

**Dr. sc. Ivan Glavić\***

## **KAZNENOPRAVNI UČINCI AKTA O DIGITALNIM USLUGAMA**

*U radu se analiziraju odredbe Akta o digitalnim uslugama o nalozi-  
ma za djelovanje protiv nezakonitog sadržaja i za davanje informacija  
izdanim pružateljima usluga posredovanja za slučaj da sadržaj pred-  
stavlja kazneno djelo. Ujedno se iznosi prikaz odredbi predmetne ured-  
be Europske unije koje se odnose na obvezu pružatelja usluga smještaja  
informacija na poslužitelju da obavijeste nadležno redarstveno ili pra-  
vosudno tijelo o sumnji na kazneno djelo koje uključuje prijetnju životu  
i sigurnosti osoba. Naglasak je stavljen na korelaciju navedenih dije-  
lova Akta o digitalnim uslugama s drugim izvorima zajedničkog prava  
Europske unije, kao i s postojećim pravnim sustavima Hrvatske i dru-  
gih država članica Unije o otkrivanju i progonu počinitelja kaznenih  
djela i obvezi podnošenja kaznene prijave. Rezultati rada upućuju na  
to da Akt o digitalnim uslugama predstavlja pravnu podlogu za sprje-  
čavanje daljnjeg počinjenja, zaštitu žrtava i otkrivanje počinitelja kod  
očitih kaznenih djela na internetu neovisno o lokaciji pružatelja usluga  
posredovanja, ali pod uvjetom osiguranja u provedbenom pravu učin-  
kovite razmjene informacija između redarstvenih i pravosudnih tijela te  
izdavatelja naloga i(li) nacionalnog koordinатора za digitalne usluge.  
Kaznenopravna odgovornost pružatelja usluga smještaja informacija  
na poslužitelju i njegovih odgovornih osoba zbog povrede obveze pri-  
javljivanja kaznenih djela koja uključuju prijetnju životu i sigurnosti  
osoba pritom je teoretski moguća, ali u praksi teško ostvariva.*

*Ključne riječi: Akt o digitalnim uslugama, nalog za djelovanje pro-  
tiv nezakonitog sadržaja, nalog za davanje informacija, europski nalog  
za dostavljanje elektroničkih dokaza, neprijavljivanje kaznenih djela*

---

\* Dr. sc. Ivan Glavić, zamjenik državnog odvjetnika u Županijskom državnom odvjetništvu u Zagrebu; ivan.glavic@zdoz.dorh.hr; ORCID iD: <https://orcid.org/0000-0003-4055-3286>

## 1. UVOD

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)<sup>1</sup> na snazi je od 16. studenog 2022., a kao obvezujuća se u potpunosti izravno primjenjuje u svim državama članicama od 17. veljače 2024.

Predmetnim izvorom zajedničkog prava Europske unije nastoji se otkloniti rascjepkanost nacionalnih pravnih sustava u području usluga pristupa internetu i informacijskog društva, poboljšati transparentnost rada i osigurati proaktivnost njihovih pružatelja u zaštiti korisnika i društva u cjelini te odrediti jasne uvjete za pružanje mrežnih usluga i slobodu trgovine. U konačnici, nastoji se spriječiti da izvan domašaja ostanu oni gospodarski subjekti koji se nalaze ili su pohranili sadržaj izvan Europske unije budući da je za primjenu Akta o digitalnim uslugama presudno jesu li one ponuđene primateljima s poslovnim nastanom ili koji se nalaze na njezinu području te postoji li pritom bitna veza s Europskom unijom. Taj dodatni uvjet smatrat će se ostvarenim ako je poslovni nastan pružatelja usluge u državi članici, ali se također može izvesti iz drugih okolnosti slučaja, neovisno o samoj lokaciji pružatelja usluga. Primjer navedenog jesu izvaneuropski gospodarski subjekti sa znatnim brojem klijenata, primatelja usluge, u jednoj ili više država članica, ili koji usmjeravaju aktivnosti prema jednoj ili više država članica Europske unije.<sup>2</sup>

Akt o digitalnim uslugama primjenjuje se na pružatelje usluga posredovanja. Riječ je o pojedinim uslugama informacijskog društva, tj. onima koje se obično pružaju uz naknadu, na daljinu, elektroničkim sredstvima te na osobni zahtjev primatelja usluga,<sup>3</sup> a za koje je ocijenjeno kako je eksponencijalni rast njihova korištenja, uglavnom u zakonite i društveno korisne svrhe, također povećao njihovu ulogu u posredovanju i širenju nezakonitih ili na druge načine štetnih informacija i aktivnosti.<sup>4</sup> Usluge posredovanja razvrstane su u tri kategorije: a) usluga „samo prijenosnik informacija“, koja se sastoji od prijenosa informacija u komunikacijskoj mreži dobivenih od primatelja usluge ili od davanja pristupa komunikacijskoj mreži; b) usluga „privremeni smještaj“, koja se sastoji od prijenosa informacija u komunikacijskoj mreži

---

<sup>1</sup> Službeni list Europske unije, br. L 277/1 od 27. listopada 2022. (u daljnjem tekstu Akt o digitalnim uslugama).

<sup>2</sup> Čl. 2. st. 1., čl. 3. toč. e) Akta o digitalnim uslugama.

