovanja nadležnim tijelima ako smatraju da je došlo do povrede odredbi DSA. O podnesenim pritužbama odlučuje HAKOM kao koordinator za digitalne usluge (članak 4. ZPDSA), odlukom protiv koje se može pokrenuti upravni spor (članak 14. ZPDSA). Ovdje je važno napomenuti kako su koordinatori za digitalne usluge, temeljem DSA, nadležni isključivo za utvrđivanje postupa li platforma u skladu s obvezama DSA, ne ulazeći pritom u sam sadržaj koji se nalazi na platformi ni u ispravnost odluke platforme kojom je primjerice primatelju onemogućen pristup informacijama ili mu je suspendirano ili ukinuto pružanje usluga. Također, jedna od ključnih odrednica, posebice u kontekstu borbe protiv nezakonitih/štetnih sadržaja u skladu s DSA je uspostava instituta pouzdanih prijavitelja pri čemu HAKOM ima obvezu donijet pravilnik o kriterijima i načinu dodjeljivanja, suspendiranja ili opozivanja statusa pouzdanog prijavitelja (članak 5(3) ZPDSA). U pogledu obveza pružatelja usluga posredovanja ZPDSA obvezuje pružatelje usluga posredovanja s poslovnim nastanom u RH dostaviti HAKOM-u obavijest o pružanju usluga. HAKOM ima obvezu u roku od mjesec dana od stupanja na snagu ZPDSA na svojoj mrežnoj stranici objaviti detaljne informacije o načinu podnošenja takve obavijesti, a rok za podnošenje je 3 mjeseca od objave spomenute informacije. Prekršajnim odredbama ZPDSA definirane su novčane kazne za pružatelje usluga posredovanja koje se kreću od 6.630,00 do 66.360,00 eura ili u iznosu do 6 % godišnjeg svjetskog prihoda dotičnog pružatelja usluga posredovanja u prethodnoj financijskoj godini, ovisno o tome koji iznos je veći. Također, za fizičke osobe-obrtnike zakon propisuje novčane kazne u iznosu od 1.320,00 do 6.630,00 eura.

3. Europski Akt o slobodi medija

U kontekstu borbe protiv dezinformacija svakako je potrebno razmotriti i pojedine odredbe Europskog Akta o slobodi medija (EMFA) kao jednog od ključnih dokumenata kojim se želi urediti fragmentirana nacionalna zakonodavstva država članica a koja uređuju djelovanje medija te su povezani s medijskim slobodama,

pluralizmom medija te uređivačkom neovisnošću. Donošenjem EMFA-e uspostavlja se bolje funkcioniranje unutarnjeg tržišta medijskih usluga te sprječava nastanak prepreka za rad pružatelja medijskih usluga u EU. Tako se kao neki od najvažniji ciljeva EMFA-e mogu izdvojiti zaštita uredničke neovisnosti, zaštita novinarskih izvora (među ostalim od uporabe špijunskog softvera), neovisno funkcioniranje javnih medija, povećana transparentnost vlasništva nad medijima, pružanje zaštitnih mjera u situacijama kad velike internetske platforme neopravdano uklanjaju medijski sadržaj, uvesti pravo prilagodbe medijske ponude na uređajima i sučeljima platformi, transparentnost državnog oglašavanja za pružatelje medijskih usluga i internetskih usluga, dostavu procjene učinka koncentracija na medijskom tržištu na medijski pluralizam i uredničku neovisnost te povećanje transparentnost mjerenja gledanosti publike za pružatelje medijskih usluga i oglašivače. Od tih ciljeva nekih se posebno ističu u kontekstu borbe protiv dezinformacija. Prvi od njih je osiguranje pristupa pluralističkom medijskom okruženju što uključuje transparentnost vlasništva i nadzor nad koncentracijama na medijskom tržištu, te se člankom 3. EMFA-e uređuje da "države članice poštuju pravo primatelja medijskih usluga na pristup pluralnosti uredički neovisnog medijskog sadržaja i osiguravaju uspostavu okvirnih uvjeta u skladu s ovom Uredbom kako bi se to pravo zaštitilo, u korist slobodnog i demokratskog diskursa." Nepoštivanje navedene odredbe promatra se kao oblik mogućeg kršenja obveza iz TFEU od strane država članica. Nadalje, uvodna izjava 14 EMFA-e ukazuje na nužni pluralizam sadržaja kada su u pitanju vijesti i aktualni događaji, kao i na kvalitetu novinarstva kao protutežu dezinformacijama. Sljedeći cilj koji se može istaknuti u kontekstu borbe protiv dezinformacija je pravo prilagodbe medijskog sadržaja i ograničenja u pogledu dizajniranja korisničkog sučelja. Tako se člankom 20. EMFA-e nameće obveza proizvođačima, developerima i uvoznicima da omoguće korisnicima da ponudu medijskih usluga prilagode svojim interesima ili preferencijama u skladu s pravom Unije. Time bi korisnici trebali imati pravo jednostavno promijeniti konfiguraciju, uključujući zadane postavke svakog uređaja ili korisničkog sučelja kojima se kontrolira pristup medijskim uslugama koje pružaju programe i njihovo korištenje, odnosno kojima se upravlja pristupom takvim uslugama i njihovim korištenjem. Istovremeno, vizualni identitet pružatelja usluga medija kojima se pristupa putem uređaja ili nekog sučelja dosljedno mora biti jasno vidljiv svim korisnicima. Navedena odredba ima namjeru osnažiti korisnike da sami odabiru izvore informacija i informiraju se, te da samostalno donose odluke o sadržaju koji konzumiraju (i na taj način određuju kako oblikuju svoje mišljenje). Za borbu protiv dezinformacija također je bitno jasno urediti odnose između platformi koje distribuiraju medijski sadržaj i samih medija koji su korisnici tih platformi. Naime, platforme igraju ključnu ulogu u online distribuciji sadržaja i imaju značajnu ulogu u prenošenju informacija do krajnjih korisnika. To predstavlja izazov za distribuciju medijskih sadržaja u svim medijskim sektorima a posebno kada su u pitanju mediji s manjim dosegom (radio i tisak). Tako EMFA uključuje odredbu koja uređuje objavu sadržaja pružatelja medijskih usluga na VLOP-ima, pri čemu VLOP-i moraju uspostaviti mehanizam koji omogućuje pružateljima medijskih usluga da se identificiraju kao takvi. Ako pružatelj medijskih usluga izjavi da zadovoljava određene kriterije koji se u biti odnose na njihovo kvalificiranje kao „kvalitetne medije" (u skladu s člankom 18. EMFA-e), VLOP-ovi njihov sadržaj mora tretirati preferirano pri moderiranju sadržaja. Izjava pružatelja medijskih usluga podrazumijeva da poštuje određene utvrđene kriterije koji uključuju transparentnost vlasništva i financiranja, uredničku neovisnost, neovisnost od država članica, političkih stranaka, trećih zemalja i subjekata koje kontroliraju ili financiraju treće zemlje, obavljanje djelatnosti pružanja medijskih usluga u skladu s regulatornim zahtjevima, te izostanak objave sadržaja koji su generirali sustavi umjetne inteligencije bez podvrgavanja istog ljudskom pregledu

ili uredničkoj kontroli. Kada su zadovoljeni svi predviđeni kriteriji te se prihvati izjava pružatelja medijske usluge od strane VLOP-a, u slučaju da VLOP namjerava ograničiti pristup određenom sadržaju predmetnog pružatelja medijske usluge (blokirati ili ograničiti) dužan ga je o tome obavijestiti te mu dati obrazloženje za uvođenje ograničenja. Također, pružatelju medijskih usluga se u tom slučaju daje mogućnost za dostavljanje vlastitog mišljenja u odnosu na predviđeno ograničenje, te je predviđen rok za mirovanje od 24 sata u kojem VLOP zastaje s moderiranjem sadržaja predmetnog pružatelja medijske usluge. Sve pritužbe pružatelja medijskih usluga na moderiranje od strane VLOP-a moraju biti obrađene prioritetno i bez odgađanja. Razlog za uvođenje preferencijalnog tretmana za pružatelje medijskih usluga u odnosu na VLOP-e je da njihovo poslovanje već podliježe regulativnom okviru za medije (npr. AVMSD) te u pojedinim područjima samoregulativnim i koregulativnim aktima, pa se u slučaju dodatnog moderiranja sadržaja od strane VLOP-a istovremeno suočavaju s još jednim dodatnim slojem nadzora od strane platformi po pitanju diseminacija njihovog sadržaja online. Ovakav pristup preferencijalnog tretiranja sadržaja pružatelja medijskih usluga također doprinosi borbi protiv dezinformacija jer se promiče i štiti objava sadržaja iz "pouzdanih" izvora.

Konačno, može se reći da EMFA ima za cilj djelovati unutar šireg sustava europskih inicijativa koje su osmišljene za jačanje borbe protiv dezinformacija i provjere objavljenih informacija. Odnos između EMFA-e i pojedinih uspostavljenih standarda za provjeru točnosti informacija (kao npr. standarde EFCSN-a) posebno je važan jer je pravna zaštita koju pruža EMFA najučinkovitija kada se primjenjuje na organizacije koje zadovoljavaju visoke profesionalne standarde. Uspostavljeni standardi za provjeru objavljenih informacija zahtijevaju od provjeravatelja informacija da budu transparentni u vezi sa svojim izvorima financiranja, otkrivaju potencijalne sukobe interesa i slijede stroge metodološke pristupe provjere što je u bliskoj vezi sa standardima koje nameće EMFA u pogledu transparentnosti i uredničke neovisnosti. Tako se usvajanjem EMFA-e kreira okvir koji jača pravnu zaštitu za pružatelje medijskih usluga i provjeravatelje informacija ali ujedno naglašava i potreba za implementacijom profesionalnih standarda.

4. Direktiva o audiovizualnim medijskim uslugama

Direktiva o audiovizualnim medijskim uslugama (AVMSD), revidirana je 2018. te uspostavlja ključni okviri za regulaciju audiovizualnog medijskog sadržaja, uključujući odredbe koje izravno i neizravno podržavaju rad provjeravatelja informacija. U RH, AVMSD je implementirana putem Zakona o elektroničkim medijima[7] iz 2021. godine (dalje u tekstu: ZEM). Kako su odredbe AVMSD o kojima se ovdje raspravlja implementirane u hrvatski zakonodavni okvir u svom izvornom obliku, rasprava o pojedinim odredbama AVMSD se istovjetno odnosi i na odgovarajuće odredbe iz ZEM-a.