<sup>3</sup> Čl. 1. st. 1. toč. b) Direktive (EU) 2015/1535 Europskog parlamenta i Vijeća od 9. rujna 2015. o utvrđivanju postupka pružanja informacija u području tehničkih propisa i pravila o uslugama informacijskog društva (kodificirani tekst), Službeni list Europske unije, br. L 241/I od 17. rujna 2015.

<sup>4</sup> Odjeljak 5. uvoda Akta o digitalnim uslugama.

dobivenih od primatelja usluge i uključuje automatsku, prijelaznu i privremenu pohranu tih informacija koja se provodi isključivo u svrhu učinkovitijeg daljnjeg prijenosa informacija drugim primateljima na njihov zahtjev; c) usluga „smještaj informacija na poslužitelju”, koja se sastoji od pohrane informacija dobivenih od primatelja usluge i na njegov zahtjev.<sup>5</sup> Posljednja kategorija, pored usluga kao što su poslovanje u oblaku (*engl.* cloudu) ili smještaj internetskih stranica i elektroničke pošte na poslužitelju (*engl.* serveru), kao potkategoriju obuhvaća i internetske platforme. Te usluge uz smještaj informacija na poslužitelju kumulativno obuhvaćaju i njihovo širenje u javnosti na zahtjev primatelja usluge.<sup>6</sup> Najveće internetske platforme primateljima u Europskoj uniji pružaju usluge *online*-trgovine, društvenih mreža te dijeljenja sadržaja na internetu.<sup>7</sup>

Odredbe o položaju pružatelja usluga posredovanja odnose se na njihovu opću odgovornost te na obveze dužne pažnje za transparentno i sigurno internetsko okruženje. Tema ovog rada ograničena je na kaznenoprocne i materijalne učinke Akta o digitalnim uslugama. U tom kontekstu pružatelji sve tri kategorije usluga posredovanja u obvezi su postupiti sukladno nalogima nacionalnih tijela za djelovanje protiv nezakonitog sadržaja iz čl. 9. te nalogima za davanje informacija iz čl. 10. Akta o digitalnim uslugama. Dodatno, u smislu čl. 18. Akta o digitalnim uslugama, pružatelji usluga smještaja informacija na poslužitelju u obvezi su prijaviti sumnju na određene vrste predstojećih, počinjenih ili kaznenih djela u tijeku.

Odlukom Vlade Republike Hrvatske od 15. veljače 2024.<sup>8</sup> koordinatorom za digitalne usluge, nadležnim za usklađivanje aktivnosti nacionalnih provedbenih tijela te ujedno za nadzor pružatelja usluga posredovanja i izvršavanje Akta o digitalnim uslugama, imenovana je Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM). Trenutačno je dostupan Nacrt prijedloga Zakona 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),<sup>9</sup> usvojen na sjednici Vlade Republike Hrvatske 29. kolovoza 2024.

---

<sup>5</sup> Čl. 3. toč. g) Akta o digitalnim uslugama.

<sup>6</sup> Usp. čl. 3. toč. i) Akta o digitalnim uslugama i odjeljke 13. i 14. uvida Akta o digitalnim uslugama.

<sup>7</sup> <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> (20. 7. 2024.)

<sup>8</sup> Odluka o imenovanju koordinatora za digitalne usluge, klasa 022-03/24-04/61, ur. broj 50301-05/16-24-6 od 15. veljače 2024. (Narodne novine, br. 19/2024).

<sup>9</sup> <https://vlada.gov.hr/sjednice/21-sjednica-vlade-republike-hrvatske-42899/42899> (4. 9. 2024.), u daljnjem tekstu Nacrt prijedloga Zakona o provedbi Akta o digitalnim uslugama.

U ovom članku analiziraju se i odredbe pozitivnog hrvatskog prava, osobito Zakona o kaznenom postupku,<sup>10</sup> Kaznenog zakona<sup>11</sup> i Zakona o odgovornosti pravnih osoba za kaznena djela<sup>12</sup> te se dovode u vezu s pravnim institutima Akta o digitalnim uslugama, iznosi se osvrt na poredbeno pravo država članica Europske unije te se daje ocjena Nacrta prijedloga Zakona o provedbi Akta o digitalnim uslugama.

## **2. SUZBIJANJE SADRŽAJA KOJI PREDSTAVLJA KAZNENO DJELO PRISILNIM MJERAMA PREMA PRUŽATELJU USLUGE**

### **2.1. Odredbe Akta o digitalnim uslugama**

Nalog za djelovanje protiv nezakonitog sadržaja iz čl. 9. Akta o digitalnim uslugama izdaje nadležno pravosudno ili upravno tijelo (uključujući i tijelo za izvršavanje zakonodavstva<sup>13</sup>) države članice i dostavlja ga kontaktnoj točki pružatelja usluga posredovanja za izravnu elektroničku komunikaciju. Premda sam način izvršenja naloga tom normom nije pobliže određen, iz okolnosti da njegov obvezni sadržaj uključuje informacije koje omogućuju identifikaciju i lociranje nezakonitog sadržaja, kao što su jedan ili više točnih URL-ova, kao i iz izraza „moderiranje sadržaja“ kao aktivnosti pružatelja usluga posredovanja, među ostalim, sa svrhom suzbijanja nezakonitog sadržaja,<sup>14</sup> proizlazi da je riječ o mjerama usmjerenima protiv nezakonitog sadržaja ili primatelja usluge općenito (npr. zatvaranje korisničkog računa, uklanjanje ili kriptiranje sadržaja na poslužitelju) ili u odnosu na pojedine države (npr. geografsko blokiranje pristupa sadržaju iz pojedine države članice putem IP adrese ili podataka ostavljenih prilikom registracije na uslugu). Aktom o digitalnim uslugama nije izričito normirano da obveza pružatelja usluga posredovanja da postupi prema izdanom nalogu podrazumijeva i poduzimanje mjera protiv ponovne objave istovjetnog ili ekvivalentnog sadržaja i takvo je tumačenje u pravnoj teoriji sporno.<sup>15</sup>

---

<sup>10</sup> Narodne novine, br. 152/2008, 76/2009, 80/2011, 121/2011, 91/2012, 143/2012, 56/2013, 145/2013, 152/2014, 70/2017, 126/2019, 130/2020, 80/2022, 36/2024.

<sup>11</sup> Narodne novine, br. 125/2011, 144/2012, 56/2015, 61/2015, 101/2017, 118/2018, 126/2019, 84/2021, 114/2022, 114/2023, 36/2024.

<sup>12</sup> Narodne novine, br. 151/2003, 110/2007, 45/2011, 143/2012, 114/2022, 114/2023.

<sup>13</sup> Odjeljak 31. uvida Akta o digitalnim uslugama, pod tim pojmom podrazumijevaju se redarstvena tijela (engl. *law enforcement*, njem. *Strafvollzugsbehörde*).

<sup>14</sup> Usp. čl. 3. toč. t) Akta o digitalnim uslugama.

<sup>15</sup> Usp. Rojszczak, M., The Digital Services Act and the Problem of Preventive Blocking of (Clearly) Illegal Content, *Institutiones Administrationis – Journal of Administrative Sciences*, vol. 3, br. 2/2023, str. 50.

Sukladno čl. 3. toč. h) Akta o digitalnim uslugama, nezakonit sadržaj predstavlja svaka informacija koja, sama po sebi ili u vezi s određenom aktivnošću, uključujući i prodaju proizvoda ili pružanje usluga, nije u skladu s pravom Europske unije ili pravom bilo koje države članice koje je u skladu s pravom Unije. Kao ogledni primjeri u uvodnom dijelu navedeni su govor mržnje, teroristički i diskriminirajući sadržaj, dijeljenje slika koje prikazuju seksualno zlostavljanje djece, nezakonito dijeljenje privatnih slika bez pristanka, uhođenje na internetu, prodaja nesukladnih ili krivotvorenih proizvoda, prodaja proizvoda ili pružanje usluga kojima se povrjeđuje pravo o zaštiti potrošača, neovlašteno korištenje materijala zaštićenog autorskim pravom, nezakonita ponuda usluga smještaja i nezakonita prodaja živih životinja.<sup>16</sup>

Nezakonit sadržaj nije istovjetan kaznenom djelu i može se odnositi na bilo koju zabranu, bez obzira na to izaziva li njezina povreda kaznenu, prekršajnu ili građansko-upravnu odgovornost. Naposljetku, nije li riječ o kaznenim djelima određenim zajedničkim pravom Europske unije, kao što je stavljanje na raspolaganje alata za napade na informacijske sustave,<sup>17</sup> javno poticanje na terorizam<sup>18</sup> ili širenje dječje pornografije,<sup>19</sup> pojedini sadržaj u jednoj državi članici može predstavljati kazneno djelo, u drugoj tek uz ostvarenje dodatnih uvjeta, a u trećoj biti dopušten.

Predmetna rascjepkanost prava u pogledu određivanja kaznenih djela i općenito dosega nezakonitog dovela je do upućivanja kritika o nedostatku jasne definicije u Aktu o digitalnim uslugama onoga što je zabranjeno.<sup>20</sup> Međutim, navedenim izvorom prava nisu se mogle prijeći granice nadležnosti Europske unije<sup>21</sup> i unificirati nacionalna prava u onim područjima koja nisu zajednička. Umjesto toga u čl. 9. st. 2. istog Akta normirano je da obvezni sadržaj naloga uključuje obrazloženje zašto su informacije nezakonit sadržaj, s upućivanjem na konkretnu odredbu (prava Europske unije ili) nacionalnog prava, dok se

---

<sup>16</sup> Odjeljak 12. uvida Akta o digitalnim uslugama.

<sup>17</sup> Čl. 7. Direktive 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, Službeni list Europske unije, br. L218/8, 14. kolovoza 2013.

<sup>18</sup> Čl. 5. Direktive (EU) 2017/541 Europskog parlamenta i Vijeća od 15. ožujka 2017. o suzbijanju terorizma i zamjeni Okvirne odluke Vijeća 2002/475/PUP i o izmjeni Odluke Vijeća 2005/671/PUP, Službeni list Europske unije, br. L 88/6, 31. ožujka 2017.