Značajna promjena u zakonodavnom okviru za elektroničke medije dogodila se revizijom AVMSD-a 2018. uvođenjem odredbi koje reguliraju platforme za dijeljenje video sadržaja (dalje u tekstu: VSP). Člankom 28(a)(b) AVMSD, (članak 96. ZEM) uvode se obveze za VSP-ove koje podrazumijevaju transparentnost postupanja povodom prigovora u svrhu adresiranja štetnih sadržaja što uključuje i dezinformacije. Sada su VSP-ovi dužni uspostaviti mehanizme koji korisnicima omogućavaju prijavu nezakonitog ili štetnog sadržaja, dati objašnjenje u slučaju uklanjanja pojedinog sadržaja te omogućiti osporavanje donesene odluke te surađivati sa provjeravateljima informacija u pogledu sadržaja koji je prijavljen kao nezakonit ili štetan. Nadalje, VSP-ovi moraju implementirati mjere za zaštitu maloljetnika u pogledu sadržaja koji

[7] Zakon o elektroničkim medijima (Narodne novine br. 111/2021)

bi mogao naštetiti njihovom razvoju (sustavi za provjeru dobi korisnika), redovito uklanjati sadržaj koji potiče na mržnju ili nasilje te jasno označavati komercijalne komunikacije u svrhu sprječavanja širenja obmanjujućeg sponzoriranog sadržaja.

U odnosu na sve pružatelje audiovizualnih medijskih usluga, važne odredbe AVMSD-a koje se ovdje mogu izdvojiti u kontekstu borbe protiv dezinformacija su odredbe koje se odnose na transparentnost vlasništva i odgovornost pružatelja usluga. Tako se člankom 5. AVMSD (članak 13. ZEM), nalaže svim pružateljima audiovizualnih medijskih usluga objava kontaktnih podataka te informacija o vlasničkoj strukturi pružatelja medijskih usluga. To pomaže provjeravateljima informacija da lakše identificiraju potencijalne pristranosti ili sukobe interesa koji stoje iza dezinformacijskih kampanja ili objavljenog sadržaja. Nadalje, AVMSD u članku 4.a (članak 12 ZEM) potiče koregulativne i samoregulativne inicijative uređene kodeksima ponašanja koji značajno mogu doprinijeti i borbi protiv dezinformacija. U pogledu teritorijalne nadležnosti za provedbu AVMSD-a primjenjuje se načelo "zemlje porijekla". To podrazumijeva da su pružatelji usluga u nadležnosti regulatornih tijela one države članice u kojoj imaju poslovni nastan. Izuzeće od tog pravila predstavlja nadležnost Europskog odbora za medijske usluge (osnovan temeljem EMFA-e) da posreduje i omogući prekograničnu suradnju nadležnih tijela kako bi se spriječile dezinformacijske kampanje koje se protežu kroz više jurisdikcija (država članica). Također, države članice prema članku 3. AVMSD (članak 91. ZEM) imaju pod određenim uvjetima mogućnost derogacije načela zemlje porijekla u slučajevima kada audiovizualne medijske usluge koje dolaze iz druge države članice Europske unije očito, ozbiljno i teško krše odredbe članka 14. stavka 2. ZEM-a (govor mržnje) i članka 24. stavaka 2. i 3. ZEM-a (nezakoniti sadržaj, zaštita maloljetnika) ili se dovodi u pitanje javno zdravlje ili predstavlja ozbiljan i težak rizik od dovođenja javnog zdravlja u pitanje. Konačno, nametnutom obvezom promocije europskih djela AVMSD i ZEM promiču raznovrsnost medijskog sadržaja te se time neizravno suprotstavljaju jednoobraznim narativima koji također mogu biti podloga za promicanje dezinformacija.

Prilikom razmatranja pojedinih odredbi AVMSD-a bitno je istaknuti da iako se AVMDS odnosi i primjenjuje na pružatelje audiovizualnih medijskih usluga te na VSP-ove (*lex specialis*) potrebno ga je tumačiti u kontekstu cjelokupnog regulatornog okvira te uzeti u obzir i pojedine odredbe općih propisa DSA i EMFA-e koje su primjenjive na sve pružatelje medijskih usluga pa tako i na pružatelje audiovizualnih medijskih usluga i VSP-ove.

5. Smjernice Vijeća Europe

Uz prethodno razmatranje relevantnog zakonodavnog okvira za borbu protiv dezinformacija ovdje je potrebno razmotriti i smjernice Vijeća Europe naziva "Smjernice o suzbijanju širenja online dezinformacija i misinformacija kroz provjeru činjenica i rješenja dizajna platforme na način usklađen s ljudskim pravima"[8] (dalje u tekstu: Smjernice). Iako Smjernice ne spadaju u zakonodavni okvir, te nisu obvezujuće, one predstavljaju cjelovit dokument koji se bavi mehanizmima za sprječavanje širenja misinformacija i dezinformacija te je namijenjen širokoj publici uključujući donositelje politika (zakonodavce), platforme, novinske organizacije i osobe koje provjeravaju činjenice, zalažući se za transparentnost, neovisnost i osnaživanje korisnika. Smjernice detaljno opisuju izazove i najbolje prakse u provjeri činjenica, dizajnu platformi i obrazovanju korisnika, dok se istovremeno naglašava nužnost medijskog pluralizma i zaštita ranjivih skupina. Dokument ima za cilj poticati zdrav medijski ekosustav u kojem se korisnici mogu kritički baviti internetskim sa-

[8] Dostupno na https://edoc.coe.int/en/internet/11885-guidance-note-on-countering-the-spread-of-online-mis-and-disinformation-through-fact-checking-and-platform-design-solutions-in-a-human-rights-compliant-manner.html.

držajem i pridonijeti informiranom javnom diskursu te se napori u borbi protiv misinformacija i dezinformacija usmjeravaju na rješavanje mehanizama koji brzo povećavaju razmjere i opseg dezinformacija te na povećanje uočljivosti i otkrivanja točnih informacija iz pouzdanih izvora.

Dokument se temelji na tri glavna stupa: provjeri točnosti informacija, rješenjima za dizajn platforme i osnaživanju korisnika.

Prvi stup bavi se centralnom ulogom provjere činjenica (i provjeravatelja informacija) te naglašava njihovu ključnu ulogu za osiguravanje "zdrave" javne rasprave. Pri tome je nužno voditi računa o bitnim karakteristikama postupka provjere informacija i provjeravatelja informacija, a što uključuje: transparentnost kao ključnu osobinu za neovisnost osoba koje provjeravaju činjenice, s fokusom na financiranje, unutarnju organizaciju i kontrolu kvalitete; neovisnost koja jamči uredničke slobode i neovisnost osoba koje provjeravaju činjenice; financiranje koje treba osigurati i raspodijeliti na temelju zaštitnih mjera koje jamče neovisnost; povjerenje korisnika u provjeru točnosti informacija temeljeno na učinkovitosti; te kontroli kvalitete pri čemu osobe koje provjeravaju činjenice trebaju provoditi robusne i transparentne procese kontrole.

Drugi stup bavi se dizajnom platformi koji omogućava zdravo informacijsko okruženje. Pri tome bi same platforme trebale: baviti se načinom na koji njihovi algoritmi mogu promicati pogrešne informacije i dezinformacije; dizajnirati svoje usluge na način da se promiču i štite ljudska prava; uključiti sigurnost u svoje odluke o dizajnu posebice kada su u pitanju sustavi umjetne inteligencije; osigurati transparentnost usluga, politika i načina njihove provedbe; te konačno, osigurati učinkovite mehanizme pravne zaštite.

Treći stup bavi se osnaživanjem korisnika u borbi protiv dezinformacija te se temelji na uspostavi zdravog medijskog ekosustava koji zahtjeva stalnu opskrbu kvalitetnim informacijama iz pouzdanih izvora. Osnaživanje korisnika također podrazumijeva: jačanje sposobnosti korisnika da prepoznaju pouzdane izvore i propituju misinformacije i dezinformacije; promicanje prava korisnika te dostupnost informacija o mehanizmima zaštite; zaštitu ranjivih skupina; suradnju između državnih tijela, civilnog društva, platformi i medija; razvoj i dostupnost digitalnih alata koji pospješuju otkrivanje dezinformacija; sveobuhvatne strategije medijske pismenosti te reformu obrazovanja koja podrazumijeva uključivanje vještina koje korisnicima omogućuju da se zaštite od dezinformacija.

Zaključno, može se reći da Smjernice naglašavaju pristup suzbijanju dezinformacija koji uključuje sve dionika, te naglašavaju potrebu za transparentnošću, neovisnošću i suradnjom, osiguravajući da poduzete mjere ne krše temeljna prava poput slobode izražavanja.

6. Zaključak

Borba protiv dezinformacija u digitalnom okruženju zahtijeva sveobuhvatan, višeslojan i pravno precizan pristup koji ujedno balansira između zaštite temeljnih prava građana, slobode izražavanja i potrebe za suzbijanjem štetnog i nezakonitog sadržaja. Europska unija kroz Akt o digitalnim uslugama (DSA), Europski akt o slobodi medija (EMFA) i Direktivu o audiovizualnim medijskim uslugama (AVMSD), uspostavlja robustan zakonodavni okvir koji obuhvaća sve ključne aspekte digitalnih i medijskih usluga, a posebno naglašava transparentnost, odgovornost i suradnju između platformi, medija i neovisnih provjeravatelja informacija. Pri tome, DSA kao opći propis, donosi jasna pravila za otkrivanje, označavanje i uklanjanje nezakonitih sadržaja i dezinformacija, uvodi mehanizme za prijavu sumnjivog sadržaja, status pouzdanih prijavitelja i obvezu procjene rizika za vrlo velike internetske platforme i tražilice. Dodatno, integracija Kodeksa dobre prakse u suzbijanju dezinformacija u regulatorni okvir DSA osigurava strožu provedbu mjera, posebice u

domeni demonetizacije dezinformacija, transparentnosti političkog oglašavanja i osnaživanja korisnika za kritičko promišljanje. EMFA dodatno jača pluralizam, uredničku neovisnost i transparentnost vlasništva nad medijima, a posebne odredbe usmjerene su na preferencijalni tretman pouzdanih medijskih izvora na platformama, čime se štiti kvalitetno novinarstvo i smanjuje prostor za širenje dezinformacija. AVMSD i nacionalni zakonodavni okvir (ZEM) obvezuju pružatelje audiovizualnih medijskih usluga i platforme za dijeljenje video sadržaja na transparentnost, odgovornost i suradnju s provjeravateljima informacija, uz posebne mjere za zaštitu maloljetnika i sprječavanje širenja govora mržnje i obmanjujućeg sadržaja. Smjernice Vijeća Europe dodatno naglašavaju važnost transparentnosti, neovisnosti, edukacije korisnika i multidisciplinarnu suradnju svih dionika u borbi protiv dezinformacija, uz stalno poštivanje ljudskih prava i slobode izražavanja. Kada sve prethodno promatramo sumarno, možemo zaključiti da učinkovit odgovor na izazove u borbi protiv dezinformacija temeljimo na:

- jasnom i provedivom zakonodavnom okviru,
- transparentnosti i odgovornosti svih dionika,
- jačanju kapaciteta neovisnih provjeravatelja informacija,
- poticanju medijske pismenosti i osnaživanju korisnika,
- te kontinuiranoj suradnji između regulatornih tijela, platformi, medija, civilnog društva i akademske zajednice.