<sup>19</sup> Čl. 5. Direktive 2011/93/EU Europskog parlamenta i Vijeća od 13. prosinca 2011. o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije te o zamjeni Okvirne odluke Vijeća 2004/68/PU, Službeni list Europske unije, br. L 335/1, 17. prosinca 2011.

<sup>20</sup> Usp. Turillazzi, A., Taddeo, M., Floridi, L., Casolari, F., *The Digital Services Act: an analysis of its ethical, legal, and social implications*, Law, Innovation and Technology, vol. 15, br. 1/2023, str. 94; Rojszczak, M., *op. cit.* (bilj. 15), str. 47.

<sup>21</sup> Usp. čl. 3. i 4. Ugovora o funkcioniranju Europske unije (pročišćena verzija), Službeni list Europske unije, br. C 202/49, 7. lipnja 2016.

teritorijalno područje primjene ograničava na ono što je nužno za ostvarivanje ciljeva naloga. Posljedično, ne radi li se o nezakonitosti sadržaja proizašlog iz zajedničkog prava Europske unije ili međunarodnog prava, nalog bi načelno trebao biti ograničen na područje one države članice koja ga je izdala.<sup>22</sup> Budući da se izdani nalog u skladu s čl. 9. st. 3. i 4. Akta o digitalnim uslugama dostavlja nacionalnom koordinatorskom tijelu za digitalne usluge, a on ga proslijeđuje ostalim koordinatorskim tijelima država članica, nema zapreke da nadležno tijelo u drugoj državi izda novi nalog kojim bi se djelovalo i na njezinu teritoriju.

Iako same odredbe Akta o digitalnim uslugama omogućuju brzo i učinkovito uklanjanje sadržaja za koji je očito da predstavlja kazneno djelo, postojat će i slučajevi u kojima je izdavanje naloga za djelovanje protiv nezakonitog sadržaja ostvarivo tek nakon opsežnog utvrđivanja relevantnih okolnosti i analize primjenjivog prava. U hrvatskom Kaznenom zakonu to se osobito odnosi na situacije u kojima kaznenog djela nema, iako su ostvarena njegova zakonska obilježja, postoji li pored legitimnog interesa zaštite pravnog dobra koje je objekt kaznenog djela i drugi, pretežniji, legitimni interes, kao što je pravo na javnu dostupnost određenih podataka ili zaštita žrtve kaznenog djela.<sup>23</sup> Ocjena predstavlja li ono što je preneseno, pohranjeno ili objavljeno kazneno djelo pritom često nije moguća uvidom u sam sporni sadržaj, bez prikupljanja podataka o identitetu primatelja usluge, njegovim motivima ili nastupjelim posljedicama.

Također, u odnosu na kaznena djela koja nisu univerzalna i u pojedinim državama ulaze u područje slobode izražavanja, nalogima za djelovanje protiv nezakonitog sadržaja ne izbjegava se potencijalni konflikt zakonodavstava u kojem se može naći izvanoeuropski pružatelj usluge. Primjerice, američki sud i ranije je odbijao izvršiti francuski nalog za uklanjanje nacističke memorabilije s aukcijske web-stranice dostupne korisnicima u Francuskoj, gdje je bila nezakonita, ali je u Sjedinjenim Američkim Državama zaštićena Prvim amandmanom na Ustav.<sup>24</sup>

U pogledu procesnih jamstava svaki nalog za djelovanje protiv nezakonitog sadržaja sadržava informacije o mehanizmima pravne zaštite dostupni-

---

<sup>22</sup> Usp. odjeljak 36. uvoda Akta o digitalnim uslugama.

<sup>23</sup> Usp. za kazneno djelo uvrde čl. 148.a Kaznenog zakona, odavanja i neovlaštenog pri-  
bavljanja poslovne tajne čl. 262. st. 3. Kaznenog zakona, odavanja službene tajne čl. 300. st. 2.  
Kaznenog zakona, neovlaštenog otkrivanja sadržaja izvidne ili dokazne radnje čl. 307.a st. 3.  
Kaznenog zakona.

<sup>24</sup> Usp. Hadas, R., International Internet Jurisdiction; Whose Law is Right? Yahoo!, Inc.  
v. La Ligue Contr. La Ligue Contre le Racisme et L e le Racisme et L'Antisemitisme, 169 F  
Antisemitisme, 169 F. Supp. Supp. 2d 1182 (N.D. Cal. 2001), Florida Journal of International  
Law, vol. 15, br. 2/2002, str. 302–308; Kelly, A., Yahoo! Inc. v. La Ligue Contre le Racisme  
et l' Antisemitisme 379 F.3d 1120 (9TH CIR. 2004), DePaul Journal of Art, Technology &  
Intellectual Property Law, vol. 15, br. 1/2004, str. 257–264.

ma pružatelju usluga posredovanja i primatelju usluge koji je dao sadržaj.<sup>25</sup> Najkasnije u trenutku provedbe ili, ako je to primjenjivo, u trenutku koji je tijelo izdavatelj navelo u nalogu pružatelj usluga posredovanja o zaprimanju i provedbi naloga dostavlja primatelju usluga obrazloženu obavijest s uputom o dostupnoj pravnoj zaštiti i opisu teritorijalnog područja primjene.<sup>26</sup>