Ovakav pristup omogućuje uspostavu pluralističkog sustava medijskih usluga i platformi koji štiti demokratske procese i osigurava da borba protiv dezinformacija ne ugrozi temeljna prava građana.

Odgovornost za štetu – u predmetima za naknadu štete zbog povrede prava osobnosti objavljenom informacijom u medijima kroz sudsku praksu

Perica Norac-Kevo
sutkinja Županijskog suda u Velikoj Gorici

1. Uvod

Temeljna pretpostavka slobode izražavanja u demokratskom društvu je sloboda medija. Sloboda izražavanja je jedno od temeljnih prava građanina jer bez nje nema ni demokracije, time što ona omogućuje suprotstavljanje mišljenja, ona utire put plodonosnim sintezama koje su korak naprijed na putu društvenog napretka. Pravo na slobodu izražavanja, kao jedno od temeljnih ljudskih prava, sudska praksa deklarira kao temelj demokratskog društva i jedan od preduvjeta njegova napretka i razvoja svakog pojedinca.

Pravna shvaćanja sudova u Republici Hrvatskoj u suglasju su sa shvaćanjem Europskog suda za ljudska prava (dalje u tekstu: ESLJP) te je sastavni dio obrazloženja sudskih odluka pravno shvaćanje da sloboda izražavanja predstavlja jedno od temeljnih načela demokratskog društva i jedan od osnovnih uvjeta za njegov napredak i za ispunjenje svakog pojedinca. Pravo na slobodu izražavanja odnosi se ne samo na „informacije“ ili „ideje“ koje su blagonaklono prihvaćene ili se ne smatraju uvredljivima ili ne izazivaju nikakvu reakciju, nego i na one koje vrijeđaju, šokiraju ili uznemiruju. To zahtijevaju pluralizam, tolerancija i slobodoumlje bez kojih nema demokratskog društva.

Međutim, pravo na slobodu izražavanja nije apsolutno pravo. U brojnim odlukama Ustavnog suda Republike Hrvatske izraženo je pravno shvaćanje da ustavom zajamčena sloboda mišljenja i izražavanja misli, koja u sebi sadrži i slobodu primanja i širenja informacija, nema značenje apsolutne slobode, već je podložna ograničenjima propisanim Ustavom i zakonom da bi se zaštitila prava i interesi drugih (*npr. odluka U-I-884/1997 od 3. veljače 2000., U-III-1810/2004 od 20. rujna 2006. i U-II-593/1997 od 14. ožujka 2001.*).

Drugim riječima, pravo na slobodu izražavanja ne isključuje dužnost i odgovornost, među ostalim i radi zaštite prava drugih, i može biti ograničeno, ako je to nužno u demokratskom društvu. No, ta ograničenja moraju biti strogo tumačena i moraju imati legitiman cilj koji se očituje u zaštiti ustavnih i konvencijskih prava drugih. Ovo stoga, jer s jedne strane imamo medijsku slobodu izražavanja, a s druge strane pravo pojedinca na zaštitu časti, ugleda, dostojanstva i privatnosti, koja prava su prava jednake vrijednosti i zaslužuju jednaku zaštitu.

Pravo na slobodu izražavanja kao općeprihvaćeni standard demokratskog društva i temeljno pravo u sebi uključuje pravo, a i dužnost medija da prikupljaju i objavljuju točne, potpune i provjerene informacije kao i pravo građana da takve informacije prime.

U smislu rečenog sloboda medija ne smije prekoračiti određene granice, posebice kada se tiče zaštite ugleda i prava drugih, gdje ni osnovni zadatak priopćavanja informacija o pitanjima od javnoga interesa ne smije preći te granice. Ovo stoga, jer je sloboda medija uvjetovana i postupanjem novinara u dobroj vjeri u skladu s novinarskom etikom (*ESLJP u predmetima Stoll protiv Švicarske, br. 69698/01, § 103., presuda od 10. prosinca 2007. i Pedersen i Baadsgaard protiv Danske br. 49017/99, § 78., presuda od 17. prosinca 2004.*).

Iako sloboda medija ne smije prekoračiti određene granice, posebice kada se tiče zaštite ugleda i prava drugih, ne smije se smetnuti s uma da je njezin osnovni zadatak priopćiti - na način koji je u skladu s njihovim obvezama i odgovornostima - informacije i ideje o svim pitanjima od javnoga interesa. Ne samo da mediji imaju zadatak priopćavati informacije i ideje od javnog interesa, već ih javnost ima pravo i dobiti. Stoga je ključna uloga medija olakšavanje i osnaživanje prava javnosti da prima informacije i ideje. Kada ne bi bilo tako, mediji ne bi bili u mogućnosti ostvariti svoju ulogu "psa čuvara demokracije" (*ESLJP u predmetima Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske, [Vv], br. 931/13, presuda od 27. lipnja 2017, §§ 125. i 126. i Magyar Helsinki Bizottság protiv Mađarske [Vv], br. 18030/11, § 165., presuda od 8. studenoga 2016.*).

Takva uloga u demokratskom društvu slijedi iz primjera u kojima su u otkrivanju i suzbijanju organiziranog kriminala, zlouporabe vlasti, korupcije, kršenja temeljnih prava i ekstremizma ključnu ulogu imali upravo istraživački novinari.

Iako je u današnje vrijeme jasno da je razvoj komunikacijske tehnologije doveo do toga da svatko može širiti informacije, a demokracija je dovela do toga da se svakom jamči sloboda izražavanja, ipak samo mediji imaju posebno važnu ulogu u odnosu na pravo na slobodu izražavanja.

U ovom tekstu iznijet će se zakonodavni okvir odgovornosti za štetu u predmetima za naknadu štete uslijed povrede prava osobnosti objavljenom informacijom, te dati sažeti prikaz kriterija prema kojima sud, načelno ocjenjuje, je li u konkretnom slučaju postignuta ili je prekoračena pravična ravnoteža između sukobljenih prava – prava na slobodi izražavanja i prava na čast, ugled, dostojanstvo i privatnost - te će se iznijeti recentna sudska praksa sudova u Republici Hrvatskoj, Suda Europske unije i Europskog suda za ljudska prava u kojoj su zauzeta pravna shvaćanja pri odgovaranju na pitanje koje od sukobljenih prava preteže u pojedinom konkretnom slučaju i kojemu od njih je potrebno pružiti zaštitu.

2. Zakonodavni okvir

Ustav Republike Hrvatske („Narodne novine", broj 56/90, 135/97, 113/00, 28/01, 76/10 i 5/14-dalje u tekstu: Ustav). Jamstvo slobode mišljenja i izražavanja misli uređeno je čl. 38. Ustava. U Ustavu sloboda izražavanja obuhvaća osobito: slobodu tiska i drugih sredstava priopćavanja, slobodu govora i javnog nastupa, slobodu osnivanja svih ustanova javnog priopćavanja. Ustav izrijekom zabranjuje cenzuru, a novinarima jamči pravo na slobodu izvještavanja i pristupa informaciji. Ustav svakomu jamči pravo na ispravak, ako mu je javnom viješću povrijeđeno Ustavom i zakonom utvrđeno pravo.

Ograničenje Ustavnog prava na slobodu izražavanja sadržano je u čl. 16., ali samo ako je ograničenje propisano zakonom, i to radi zaštite slobode i prava drugih ljudi te pravnog poretka, javnog morala i zdravlja.

Uz slobodu izražavanja treba povezati i čl. 35. Ustava kojim je određeno da se svakomu jam-

či štovanje i pravna zaštita njegovog osobnog i obiteljskog života, dostojanstva, ugleda i časti.

Opća deklaracija o ljudskim pravima („Narodne novine“, Međunarodni ugovori, broj 12/2009- dalje u tekstu: Opća deklaracija) usvojena i proglašena na Općoj skupštini UN, rezolucijom 217A(III) 10. prosinca 1948.

Povelja Europske unije o temeljnim pravima (Službeni list Europske unije, C 202/389- dalje u tekstu: Povelja).

Pravo na slobodu izražavanja sadržano je u čl. 19. Opće deklaracije o ljudskim pravima, a sadrži ga i Povelja Europske unije o temeljni pravima u čl. 11.

Prema odredbi čl. 19. svatko ima pravo na slobodu mišljenja i izražavanja; to pravo uključuje slobodu zadržavanja mišljenja bez uplitanja i slobodu traženja, primanja i širenja informacija i ideja putem bilo kojeg medija i bez obzira na granice.

Odredba čl. 11. Povelje jamči pravo na slobodu izražavanja, koje uključuje slobodu mišljenja te primanja i širenja informacija i ideja bez miješanja tijela javne vlasti i bez obzira na granice ukazujući na imperativ poštivanja slobode i pluralizma medija.

I prema Povelji pravo na slobodu izražavanja nije apsolutno. Ograničenja su dopuštena pod uvjetom da su propisana zakonom, poštuju bit prava, proporcionalna legitimnim ciljevima.

(Europska) Konvencija za zaštitu ljudskih prava i temeljnih sloboda („Narodne novine“- Međunarodni ugovori, broj 18/97, 6/99 – pročišćeni tekst, 8/99 – ispravak, 14/02, 13/03, 9/05, 1/06, 2/10 i 13/17-dalje u tekstu: Konvencija).

Sastavni dio pravnog poretka Republike Hrvatske čini i Konvencija zajedno sa svim Protokolima koje je Republika Hrvatska ratificirala. Slobodu izražavanja određuje čl. 10. Konvencije, prema kojem svatko ima pravo na slobodu izražavanja, što obuhvaća slobodu mišljenja i slobodu primanja i širenja informacija i ideja bez miješanja javne vlasti i bez obzira na granice. Iako konvencijsko i univerzalno priznato pravo, ono može biti podvrgnuto formalnostima, uvjetima, ograničenjima ili kaznama propisanim zakonom, koji su u demokratskom društvu nužni radi interesa državne sigurnosti, teritorijalne cjelovitosti ili javnog reda i mira, radi sprečavanja nereda ili zločina, radi zaštite zdravlja ili morala, radi zaštite ugleda ili prava drugih, radi sprečavanja odavanja povjerljivih informacija ili radi očuvanja autoriteta i nepristranosti sudbene vlasti.

Uz slobodu izražavanja nužno povezujemo i čl. 8. Konvencije, prema kojem svaka osoba ima pravo na poštovanje svoga privatnog i obiteljskog života, doma i dopisivanja. Ograničenja tog prava moraju biti u skladu sa zakonom i ako je u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira, ili gospodarske dobrobiti zemlje, te radi sprečavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih.

Zakon o medijima (“Narodne novine”, broj 59/04, 84/11, 81/13 i 114/22- dalje u tekstu: ZM).

Zakon o medijima, između ostalog, uređuje pretpostavke za ostvarivanje načela slobode medija, prava novinara i drugih sudionika u javnom informiranju na slobodu izvješćivanja i dostupnost javnim informacijama, ostvarivanje prava na ispravak i odgovor, te prava i obveze drugih pravnih i fizičkih osoba koje djeluju na području javnog informiranja. Odredbe ovoga Zakona primjenjuju se i tumače sukladno Konvenciji i u njega su implementirane odredbe koje su u skladu s Direktivom 2006/123/EZ Europskog parlamenta i Vijeća od 12. prosinca 2006. o uslugama na unutarnjem tržištu (SL L 376, 27. 12. 2006.).

Iako je ZM temeljni zakon koji uređuje slobodu medija, kao i doseg te slobode, u Republici Hrvatskoj je primjena prava iz pravne stečevine EU jednako obvezujuća kao i primjena domaćeg prava.

Odredba čl. 2. ZM-a definira što su mediji, a što nisu mediji.

Prema pozitivnoj definiciji mediji su: novine i drugi tisak, radijski i televizijski programi, programi novinskih agencija, elektroničke publikacije, teletekst i ostali oblici dnevnog ili periodičnog objavljivanja uredničkи oblikovanih programskih sadržaja prijenosom zapisa, glasa, zvuka ili slike.

Prema negativnoj definiciji mediji nisu: knjige, udžbenici, bilteni, katalozi ili drugi nositelji objavljivanja informacija koji su namijenjeni isključivo obrazovnom, znanstvenom i kulturnom procesu, oglašavanju, poslovnoj komunikaciji, radu trgovačkih društava, zavoda i ustanova, udruga, političkih stranaka, vjerskih i ostalih organizacija, školska glasila, »Narodne novine« Republike Hrvatske, službena glasila jedinica lokalne i područne (regionalne) samouprave i ostala službena priopćenja, plakati, letci, prospekti i transparenti, te video stranice bez žive slike i druge besplatne obavijesti, osim ako ovim Zakonom nije drukčije propisano.

Odredbom čl. 3. ZM-a jamči se sloboda izražavanja i sloboda medija, definira se što obuhvaća slobodu medija, kada je dopušteno ograničiti slobodu medija i što je u medijima zabranjeno.

U toj zakonskoj odredbi nalazimo ograničenje slobode medija, koje mora biti nužno u demokratskom društvu i utemeljeno na zakonu te je taksativno navedeno što je to medijima zabranjeno.

Uz jamstvo slobode izražavanja mišljenja te da novinar ima pravo izražavati stajalište o svim događajima, pojavama, osobama, predmetima i djelatnostima (čl. 27. st. 1. ZM), zakon veže uvažavanje zaštite ljudske osobnosti, privatnosti i dostojanstva i ograničenje slobode medija radi zaštite ugleda ili prava drugih.

Zaštita privatnosti dostojanstva, ugleda i časti regulirana je odredbama čl. 7., 8. i 16. ZM-a. Kroz te odredbe ZM propisuje medijima dužnost poštovati privatnost, dostojanstvo, ugled i čast građana, a osobito djece, mladeži i obitelji bez obzira na spol i spolno opredjeljenje. ZM isključuje povredu prava na zaštitu privatnosti ako u pogledu informacije prevladava opravdani javni interes nad zaštitom privatnosti u odnosu na djelatnost novinara ili na informaciju. Ujedno je ograničena razina zaštite privatnosti osobe koja svojim izjavama, ponašanjem i drugim djelima u vezi s njezinim osobnim ili obiteljskim životom sama privlači pozornost javnosti, dok je naglašena dužnost medija na poštovanje prava na zaštitu identiteta svjedoka i oštećenika kaznenih djela, i da bez njihova znanja i pristanka ne smiju otkriti njihov identitet. S druge strane osoba koja obavlja javnu službu ili dužnost ima pravo na zaštitu privatnosti, osim u slučajevima koji su u vezi s javnom službom ili dužnosti koju osoba obavlja.

O povredama prava na slobodu izražavanja i slobodi medija odlučuje sud.

Sudovi sude na temelju Ustava, pravne stečevine Europske unije, međunarodnih ugovora, zakona i drugih važećih izvora prava (čl. 115. st. 3. Ustava i čl. 5. Zakona o sudovima), te činjenica koje proizlaze iz spisa.

Svaki se predmet ispituje na temelju vlastitih činjenica, a utvrđena činjenica mora biti potkrijepljena dokazom, dok teret dokaza, u pravilu, leži na tužitelju. Tuženiku je naravno dopušteno dokazivati suprotno, a snagu dokaza ocjenjuje sud prema svom uvjerenju na temelju savjesne i brižljive ocjene svakog dokaza zasebno i svih dokaza zajedno, a i na temelju rezultata cjelokupnog postupka. Nikakav ni osobni ni vanjski utjecaj ne može biti kriterij na temelju kojeg sud sudi.

Odredba čl. 30. ZM-a, propisuje zaštitu izvora informacije prema kojoj novinar nije dužan dati podatke o izvoru objavljene informacije ili informacije koju namjerava objaviti te propisuje tko, kada i pod kojim uvjetima može naložiti novinaru da iznese podatke o izvoru objavljene informacije ili informacije koju namjerava objaviti.

Odgovornost za štetu i pretpostavke oslobođenja odgovornosti za štetu propisani su odredbom čl. 21. ZM-a, dok je u čl. 40. do čl. 58. propisano pravo na objavljivanje ispravaka i odgovora.

Zakon o elektroničkim medijima („Narodne novine“, broj 111/21 i 114/22).

Odredbe čl. 3. st. 3. i 4. ovog Zakona upućuju na primjenu ZM-a (kada je u pitanju pravo na ispravak objavljene informacije ili na odgovor na objavljenu informaciju) te primjenu Konvencije na odnose uređene ovim Zakonom.

Nakon svih nedoumica u sudskoj praksi u čl. 94. tog Zakona odgovoreno je na pitanje tko je odgovoran za uvredljive komentare objavljene na internetu. Prema stavku 3. tog članka pružatelj elektroničke publikacije odgovoran je za cjelokupni sadržaj objavljen na elektroničkoj publikaciji, uključujući i sadržaj koji generiraju korisnici ako propusti registrirati korisnika i ako nije na jasan i lako uočljivi način upozorio korisnika na pravila komentiranja i na kršenja odredaba iz stavka 2. ovoga članka.

U pogledu zaštite osobnih podataka primjenjuje se Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (**Opća uredba o zaštiti podataka**).

Člankom 85. Opće uredbe o zaštiti podataka dana je mogućnost državama članicama da u vezi s obradom koja se obavlja u novinarske svrhe ili u svrhe akademskog, umjetničkog ili književnog izražavanja, države članice mogu predvidjeti izuzeća ili odstupanja ako su ona potrebna kako bi se uskladilo pravo na zaštitu osobnih podataka sa slobodom izražavanja i informiranja. Riječ je o jednoj od posebnih situacija obrade osobnih podataka, uređenih Poglavljem IX. Opće uredbe.

Kodeks časti hrvatskih novinara (HND, 2009.-dalje u tekstu: Kodeks), sadrži jasne norme novinarskog etičkog kodeksa, a koji novinare obvezuje iznositi točnu, potpunu i provjerenu informaciju (točka 5. Kodeksa), a obvezuju ih i na dužnost ispravka netočne informacije (točka 12. Kodeksa) i na to da osobu koja daje informaciju moraju upoznati u kojem će mediju i u kojem kontekstu ta informacija biti objavljena uz izričitu zabranu iskrivljavanja smisla izjava i intervjua.

3. Građanskopravna zaštita privatnosti

Kao što smo uvodno naveli, pravo na slobodu izražavanja nije apsolutno pravo i često se nalazi u koliziji s pravom na zaštitu privatnosti, ugleda, časti i dostojanstva kao sastavnog dijela prava na štovanje osobnog života zajamčenog čl. 35. Ustava, odnosno njemu srodnog prava na poštovanje privatnog života zajamčenog čl. 8. Konvencije. Radi se o dva temeljna prava između kojih je u sudskom postupku potrebno uspostaviti pravičnu ravnotežu vaganjem relevantnih čimbenika koji se odnose na te dvije zaštićene vrednote s obzirom na okolnosti svakog pojedinog slučaja (*predmeti ESLJP-a Von Hannover protiv Njemačke br. 40660/08 i 60641/08, §§ 104. - 107., presuda od 7. veljače 2012.; Axel Springer AG protiv Njemačke, br. 39954/08, §§ 85.-88., presuda od 7. veljače 2012.; Couderc i Hachette Filipacchi Associés protiv Francuske br. 40454/07, §§ 90. - 93., presuda od 10. studenoga 2015.; i Medžlis Islamske zajednice Brčko i drugi protiv Bosne i Hercegovine, br. 17224/11, § 77., presuda od 27. lipnja 2017.*).