Onemogućavanje ili ograničavanje pristupa nezakonitom sadržaju po prirodi je vidljivo primatelju usluge koji ga je dostavio radi daljnjeg prijenosa ili pohrane i implicira da je njegova aktivnost otkrivena, neovisno o tome je li mu dostavljena obavijest i koje je tijelo izdalo nalog. Stoga izvršenje naloga za djelovanje protiv nezakonitog sadržaja može imati za posljedicu ometanje prikupljanja dokaza u tekućem kaznenom predmetu, osobito posebnih dokaznih radnji kao što su presretanje računalnih podataka i simulirana prodaja ili otkup predmeta; promjenu načina počinjenja kaznenog djela korištenjem drugog pružatelja usluge; poduzimanje mjera sakrivanja identiteta od strane počinitelja ili čak ugrožavanje života i osobne sigurnosti pouzdanika, prikrivenih istražitelja ili žrtava. Uvod Akta o digitalnim uslugama stoga sadrži pojašnjenje da se obveza da nalozi sadržavaju obrazloženje zašto su informacije nezakonit sadržaj ili dostava obavijesti primatelju usluga mogu prilagoditi primjenjivom nacionalnom kaznenoprocесnom pravu.<sup>27</sup>

Nalog za djelovanje protiv nezakonitog sadržaja nije prvi usporediv institut na razini Europske unije. Njegov je prethodnik nalog za uklanjanje, normiran Uredbom (EU) 2021/784 Europskog parlamenta i Vijeća od 29. travnja 2021. o borbi protiv širenja terorističkog sadržaja na internetu,<sup>28</sup> u odnosu na koji je Hrvatska donijela i provedbeni zakon.<sup>29</sup> Područje je primjene potonjeg naloga s jedne strane uže s obzirom na to da su njegovi adresati samo pružatelji usluga smještaja informacija na poslužitelju. Međutim, kako se radi o nezakonitom sadržaju koji je kazneno djelo temeljem zajedničkog prava Europske unije, nalog proizvodi pravni učinak u svim državama članicama, a popraćen je i dodatnim mehanizmima zaštite od ometanja kaznenog postupka (čuvanje kroz određeno vrijeme uklonjenog ili onemogućenog sadržaja, odgoda informiranja pružatelja sadržaja iz razloga povezanih s javnom sigurnosti).

---

<sup>25</sup> Čl. 9. st. 2. toč. a) Akta o digitalnim uslugama.

<sup>26</sup> Čl. 9. st. 5. Akta o digitalnim uslugama.

<sup>27</sup> Odjeljak 34. uvoda Akta o digitalnim uslugama.

<sup>28</sup> Službeni list Europske unije, br. L 172/79, 17. svibnja 2021.

<sup>29</sup> Zakon o provedbi Uredbe (EU) 2021/784 Europskog parlamenta i Vijeća od 29. travnja 2021. o borbi protiv širenja terorističkog sadržaja na internetu, Narodne novine, br. 83/22.

## 2.2. Pretraga računalnog sustava

Nastojanje da se pružatelji usluga posredovanja obvežu na uklanjanje ili činjenje nedostupnim sadržaja koji je pohranjen i(li) objavljen od strane njihovih klijenata, a predstavlja kazneno djelo, prvotno se pojavljuje u okviru kaznenog postupka, kao integralni dio dokazne radnje pretrage računalnog sustava. Različito od Akta o digitalnim uslugama, u kojem je fokus na ulozi pružatelja usluge posredovanja u informacijskom društvu i području na kojem se usluge nude, kod pretrage računalnog sustava isti poslovni subjekt relevantan je samo kao imatelj posjeda ili kontrole nad medijem na koji su primatelji usluge pohranili računalne podatke. Posljedično, fokus je na lokaciji opreme pružatelja usluge i prikupljanju dokaza o kaznenom djelu, što otvara pitanje jurisdikcije za poduzimanje postupovnih radnji kada se računalni sustav fizički ne nalazi na teritoriju države čija tijela provode kazneni postupak.

Poslužitelj pružatelja usluge posredovanja obuhvaćen je pojmom uređaja koji služe prikupljanju, pohranjivanju i prijenosu podataka računalnim komunikacijama kao objekata dokazne radnje pretrage iz čl. 257. st. 1. hrvatskog Zakona o kaznenom postupku. Međutim, ta vrsta računala u pravilu se ne može oduzeti prilikom pretrage, ne samo zbog fizičke veličine već i zbog nerazmjerne štete koja bi prekidanjem usluge nastala samom pružatelju i brojnim klijentima koji su na isti poslužitelj zakonito pohranili podatke i trebaju im za daljnju uporabu. Ujedno, već samo oduzimanje velikih nositelja podataka ili cijelih računalnih instalacija samo radi prikupljanja male količine podataka smatra se protivnim načelima minimalne prisile i razmjernosti.<sup>30</sup>

Polazeći od toga da se oduzimanje računalnih podataka razlikuje od oduzimanja fizičkih predmeta, čl. 19. st. 3. toč. d) Konvencije o kibernetičkom kriminalu<sup>31</sup> Vijeća Europe iz 2001. obvezuje članice da poduzmu mjere za ovlašćivanje tijela koje provodi pretragu na činjenje nepristupačnim ili odstranjivanje računalnih podataka iz računalnog sustava kojemu je pristupljeno. Prema popratnom obrazloženju, mjere se odnose na kriptiranje ili druge tehnološke postupke kojima se svakome uskraćuje pristup podacima postoji li opasnost od nastanka štete za društvo, među ostalim kada je podatak ili njegov sadržaj nezakonit, kao u slučaju dječje pornografije.<sup>32</sup>

Obveza Republike Hrvatske da ukloni pojedini sadržaj proizlazi i iz pravne stečevine Europske unije. Sukladno čl. 25. Direktive 2011/93/EU Europskog

---

<sup>30</sup> Council of Europe, Computer-related crime (Recommendation No.9(89) on computer related crime and final report of the European Committee on Crime problems, Strasbourg 1990, str. 73.