Pri tomu treba imati na umu da su medijska prava uvijek ograničena pravom na dostojanstvo, čast i ugled, kako to izričito proizlazi iz čl. 3. st. 3. ZM-a, ali i iz čl. 10. st. 2. Konvencije, koje shvaćanje je u brojnim odukama izrazio i Ustavni sud Republike Hrvatske (*npr. U-III-4057/2013 od 17. rujna 2014.*) te Vrhovni sud Republike Hrvatske (*npr. Rev-1553/09 od 24. studenoga 2009.*).

Kako ostvarivanje tih sloboda obuhvaća dužnosti i odgovornosti, ono može biti podvrgnuto formalnostima, uvjetima, ograničenjima ili kaznama propisanima zakonom, koji su u demokratskom društvu nužni. Ta ograničenja moraju biti strogo tumačena, a potreba za njima mora biti uvjerljivo utvrđena (*predmeti*

ESLJP Guja protiv Moldavije [Vv], br. 14277/04, § 69., presuda od 12. veljače 2008.; i Bédat protiv Švicarske [Vv], br. 56925/08, § 48., presuda od 29. ožujka 2016.).

Test nužnosti u demokratskom društvu zahtijeva da sud pred kojim se nađe "zahtjev" za ograničenje nečije slobode izražavanja utvrdi je li to ograničenje prijeko društveno potrebno i je li ono razmjerno legitimnom cilju, te da za to ograničenje navede relevantne i dostatne razloge (*predmet ESLJP-a Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske [Vv], br. 931/13, presuda od 27. lipnja 2017.*). Ograničenje prava na slobodu izražavanja mora se razmotriti u kontekstu slučaja u cjelini, uključujući sadržaj izjava i kontekst u kojem su one dane (*predmet ESLJP-a Europapress holding d.o.o. protiv Hrvatske, br. 25333/06, § 54., presuda od 22. listopada 2009.*).

Priroda i ozbiljnost nametnute sankcije također su čimbenici koje treba uzeti u obzir pri ocjenjivanju razmjernosti/nužnosti miješanja u pravo na slobodu izražavanja. Dosuđivanje naknade štete oštećenoj osobi mora biti u razumnom odnosu s pretrpljenim narušavanjem ugleda (*predmeti ESLJP Narodni list d.d. protiv Hrvatske, gore citirano, § 70.; Kwiecień protiv Poljske, br. 51744/99, § 56., presuda od 9. siječnja 2007.; Tolstoy Miloslavsky protiv Ujedinjenog Kraljevstva, br. 18139/91, § 49., presuda od 13. srpnja 1995.; i Europapress holding d.o.o., gore citirano, § 54.*).

Kako bi se osigurala dosljednost i izbjeglo diskrecijsko odlučivanje pri odgovaranju na pitanje koje od sukobljenih prava preteže u nekom konkretnom slučaju i kojemu od njih je potrebno pružiti zaštitu, Europski suda za ljudska prava je naveo kriterije prema kojima se, načelno, ocjenjuje je li u konkretnom slučaju postignuta ili je prekoračena pravična ravnoteža između sukobljenih prava:

a) doprinos raspravi u javnom interesu;
b) u kojoj mjeri je osoba u pitanju poznata javnosti i kakav je sadržaj danih izjava;
c) prethodno ponašanje osobe na koju se izjava odnosi;
d) metode prikupljanja informacija i njihova provjerljivost;
e) sadržaj, forma i posljedice objavljene informacije;
f) ozbiljnost dosuđene sankcije i obeshrabrujući učinak (tzv. *chilling effect*).

Ustavni sud, u tom smislu, u više svojih odluka (*npr. U-III-1084/2015 od 10. prosinca 2019., U-III-4336/2017 od 26. lipnja 2019., U-III-2944/2018 od 26. lipnja 2019. i dr.*), ističe da je prihvatio gore navedena načelna stajališta ESLJP-a, te je ispitujući opravdanost prigovora miješanja u jamstvo slobode mišljenja i izražavanja misli ukazao na potrebu provođenja tzv. *testa nužnosti u demokratskom društvu*.

Kada je sporna izjava dana u kontekstu političke debate o pitanju od javnog interesa, prihvatljiva su samo najnužnija ograničenja slobode izražavanja jer je sloboda političke debate u samoj srži koncepta demokratskog društva. Stoga su granice prihvatljive kritike šire u slučaju same osobe političara nego kod privatnih osoba. Za razliku od ovih posljednjih, političar je neizbježno i svjesno otvoreniji za pomno ispitivanje svake njegove ili njezine riječi i djela i sukladno tome mora iskazivati veći stupanj tolerancije (*predmeti ESLJP Sürek protiv Turske /br. 1/ [Vv], br. 26682/95, § 61., presuda od 8. srpnja 1999.; Mladina d.d. Ljubljana protiv Slovenije, br. 20981/10, § 40., presuda od 17. travnja 2014.; Lingens protiv Austrije, br. 9815/82, § 42., presuda od 8. srpnja 1986.; i Lopes Gomes da Silva protiv Portugala, br. 37698/97, § 30., presuda od 28. rujna 2000.*).

Kad se radi o kritici tijela javne vlasti, lokalnih dužnosnika i javnih osoba poznatih lokalnoj javnosti, granice dopuštene kritike su mnogo šire nego što je to slučaj s privatnim osobama, šire su čak i u odnosu na kritiku političara i dužnosnika. U demokratskom društvu radnje ili propusti tijela s javnim ovlastima moraju biti podložne strogoj kontroli ne samo od strane zakonodavnih i sudskih vlasti nego i od javnog

mijenja te se očekuje da pokažu visok stupanj tolerancije prema kritici (*predmeti ESLJP Şener protiv Turske,br. 26680/95, § 40., presuda od 18. srpnja 2000.; Lombardo i drugi protiv Malte,br. 7333/06, § 54., presuda od 24. travnja 2007.; i Margulev protiv Rusije, br. 15449/09, § 53., presuda od 8. listopada 2019.*).

U predmetu Oberschlick protiv Austrije (1. srpnja 1997., § 34.) austrijski su sudovi osudili novinara jer je, vođu Austrijske slobodarske stranke nazvao idiotom. Smatrajući da je time povrijeđeno pravo novinara na slobodu izražavanja, ESLJP je obrazložio da se riječ mora promatrati u svjetlu slučaja kao cjelina, uključujući podnositeljev članak i okolnosti u kojima je napisan te iznio shvaćanje da se članak, a posebice riječ idiot nesumnjivo mogu smatrati polemičnim, te da javno nazivanje političara idiotom može tog političara uvrijediti. No, ESLJP smatra da se ne radi o bezrazložnom osobnom napadu na političara, budući da je autor članka dao objektivno razumljivo obrazloženje izvedeno iz govora tog političara koji govor je sam po sebi bio polemičan i izazivajući te da se u ovom slučaju ne čini da je ta riječ nerazmjerna u odnosu na ogorčenje koje je taj političar svjesno izazvao.

U odluci Vrhovnog suda Republike Hrvatske broj: *Rev-1017/2024 od 29. listopada 2024.*, izraženo je pravno shvaćanje da se ograničenje iz čl. 7. st. 2. ZM-a o pravu na privatnost osoba koje obavljaju javnu službu odnosi na ograničeno pravo na privatnost osoba koje obavljaju javnu službu ili dužnost kada se radi o slučajevima koji su u vezi s javnom službom ili dužnosti koju osoba obavlja, ali ne i na ograničenje njihovog prava na zaštitu dostojanstva, časti i ugleda povrijeđenih neistinitim činjeničnim tvrdnjama objavljenim u medijima.

U spornom članku bila je riječ o pitanjima koja su u javnom interesu (izvještavanje o načinu donošenja zakona, propituje mogući sukob interesa osoba koje sudjeluju u radnoj skupini za izradu nacrta zakona, pravilnost popunjavanja imovinske kartice), pri čemu su korišteni i javno dostupni podaci za koje iz utvrđenja nižestupanjskih sudova ne proizlazi da su netočni niti je utvrđeno postojanje neistinitih činjeničnih tvrdnji. Sud za dijelove članka, o "*supermenu* među hrvatskim dužnosnicima", "rekorderu po broju prijava povjerenstvu za sukob interesa", da je "predavačka karijera tužitelja dosegla zvjezdane trenutke ulaskom u Ministarstvo", ocjenjuje da predstavljaju i određeni stupanj pretjerivanja koji je dopušten u novinarstvu, dok jednim dijelom predstavljaju i vrijednosne sudove autorice članka („nesposobnost da ispuni imovinsku karticu", „a ne zna se što je gore", da bi „javnost trebala povjerovati da državni tajnik zna što radi kad kreira složene zakone sa dalekosežnim posljedicama na sve velike pothvate u Hrvatskoj – a ne zna ispuniti ni običnu imovinsku karticu"). Sud je odbio tužbeni zahtjev s obzirom na to da nije utvrđeno postojanje neistinitih činjeničnih tvrdnji te da se u članku iznose podaci o tužitelju koji su vezani za njegovu javnu službu koju obavlja i u odnosu na koje je ograničeno pravo tužitelja na privatnost.

O važnosti postojanja javnog interesa za objavljivanje informacija privatne prirode ukazuju i pravna stajališta zauzeta u odlukama ESLJP prema kojima ako se vijesti o privatnim životima javnih osoba objavljuju u svrhu zabave, a ne obrazovanja, što doprinosi raznolikosti informacija dostupnih javnosti i nedvojbeno je zaštićeno čl. 10. Konvencije u predmetima koji se odnose na javnu osobu, to pravo na slobodu izražavanja zaštićeno čl. 10. Konvencije ipak može biti sekundarno zahtjevima čl. 8. ako su predmetne informacije privatne i intimne prirode i ne postoji javni interes za širenje tih informacija (*ESLJP u predmetima Mosley protiv Ujedinjenog Kraljevstva, br. 48009/08, .§131., presuda od 10. svibnja 2011.; Von Hannover protiv Njemačke (br. 2) [VV], § 110.*).

Na razinu zaštite privatnog života utječe i u kojoj je mjeri pojedinac javna ličnost ili je poznat (*ESLJP u predmetima Verlagsgruppe News GmbH protiv Austrije (br. 2), §34.; Alpha Doryforiki Tileorasi Anonymi Etairia protiv Grčke, §53. i*

naprijed navedenom Von Hannover protiv Njemačke).

U odluci Vrhovnog suda Republike Hrvatske broj: *Rev 5077/2019-2 od 24. lipnja 2020.*, postavljeno je pitanje „Može li nakladnik medija/štetnik bez ikakve suglasnosti te znanja ili privole oštećenih objavljivati putem medija video snimke ili fotografije oštećenih nastale na privatnim te za javnost zatvorenim događanjima?"

Polazeći od utvrđenja u postupku pred nižestupanjskim sudovima da je tuženica bez pristanka tužitelja emitirala na nacionalnoj televiziji fotografije i video snimku tužitelja s privatnog događanja, svadbene svečanosti, sud zaključuje da je navedenom radnjom povrijeđeno pravo tužitelja na privatnost. Naime, Vrhovni sud obrazlaže da okolnost što je događanje održano u muzeju, kojeg inače koristi javnost, nije od utjecaja na činjenicu da je svadbena svečanost na kojoj su tužitelji snimljeni privatne naravi, i kao takva bez njihove privole ne može biti predmetom objavljivanja na nacionalnoj televiziji. Pritom ne stoji usporedba drugostupanjskog suda između tužitelja i državnih dužnosnika koji su u spornom prilogu prikazani kao ilustracija odvijanja komercijalnih sadržaja u kulturnim institucijama iz razloga što tužitelji, za razliku od državnih dužnosnika, nisu javne osobe, u pogledu kojih vrijedi ograničenje prava na privatnost propisano čl. 7. st. 2. ZM-a.

Valja naglasiti da sudskoj zaštiti ne podliježe odgovornost medija kada se ugled izgubi zbog vlastitih postupaka. U predmetu Suda Europske unije u predmetu T341/12, presuda od 28. siječnja 2015. prihvaćeno je shvaćanje ESLJP da se osoba ne može pozivati na čl. 8. Konvencije za štetu nanesenu ugledu koja može predvidljivo proizaći iz njezinih vlastitih postupaka, poput kaznenog djela (*predmeti ESLJP, Sidabras i Džiautas/Litva od 27. srpnja 2004., tužbe br. 55480/00 i 59330/00, t. 49., Taliadorou i Stylianou/Cipar od 16. listopada 2008., tužbe br. 39627/05 i 39631/05, t. 56. i Gillberg/Švedska od 3. travnja 2012., tužba br. 41723/06, t. 67.*).

Prema sudskoj praksi, „obični" pojedinci uživaju najviši stupanj zaštite kada je u pitanju povreda privatnosti, dostojanstva, časti i ugleda. Prema praksi ESLJP gradacija zaštite tih prava bi bila najviša za obične građane, zatim slijede pojedinci koji ulaze u javnu sferu, javni službenici te političari i državna tijela, koji su na najnižoj razini zaštite.

U demokratskim društvima temeljni kriteriji utvrđivanja granice slobode izražavanja u odnosu prema pravu na zaštitu privatnosti je upravo opravdani interes javnosti. U svakom konkretnom slučaju u kojemu postoji opravdani interes javnosti, tada se sloboda izražavanja u pravilu smatra važnijom od prava na zaštitu privatnosti i prava osobnosti, pa se i povreda privatnosti i prava osobnosti u tom slučaju smatra dopuštenom. No, opravdani interes javnosti nije jedini kriterij kojeg je potrebno imati na umu kod razrješenja sukoba dvaju različitih prava istog ranga. Jedan od daljnjih kriterija je i doprinos izražavanja raspravi u javnom interesu. Ocjena o tome što je predmet javnog interesa ovisit će o okolnostima konkretnog slučaja.

U razrješenju tog sukoba potrebno je imati na umu jedno od temeljnih pravnih načela, a to je da se uporabom jednog prava ili slobode ne smije ugroziti ili ukinuti neko drugo pravo i sloboda, nego se svako pravo i sloboda u određenoj mjeri ograničuje kako bi opstalo i ono drugo pravo ili sloboda.

Iako je sloboda izražavanja zajamčena Ustavom i Konvencijom, zakonom je propisana odgovornost ako bi se ova sloboda zloupotrijebila. Tako je propisana odgovornost za štetu odredbom čl. 21. st. 1., 2. i 3. ZM-a, prema kojoj nakladnik koji informacijom objavljenom u mediju prouzroči drugome štetu dužan ju je naknaditi, izuzev u slučajevima propisanim ovim Zakonom. Na utvrđivanje odgovornosti za naknadu štete primjenjuju se propisi o obveznim odnosima, osim ako ZM nije drugačije određeno.

Šteta je umanjenje nečije imovine ili sprječavanje njezina povećanja (imovinska šteta) te

nanošenje drugom fizičkog ili psihičkog bola ili straha (neimovinska šteta). Odredbom čl. 22. st. 1. ZM-a propisano je da se nematerijalna šteta u pravilu naknađuje objavljivanjem ispravka informacije i isprikom nakladnika, te isplatom naknade sukladno općim propisima obveznog prava.

Dakle, iz izričite zakonske odredbe čl. 22. st. 1. ZM-a jasno proizlazi da se neimovinska šteta u pravilu naknađuje u nenovčanom obliku objavom ispravka informacije i isprikom nakladnika, ali i u novčanom obliku novčanom naknadom u skladu s općim propisima obveznog prava. Činjenica da ispravak ne eliminira u potpunosti štetu te da jednom objavljena netočna informacija djeluje i nakon ispravaka, razlog je zašto zakonodavac dopušta kumulaciju zahtjeva za nenovčanu naknadu štete sa zahtjevom za isplatu pravične novčane naknade.

Osnovne pretpostavke odgovornosti za nakladnika koji informacijom objavljenom u mediju prouzroči drugome štetu moraju biti kumulativno ispunjene, a odnose se na odgovornu osobu ili štetnika, oštećenika, štetnu radnju, štetu i uzročnu vezu.

Šteta u konkretnom slučaju mora biti prouzročena upravo objavom informacije, a informacija mora biti objektivno podobna prouzročiti štetu što znači da kod oštećenika uzrokuje poniženje, prezir od drugih, promjenu odnosa sredine prema njemu i sl. Da bi tužitelj mogao tvrditi da mu je uvredljivim izjavama povrijeđeno pravo na privatnost, dostojanstvo, čast i ugled zajamčeno čl. 35. Ustava, mora dokazati postojanje dostatne veze između navodnog napada na njegovu osobnost i izjava koje se mogu smatrati objektivno uvredljivim. Takva veza ne postoji ako okolnosti slučaja upućuju da je njegovo pravo na ugled novinskim člankom bilo pogođeno tek "marginalno ili indirektno" (*predmet ESLJP Putistin protiv Ukrajine, br. 16882/03, § 40., presuda od 21. studenoga 2013.*).

Zakon o medijima ne sadrži posebne kriterije za odmjeravanje visine pravične novčane naknade, dok se u Zakonu o obveznim odnosima u čl. 1100. propisuje da će sud u slučaju povrede prava osobnosti, ako nađe da to težina povrede i okolnosti slučaja opravdavaju, dosuditi pravičnu novčanu naknadu nezavisno od naknade imovinske štete, a i kada nje nema, te prilikom odlučivanja o visini pravične novčane naknade voditi računa o jačini i trajanju povredom izazvanih fizičkih boli, duševnih boli i straha, cilju kojemu služi ta naknada, ali i o tome da se njome ne pogoduje težnjama koje nisu spojive s njezinom naravi i društvenom svrhom.

Nematerijalna šteta može se popraviti objavljivanjem ispravka informacije (čl. 40. ZM), odgovorom na objavljenu informaciju (čl. 56. ZM). U prvom redu nakladnik može ispraviti informaciju samoinicijativno ili na zahtjev oštećenika (zahtjev upućen nakladniku u smislu procesne pretpostavke na tužbu zbog isplate pravične novčane naknade ili zahtjev upućen glavnom uredniku radi ostvarenja prava na traženje ispravka sudskim putem).

Oštećenik može svoje pravo na ispravak ostvariti sudskim i izvansudskim putem. Izvansudski postupak sastoji se od zahtjeva glavnom uredniku za objavljivanjem ispravka informacije kojom su povrijeđena prava i interesi fizičke ili pravne osobe. Sudski postupak uključuje pravo na podnošenje tužbe ako glavni urednik ne objavi ispravak u roku i na način određen Zakonom o medijima.

Objavljivanje članaka povodom istog događaja u različitim medijima predstavlja za tužitelja samostalnu štetu koju je dužan podmiriti svaki nakladnik samostalno i neovisno o drugima, ali svaka od ovih šteta mora biti razmjerna legitimnom cilju i svrsi naknade neimovinske štete. Ukupne novčane satisfakcije neimovinske štete koje će tužitelj realizirati od različitih odgovornih osoba zbog objavljivanja istih informacija moraju u svojoj ukupnosti biti u skladu sa ciljem i svrhom naknade. Naime, u skladu sa odredbom čl. 1100. Zakona o obveznim odnosima, postojanje neimovinske štete i njezina visina utvrđuje se prema specifičnim okolnostima

svakog pojedinog slučaja, no zakonska sintagma "da naknada štete ne pogoduje težnjama koje nisu spojive s njezinom naravi i društvenom svrhom", nameće obvezu sudu na jednako postupanje u jednakim ili usporedivim situacijama, ali i obvezu sudu da kao dodatni kriterij odmjeravanja konkretne štete, uzme u obzir ukupno realizirane novčane satisfakcije neimovinske štete.

Potrebno je ukazati i na tzv. strateške tužbe protiv javnog sudjelovanja - SLAPP tužbe, pojedinaca čija moć se temelji na njihovom političkom, financijskom i društvenom statusu, protiv osoba koje u javnosti kritiziraju njihov rad i djelovanje, u kojem slučaju su osobe koje su kao tuženici najčešće obuhvaćene podnošenjem SLAPP tužbi i vođenjem tih postupaka novinari, osobito istraživački novinari, borci za ljudska prava, aktivni članovi udruga za zaštitu okoliša i istaknuti članovi akademske zajednice. Naime, iako SLAPP tužbe nisu izričito regulirane domaćim propisima, na razini EU usvojena je Direktiva (EU) 2024/1069 Europskog parlamenta i Vijeća od 11. travnja 2024. o zaštiti osoba uključenih u javno djelovanje od očito neosnovanih tužbi ili zlonamjernih sudskih postupaka („strateške tužbe usmjerene protiv javnog djelovanja").