<sup>31</sup> Narodne novine, međunarodni dio, br. 9/2002.

<sup>32</sup> Odjeljak 198., Council of Europe, Explanatory report to the Convention on Cybercrime, 23. XI. 2001.

parlamenta i Vijeća od 13. prosinca 2011. o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije te o zamjeni Okvirne odluke Vijeća 2004/68/PU, države članice, među ostalim, poduzimaju potrebne mjere kako bi osigurale žurno uklanjanje internetskih stranica s poslužitelja koji se nalaze na njihovu području, a koje sadrže ili šire dječju pornografiju. Pored preventivne uloge, navedena odredba ima za svrhu i umanjene sekundarne viktimizacije žrtve.<sup>33</sup> Analogne obveze država članica u odnosu na internetski sadržaj koji predstavlja javno poticanje na kazneno djelo terorizma proizlaze iz čl. 21. Direktive (EU) 2017/541 Europskog parlamenta i Vijeća od 15. ožujka 2017. o suzbijanju terorizma i zamjeni Okvirne odluke Vijeća 2002/475/PUP i o izmjeni Odluke Vijeća 2005/671/PUP.

S druge strane, tijelu koje poduzima pretragu poslužitelja prema hrvatskom kaznenoprocесnom pravu preostaje kopirati potrebne računalne podatke o nezakonitom sadržaju na drugi medij primjenom odredbi o privremenom oduzimanju predmeta iz čl. 263. st. 1. i 3. Zakona o kaznenom postupku (snimanje u realnom vremenu). Izričitu zakonsku ovlast naložiti pružatelju usluge da takve podatke nakon izuzimanja dokaza odstrani s poslužitelja ili učini nedostupnim nema. Naime, kada je i propisano obvezno oduzimanje ili uništenje određenih predmeta, primjerice u odnosu na računalne podatke i pornografski materijal kojeg je objekt dijete iz čl. 163. st. 4., čl. 164. st. 5. i čl. 165. st. 2. Kaznenog zakona, izostaje procesnopravna podloga, jer radnje hitnog uništavanja opasnih predmeta iz čl. 190. Zakona o kaznenom postupku te trajnog oduzimanja i uništavanja iz čl. 181. st. 7., čl. 556. i čl. 556.a Zakona o kaznenom postupku, polaze od pretpostavke da su predmeti prethodno bili privremeno oduzeti prijenosom posjeda nad stvarima u fizičkom obliku.

Posljedično, tijelo koje poduzima pretragu za činjenje nedostupnim ili odstranjivanje sadržaja koji predstavlja kazneno djelo s poslužitelja upućeno je na suradnju pružatelja usluge, utemeljenu na ovlasti uskraćivanja usluge zbog povrede pretplatničkog ugovora od strane klijenta. Onemogućavanjem pristupa pohranjenim podacima za koje ima saznanja da su nezakoniti domaći pružatelj usluge ujedno otklanja i svoju odgovornost u smislu čl. 18. Zakona o elektroničkoj trgovini,<sup>34</sup> kojim je implementirana 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).<sup>35</sup> Dodatna je mogućnost, sukladno čl. 22. Pravilnika o ustrojstvu i upravljanju vršnom nacionalnom

---

<sup>33</sup> Europski parlament, Izvješće o provedbi Direktive 2011/93/EU Europskog parlamenta i Vijeća od 13. prosinca 2011. o suzbijanju seksualnog zlostavljanja i seksualnog iskorištavanja djece i dječje pornografije, br. A8-0368/2017 od 27. studenog 2017.

<sup>34</sup> Narodne novine, br. 173/03, 67/08, 36/09, 130/11, 30/14, 32/19.

<sup>35</sup> Službeni list Europske unije, br. L 178/1, 17. srpnja 2020. (dalje u tekstu Direktiva o elektroničkoj trgovini).

internetskom domenom,<sup>36</sup> od CARNET-a kao upravitelja domene zatražiti da se ona zbog zlouporabe privremeno deaktivira, pa i obriše. Međutim, na taj se način može spriječiti isključivo pristup sadržaju pohranjenom na domeni koja završava sufiksom .hr, bez obzira na lokaciju poslužitelja.