U predmetima za naknadu štete zbog povrede prava osobnosti sve veći broj predmeta pred hrvatskim sudovima se odnosi na slobodu izražavanja na internetu, pa je bitno istaknuti da se pravo na slobodu izražavanja primjenjuje na internetu jednako kao i izvan njega, a svako ograničenje mora biti u skladu sa zakonom i Konvencijom.

Do donošenja Zakona o elektroničkim medijima u sudskoj praksi se problematiziralo pitanje odgovornosti za naknadu štete u medijima kada su informacije objavljene na internetu u komentarima čitatelja.

Ustavni sud u brojnim odlukama (*npr. U-III-2669/2018 od 27. ožujka 2018.*) izrazio je shvaćanje da se sloboda izražavanja odnosi i na internet kao sredstvo komunikacije, kao i da se internet kao sredstvo komunikacije razlikuje od klasičnih medija, te predstavlja veći rizik za prava zaštićena člankom 8. Konvencije (*predmeti ESLJP Delfi AS protiv Estonije [Vv], br. 64569/09, § 131., presuda od 16. lipnja 2015. i Editorial Board of Pravoye Delo i Shtekel protiv Ukrajine, br. 41214/08 i 49440/08, § 63., presuda od 16. travnja 2019.*). U vezi odgovornosti vlasnika internetskog portala za komentare korisnika (imenovanih ili anonimnih) objavljene na portalu, a kojima se vrijeđaju prava trećih osoba, ESLJP je zaključio da se, s obzirom na specifičnu prirodu interneta, prava i obveze vlasnika internetskog portala u vezi komentara drugih osoba mogu razlikovati od vlasnika klasičnih medija te je utvrdio kriterije za utvrđivanje da li sankcioniranje vlasnika portala za takve komentare predstavlja povredu slobode izražavanja: priroda i kontekst spornih komentara; mjere koje je vlasnik portala poduzeo da spriječi ili ukloni komentare kojima se vrijeđaju prava trećih osoba; odgovornost stvarnih autora komentara kao alternativa odgovornosti vlasnika portala; te posljedice koje izrečena sankcija ima za vlasnika portala (*predmeti ESLJP Delfi AS protiv Estonije; Magyar Tartalomszolgáltatók Egyesülete i Index.hu ZRT protiv Mađarske, br. 22947/13, § 69., presuda od 2. veljače 2016.; Hřiness protiv Norveške , br. 43624/14, § 67., presuda od 19. ožujka 2019.*). Ustavni sud je prihvatio navedena načelna stajališta ESLJP u odluci broj: U-III-2669/2018 od 27. ožujka 2018.

Delfi AS protiv Estonije je prvi predmet u kojem je ESLJP ispitivao predmet u kojem se ovi interesi sukobljavaju U tom predmetu Estonska internetska stranica objavila je članak koji je izazvao niz uvredljivih i prijetećih komentara. Iako su komentari kasnije uklonjeni, tvrtka je proglašena odgovornom te je izraženo shvaćanje da nije došlo do povrede čl. 10. Konvencije i da je miješanje u pravo na slobodu izražavanja bilo u skladu sa zakonom, jer je izdavač koji moderira komentare odgovoran za njihov sadržaj. ESLJP je smatrao da je Delfi, kao profesionalni izdavač koji objavljuje na jednom od najvećih novinskih

portala u Estoniji, trebao i mogao ocijeniti rizike povezane sa svojim aktivnostima te da je razumno mogao predvidjeti posljedice koje te aktivnosti mogu imati. Stoga je Sud zaključio kako je miješanje u pravo na slobodu izražavanja bilo u skladu sa zakonom.

4. Izjave o činjenicama i vrijednosni sudovi

Dok se postojanje činjenica može dokazati, istinitost vrijednosnih sudova nije dokaziva, niti se u sudskom postupku može zahtijevati da se dokaže istinitost vrijednosnog suda. Kada se radi o vrijednosnim sudovima, razmjernost ograničenja slobode izražavanja može ovisiti o tome postoji li dostatna činjenična osnova koja te sudove podržava, u suprotnom se ti sudovi mogu smatrati pretjeranima. Kako bi se moglo razlikovati radi li se o izjavi o činjenicama ili o vrijednosnom sudu nužno je uzeti u obzir okolnosti svakog slučaja i "opći ton" (*general tone*) izjave o kojoj se radi, imajući u vidu da će tvrdnje o temama od javnog interesa u pravilu biti vrijednosni sudovi, a ne izjave o činjenicama (*predmet ESLJP-a Morice protiv Francuske[Vv], br. 29369/10, § 126., presuda od 23. travnja 2015.*).

Vrhovni sud je u brojnim odlukama (*npr. Rev-929/2009 od 15. rujna 2009.*) zauzeo shvaćanje da nakladnik ne odgovara za štetu ako je informacija kojom je šteta učinjena proizašla iz vrijednosnih sudova autora čije je objavljivanje bilo u javnom interesu i ako je ta informacija dana u dobroj vjeri. Iz odredbe čl. 21. st. 4. al. 6. ZM-a proizlazi da se za vrijednosne sudove traži da ih je autor dao u dobroj vjeri, dakle, radi se o subjektivnom odnosu autora prema iznesenom vrijednosnom sudu tj. da je isti dostatno utemeljen na njegovim intelektualnim saznanjima i zdravorazumskom zaključivanju, odnosno od autora se u tom slučaju ne traži aktivno postupanje u smislu poduzimanja uobičajenih novinarskih mjera za provjeru istinitosti i točnosti informacije, jer kao što je već rečeno, informacije koje sadrže vrijednosne sudove po naravi stvari nisu podobne za objektivno utvrđivanje (jer su subjektivno stajalište), ne podliježu dokazu istinitosti, niti je o njima uopće moguće raspravljati sa stajališta njihove istinitosti ili neistinitosti.

No, i vrijednosnim sudom se može povrijediti nečije pravo osobnosti, što ovisi o okolnostima svakog pojedinog slučaja pri čemu sudovi utvrđuju ima li vrijednosni sud bitne činjenične utemeljenosti, je li objavljivanje tih vrijednosnih sudova u javnom interesu te jesu li ti vrijednosni sudovi iznijeti u dobroj vjeri, pri čemu se sud rukovodi i primjenom testa razmjernosti. Prema sudskoj praksi (*npr. odluka Ustavnog suda broj: U-III-2937/2022 od 8. prosinca 2022.*) standard dobre vjere, podrazumijeva da je novinar, prije objave, provjerio istinitost ili točnost informacija.

ESLJP smatra da bi za novinare, kada bi mogli objavljivati samo one informacije čija se istinitost može u potpunosti dokazati, to bio nerazuman zahtjev i nemoguć zadatak (*predmet ESLJP Thorgeir Thorgeirson protiv Islanda, § 65., presuda od 25. lipnja 1992.*). No, prema praksi ESLJP jamstvo koje čl. 10. Konvencije daje novinarima u odnosu na izvještavanje o pitanjima od općeg interesa podrazumijeva da djeluju u dobroj vjeri i u skladu s novinarskom etikom.

5. Zaključak

Imajući u vidu sve navedeno, možemo zaključiti da odluka suda o odgovornosti za naknadu štete počiva na činjeničnim okolnostima svakog pojedinog slučaja i da nije moguće generalizirati odluke koje se odnose na odgovornost za štetu zbog povrede prava osobnosti objavljenom informacijom u medijima. Naime, treba naglasiti da sud sudi na temelju zakona i činjenica utvrđenih u postupku između dvije suprotstavljene strane, pri čemu provodi test proporcionalnosti odnosno „važe" između pitanja povrede prava na privatnost, dostojanstvo, čast i ugled u odnosu s pravom medija na slobodu izražavanja i slobodu mišljenja, te pri

donošenju odluke mora jasno obrazložiti utvrđenja što predstavlja vrijednosne sudove od činjeničnih tvrdnji u smislu dokazivanja njihove istinitosti. Ujedno sud provodi test nužnosti takvog ograničenja slobode izražavanja u svakom pojedinačnom slučaju, uzimajući u obzir kontekst koje bi takvo ograničenje slobode izražavanja imalo na spor, sve radi odgovora na pitanje je li, prema mišljenju suda, takvo ograničenje prava na izražavanje proporcionalno i nužno u demokratskom društvu.

Pored navedenog u sporovima u kojem se suprotstavljaju s jedne strane pravo na slobodu izražavanja i izvještavanja novinara o pitanjima od javnog interesa te s druge strane pravo na zaštitu privatnosti, dostojanstva, ugleda i časti pojedinca, sudovi su dužni razmotriti je li novinar postupao u dobroj vjeri kako bi pružio točnu i pouzdanu informaciju u skladu s novinarskom etikom. Pravni standard dobre vjere, podrazumijeva da je novinar, prije objave, provjerio istinitost ili točnost informacija.

Svaki autor članka zna ili bi barem morao znati koliko su informacije koje objavljuje vjerodostojne, ako već ne može provjeriti njihovu istinitost, odnosno postupa li po normama vlastitog etičkog kodeksa - Kodeksa časti hrvatskih novinara, koji novinare obvezuje iznositi točnu, potpunu i provjerenu informaciju (točka 5. Kodeksa).

Iako su privatnost, čast, dostojanstvo i ugled vrijednosti istog ustavnog ranga kao i sloboda izražavanja, valja ponoviti da pravo na čast, ugled, dostojanstvo i privatnost predstavlja temeljno ljudsko pravo koje nikada i nigdje nije ograničeno medijskim pravima. Zadatak sudova u primjeni medijskog zakonodavstva ogleda se u postizanju pravedne/pravične ravnoteže u ostvarenju tih dvaju suprotstavljenih vrijednosti prava uz primjenu standarda ESLJP provođenjem testa nužnosti u demokratskom društvu.

LITERATURA

Znanstveni i stručni radovi

Rajko, Alen, Odnos sudova i medija (iz perspektive informacijskog upravnog prava, Zbornik radova 10. savjetovanja Novosti u upravnom pravu i upravnosudskoj praksi. Zagreb: Organizator, 2022. str. 326.

Jurić, Katulić, Lisičar, Zaštita osobnih podataka: prvi dio, Pravni fakultet u Zagrebu, Zagreb, 2025.