Zakon o kaznenom postupku stoga reflektira opće probleme povezane s okolnošću da norme o računalnim podacima i elektroničkim dokazima često ne odražavaju njihovu nematerijalnu prirodu. U tom smislu, radi usklađivanja s obvezama preuzetim ratifikacijom Konvencije o kibernetičkom kriminalu, nedostaje i izričita ovlast da se sadržaj koji predstavlja kazneno djelo prilikom pretrage računalnog sustava, ako uzimanje samog poslužitelja ili drugog uređaja nije moguće, nakon kopiranja podataka obriše ili na drugi način učini nedostupnim nakon snimanja. S obzirom na to da navedena mjera predstavlja miješanje u pravo korisnika na slobodu izražavanja, ali i pravo pružatelja usluga na slobodu poduzetništva,<sup>37</sup> a u užem smislu nije u funkciji prikupljanja dokaza o kaznenom djelu, mora imati drugu legitimnu svrhu – primjerice u nizozemskom kaznenoprocesnom pravu to je sprječavanje postojećeg i daljnjih kaznenih djela,<sup>38</sup> u belgijskom suprotnost podataka s javnim redom i moralom ili otklanjanje opasnosti za cjelovitost računalnih sustava i podataka,<sup>39</sup> u francuskom zabranjenost posjedovanja ili uporabe podataka, odnosno otklanjanje opasnosti za sigurnost ljudi i imovine.<sup>40</sup>

Navedeno uklanjanje ili onemogućavanje pristupa sadržaju koji predstavlja kazneno djelo, kao premošćivanje nemogućnosti oduzimanja poslužitelja pružatelja usluge, supsidijarne je naravi i vezano je uz odredbe o pretrazi računalnog sustava. U tom smislu nije sporna prihvatljivost tog pravnog instituta radi li se o poslužitelju lociranom na području one države koja provodi pretragu. Međutim, kaznenoprocesnim pravima država članica Europske unije, uključujući i hrvatsko, uglavnom nije normirano proširenje te dokazne radnje na računo koje se fizički nalazi u inozemstvu, a i ondje gdje to jest slučaj, primjerice u Belgiji, takva pretraga ograničava se na kopiranje podataka.<sup>41</sup>

---

<sup>36</sup> Narodne novine, br. 83/23.

<sup>37</sup> Usp. Frosio, G., Geiger, C., Taking fundamental rights seriously in the Digital Services Act's platform liability regime, *European Law Journal*, vol. 29, br. 1–2/2023, str. 46–54, 58–60.

<sup>38</sup> Čl. 125o nizozemskog Zakona o kaznenom postupku, *Wetboek van Strafvordering*, <https://wetten.overheid.nl/BWBR0001903/2024-07-01> (26. 7. 2024.).

<sup>39</sup> Čl. 339.bis belgijskog Zakona o kaznenom postupku, *Code d'Instruction Criminelle*, [https://www.ejustice.just.fgov.be/img/\\_l/pdf/1808/11/17/1808111701M\\_F.pdf](https://www.ejustice.just.fgov.be/img/_l/pdf/1808/11/17/1808111701M_F.pdf) (11. 8. 2024.).

<sup>40</sup> Čl. 56. francuskog Zakona o kaznenom postupku, *Code de procédure pénale*, [https://www.legifrance.gouv.fr/codes/section\\_lc/LEGITEXT000006071154/LEGISCTA000006098229/#LEGISCTA000006098229](https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000006098229/#LEGISCTA000006098229) (11. 8. 2024.).

<sup>41</sup> Usp. Glavić, I., Neposredna međunarodna suradnja prema Drugom dodatnom protokolu uz Konvenciju o kibernetičkom kriminalu, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 29, broj 2/2022, str. 450–452.

Upravo u navedenim situacijama naloži za djelovanje protiv nezakonitog sadržaja iz Akta o digitalnim uslugama mogu, izostane li dobrovoljna suradnja stranog pružatelja usluge, biti učinkovito sredstvo za uklanjanje ili onemogućavanje pristupa sadržaju čija je javna objava i predmetom konkretnog kaznenog postupka.

### **2.3. Mogućnost integracije Akta o digitalnim uslugama u kazneno procesno pravo**

Nalog pružateljima usluga posredovanja da, neovisno o pretrazi računala, ograniče ili onemoguće pristup sadržaju koji je pohranjen na zahtjev prima-telja usluge nije uobičajen kao postupak *sui generis* u kaznenim procesnim pravima država članica Europske unije. Umjesto toga uklanjanje s interneta nezakonitog sadržaja koji predstavlja pojedina kaznena djela pretežito se na-stojalo ostvariti posebnim propisima o obvezivanju pružatelja usluga da hitno poduzmu mjere nakon prigovora upućenog od trećih osoba. Njemačka je ta-kav zakon donijela 2017.,<sup>42</sup> a Austrija 2020.<sup>43</sup> Navedena rješenja, osobito nje-mačko, predmetom su brojnih kritika, od kojih je osnovna postojanje rizika da će pružatelj usluga pod prijetnjom visoke novčane kazne pretjerano blokirati sadržaj te obuhvatiti i onaj koji nije nezakonit, a dodatno se navode i zanema-rivanje povezanosti svojeg i drugih pravnih sustava,<sup>44</sup> omogućavanje nepošte-nih trgovačkih praksi,<sup>45</sup> nedostatak sudskog nadzora,<sup>46</sup> nesuglasje prekratkog roka za djelovanje s oslobođenjem pružatelja usluga od odgovornosti u smislu

---

<sup>42</sup> Zakon o zaštiti prava na društvenim mrežama, Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), [https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/BGBl/BGBl\\_NetzDG.pdf?\\_\\_blob=publicationFile&v=3](https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/BGBl/BGBl_NetzDG.pdf?__blob=publicationFile&v=3) (5. 9. 2024.).