Moreno-Gil, V., Ramon-Vegas, X., & Mauri-Rí¬os, M. "Bringing journalism back to its roots: examining fact-checking practices, methods, and challenges in the Mediterranean context.", Profesional De La información, 31(2). 2022. https://doi.org/10.3145/epi.2022.mar.15

Međunarodni akti

Opća deklaracija o ljudskim pravima („Narodne novine", Međunarodni ugovori, broj 12/2009)

Europska Konvencija za zaštitu ljudskih prava i temeljnih sloboda („Narodne novine"- Međunarodni ugovori, broj 18/97, 6/99 – pročišćeni tekst, 8/99 – ispravak, 14/02, 13/03, 9/05, 1/06, 2/10 i 13/17)

Povelja Europske unije o temeljnim pravima (Službeni list Europske unije, C 202/389)

Zakonodavstvo EU

Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka, OUZP)

Uredba (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama), SL L 277, 27.10.2022., str. 1–102.

Direktiva (EU) 2018/1808 Europskog parlamenta i Vijeća od 14. studenoga 2018. o izmjeni Direktive 2010/13/EU o koordinaciji određenih odredaba utvrđenih zakonima i drugim propisima u državama članicama o pružanju audiovizualnih medijskih usluga (Direktiva o audiovizualnim medijskim uslugama) u pogledu promjenjivog stanja na tržištu, SL L 303, 28.11.2018., str. 69–92.

Uredba (EU) 2024/1083 Europskog parlamenta i Vijeća od 11. travnja 2024. o uspostavi zajedničkog okvira za medijske usluge na unutarnjem tržištu i izmjeni Direktive 2010/13/EU (Europski akt o slobodi medija), SL L, 2024/1083, 17.4.2024.

Direktiva 2000/31/EZ Europskog parlamenta i Vijeća od 8. lipnja 2000. o određenim pravnim aspektima usluga informacijskog društva na unutarnjem tržištu, posebno elektroničke trgovine (Direktiva o elektroničkoj trgovini) SL L 178, 17.7.2000., str. 1–16.

Zakoni

Ustav Republike Hrvatske, NN 56/90, 135/97, 113/00, 28/01, 76/10 i 5/14.
Zakon o medijima, NN 59/04, 84/11, 81/13, 114/22.
Zakon o elektroničkim medijima, NN 111/2021.
Zakon o pravu na pristup informacijama, NN 25/13, 85/15, 69/22.
Zakon o općem upravnom postupku, NN 47/09, 110/21.
Zakon o parničnom postupku, SL SFRJ Službe-

ni list SFRJ br. 4/1977, 36/1977, 36/1980, 6/1980, 69/1982, 43/1982, 58/1984, 74/1987, 57/1989, 20/1990, 27/1990, 35/1991, NN 53/1991, 91/1992, 112/1999, 129/2000, 88/2001, 117/2003, 88/2005, 2/2007, 96/2008, 84/2008, 123/2008, 57/2011, 25/2013, 89/2014, 70/2019, 80/2022, 114/2022, 155/2023.

Zakon o kaznenom postupku, NN 152/2008, 76/2009, 80/2011, 91/2012, 143/2012, 56/2013, 145/2013, 152/2014, 70/2017, 126/2019, 126/2019, 80/2022, 36/2024, 72/2025.

Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske, NN 79/2006, 105/2006.

Zakon o tajnosti podataka, NN 79/2007, 86/2012.

Zakon o zaštiti neobjavljenih informacija s tržišnom vrijednosti, NN 30/2018.

Zakon o odvjetništvu, NN 9/1994, 117/2008, 50/2009, 75/2009, 18/2011, 126/2021.

Zakon o javnom bilježništvu, NN 78/1993, 29/1994, 162/1998, 16/2007, 75/2009, 120/2016, 57/2022.

Zakon o kreditnim institucijama, NN 59/2013, 19/2015, 102/2015, 15/2018, 70/2019, 47/2020, 146/2020, 151/2022, 145/2024.

Opći porezni zakon, NN 115/2016, 106/2018, 121/2019, 32/2020, 42/2020, 114/2022, 152/2024.

Zakon o autorskom pravu i srodnim pravima, NN 111/2021, 114/2022.

Zakon o provedbi Uredbe (EU) 2022/2065 Europskog parlamenta i Vijeća od 19. listopada 2022. o jedinstvenom tržištu digitalnih usluga i izmjeni Direktive 2000/31/EZ (Akt o digitalnim uslugama) NN 67/2025.

Sudska praksa

Ustavni sud

Odluka U-I-884/1997 od 3. veljače 2000.

Odluka U-III-1810/2004 od 20. rujna 2006.

Odluka U-II-593/1997 od 14. ožujka 2001.

Odluka U-III-4057/2013 od 17. rujna 2014.

Odluka U-III-2669/2018 od 27. ožujka 2018.

Odluka U-III-2937/2022 od 8. prosinca 2022.

Vrhovni sud Republike Hrvatske

Rev-1553/09 od 24. studenoga 2009.

Rev-1017/2024 od 29. listopada 2024.

Rev 5077/2019-2 od 24. lipnja 2020.

Rev-929/2009 od 15.rujna 2009.

Upravni sud

Rješenje klasa UP/II-008-07/24-01/287, broj 401-01/06-24-5, od 12. rujna 2024.

Predmet klasa UP/II-008-07/23-01/184, broj: 401-01/04-23-3, od 20. travnja 2023.

Europski sud za ljudska prava

Stoll protiv Švicarske, br. 69698/01, presuda od 10. prosinca 2007.

Pedersen i Baadsgaard protiv Danske br. 49017/99, presuda od 17. prosinca 2004.

Satakunnan Markkinapörssi Oy i Satamedia Oy protiv Finske, br. 931/13, presuda od 27. lipnja 2017.

Magyar Helsinki Bizottság protiv Mađarske br. 18030/11, presuda od 8. studenoga 2016.

Von Hannover protiv Njemačke br. 40660/08 i 60641/08, presuda od 7. veljače 2012.

Axel Springer AG protiv Njemačke, br. 39954/08, presuda od 7. veljače 2012.

Couderc i Hachette Filipacchi Associés protiv Francuske br. 40454/07, presuda od 10. studenoga 2015.

Medžlis Islamske zajednice Brčko i drugi protiv Bosne i Hercegovine, br. 17224/11, presuda od 27. lipnja 2017.

Guja protiv Moldavije, br. 14277/04, § 69., presuda od 12. veljače 2008.

Bédat protiv Švicarske, br. 56925/08, presuda od 29. ožujka 2016.

Europapress holding d.o.o. protiv Hrvatske, br. 25333/06, presuda od 22. listopada 2009.

Narodni list d.d. protiv Hrvatske, br.2782/12, presuda od 18. ožujka 2019.

Kwiecień protiv Poljske, br. 51744/99, presuda od 9. siječnja 2007.

Tolstoy Miloslavsky protiv Ujedinjenog Kraljevstva, br. 18139/91 presuda od 13. srpnja 1995.

Sürek protiv Turske, br. 26682/95., presuda od 8. srpnja 1999.

Mladina d.d. Ljubljana protiv Slovenije, br. 20981/10, presuda od 17. travnja 2014.

Lingens protiv Austrije, br. 9815/82, presuda od 8. srpnja 1986.

Lopes Gomes da Silva protiv Portugala, br. 37698/97, presuda od 28. rujna 2000.
Şener protiv Turske, br. 26680/95, presuda od 18. srpnja 2000.
Lombardo i drugi protiv Malte, br. 7333/06, presuda od 24. travnja 2007.
Margulev protiv Rusije, br. 15449/09, presuda od 8. listopada 2019.
Mosley protiv Ujedinjenog Kraljevstva, br. 48009/08, presuda od 10. svibnja 2011.
Putistin protiv Ukrajine, br. 16882/03, presuda od 21. studenoga 2013.
Delfi AS protiv Estonije, br. 64569/09, presuda od 16. lipnja 2015.
Editorial Board of Pravoye Delo i Shtekel protiv Ukrajine, br. 41214/08 i 49440/08, presuda od 16. travnja 2019.
Hřiness protiv Norveške , br. 43624/14, presuda od 19. ožujka 2019.
Morice protiv Francuske, br. 29369/10, presuda od 23. travnja 2015.
Thorgeir Thorgeirson protiv Islanda, br. 13778/88, presuda od 25. lipnja 1992.

Elektronički izvori

Povjerenik za informiranje, Pravo na pristup informacijama: Vodič za medije i udruge (dostupno na https://pristupinfo.hr/wp-content/uploads/2018/10/esf-vodic_web.pdf?x45242).

Smjernice za provedbu Zakona o pravu na pristup informacijama: Pristup informacijama i poslovnoj tajni, 2024, dostupno na https://pristupinfo.hr/wp-content/uploads/2025/01/Smjernice-poslovna-tajna.pdf?x45242.

Smjernice za provedbu Zakona o pravu na pristup informacijama: Pristup informacijama i klasificiranim podacima, 2024, dostupno na https://pristupinfo.hr/wp-content/uploads/2025/01/Smjernica-pristup-informacijama-i-klasificiranim-podacima.pdf?x45242.

Smjernice za provedbu Zakona o pravu na pristup informacijama: Test razmjernosti i javnog interesa, dostupno na https://www.pristupinfo.hr/wp-content/uploads/2018/10/Smjernice-Test-razmjernosti-i-javnog-interesa-1.pdf.

Odluke dostupne odgovarajućim filtiranjem na stranici https://tom.pristupinfo.hr/pregledfilter1.php.

Stanford Encyclopedia of Philosophy, Freedom of Speech, Siječanj 19, 2024 https://plato.stanford.edu/entries/freedom-speech/.

ICO Data Protection and Journalism Code of Practice 2023, dostupan na adresi: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-and-journalism-code-of-practice/journalism-code/.

IFCN Code of Principles, dostupan na stranicama IFCN https://ifcncodeofprinciples.poynter.org.

The Digital Services Act (DSA) and combating disinformation – 10 key takeaways, https://chamber.com/articles/the-digital-services-act-dsa-and-combating-disinformation-10-key-takeaways.

Smjernice Vijeća Europe, Smjernice o suzbijanju širenja online dezinformacija i misinformacija kroz provjeru činjenica i rješenja dizajna platforme na način usklađen s ljudskim pravima, dostupno na https://edoc.coe.int/en/internet/11885-guidance-note-on-countering-the-spread-of-online-mis-and-disinformation-through-fact-checking-and-platform-design-solutions-in-a-human-rights-compliant-manner.html.

Kodeks časti hrvatskih novinara (HND, 2009).