<sup>43</sup> Zakon o komunikacijskim platformama, Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen (Kommunikationsplattformen-Gesetz – KoPl-G), [https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA\\_2020\\_I\\_151/BGBLA\\_2020\\_I\\_151.pdf#sig](https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2020_I_151/BGBLA_2020_I_151.pdf#sig) (5. 9. 2024.).

<sup>44</sup> Bello, B. G., Tackling online hate speech from a European perspective: Potentials and challenges of inter-legality, Oñati Socio-Legal Series, vol. 13, br. 4/2023, str. 1398.

<sup>45</sup> Sagar, S., Hoffmann, T., Intermediary Liability in the EU Digital Common Market – from the E-Commerce Directive to the Digital Services Act, IDP – revista de Internet, derecho y política = revista d’Internet, dret i política, br. 34/2021, str. 5.

<sup>46</sup> Tan, Z. Y., Saving the Sinking Ship: How the United States Can Create an Effective Content Moderation Policy by Looking Abroad, Hastings Law Journal, vol. 73, br. 2/2022, str. 542–543; Zurth, P., The German NetzDG as Role Model or Cautionary Tale? Implications for the Debate on Social Media Liability, Fordham Intellectual Property, Media & Entertainment Law Journal, vol. 31, br. 4/2021, str. 1132–1135.

čl. 14. Direktive o elektroničkoj trgovini.<sup>47</sup> U konačnici, pokušaj normiranja u Francuskoj 2020.<sup>48</sup> završio je odlukom Ustavnog suda o ukidanju pretežitog dijela zakona izglasanog u Nacionalnoj skupštini kao neprikladnog, nepotrebnog i nerazmjernog miješanja u slobodu izražavanja i komunikacije.<sup>49</sup>

Kao iznimka, prema nizozemskom Zakonu o kaznenom postupku,<sup>50</sup> za sva kaznena djela s propisanom kaznom zatvora u trajanju od četiri ili više godina te za druga posebno nabrojena kaznena djela u ovlasti je državnog odvjetnika, po odobrenju suca istrage i nakon što je pružatelju komunikacijske usluge dana mogućnost da bude saslušan, naložiti mu poduzimanje razumno očekivanih mjera činjenja nedostupnim pohranjenih ili prenesenih podataka ako je to nužno za prestanak postojećeg i sprječavanje daljnjih kaznenih djela. Adresati navedene norme fizičke su i pravne osobe koje u okviru svoje profesije ili poslovanja omogućuju primateljima svojih usluga da komuniciraju koristeći automatiziranu obradu podataka ili u tu svrhu pohranjuju podatke. Nepostupanje pružatelja usluga sukladno zaprimljenom nalogu predstavlja kazneno djelo *sui generis*,<sup>51</sup> osim ako je u istom predmetu osumnjičen da je počinio kazneno djelo u odnosu na nezakonit sadržaj.<sup>52</sup>

Vezano uz naloge za djelovanje protiv nezakonitog sadržaja, još je manje razloga za nužnost njihova normiranja kao dijela hrvatskog kaznenoproglašnog prava. Zakon o kaznenom postupku konstruiran je tako da obuhvaća radnje koje se provode na području Republike Hrvatske, domaćem zrakoplovu ili brodu, dok se nalog iz Akta o digitalnim uslugama izdaje i pružatelju koji ih nudi na području Europske unije, pa i kada nema poslovni nastan na području države članice. Nadalje, teritorijalno mogu biti primjenjivi na cijelu Europsku uniju. U tom slučaju i nije presudno pozivanje na neko od kazne-

---

<sup>47</sup> Ukrow, J., Core problems of public international law regarding the regulation of the “media sector” with respect to possible tensions with EU law, u: Cole, M. D., Ukrow, J., Etteldorf, C. (ur.), On the Allocation of Competences between the European Union and its Member States in the Media Sector – Zur Kompetenzverteilung zwischen der Europäischen Union und den Mitgliedstaaten im Mediensektor, Baden-Baden 2021, str. 323.

<sup>48</sup> [https://www.assemblee-nationale.fr/dyn/15/textes/115t0419\\_texte-adopte-seance](https://www.assemblee-nationale.fr/dyn/15/textes/115t0419_texte-adopte-seance) (18. 8. 2024.).

<sup>49</sup> Décision n° 2020-801 DC du 18 juin 2020, <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031998> (18. 8. 2024.).

<sup>50</sup> Čl. 125.p u svezi s čl. 67. i čl. 138g, *op. cit.* (bilj. 38).

<sup>51</sup> Usp. Kooijmans, T., Mevis, P., ICT in the context of criminal procedure: The Netherlands, *Revue électronique de l'AIDP / Electronic Review of the IAPL / Revista electrónica de la AIDP*, 2014, dostupno na: str. 13, <https://www.penal.org/sites/default/files/files/RA%20-%2011.pdf> (28. 7. 2024.).

<sup>52</sup> Usp. Lodder, A. R., Sandvliet, K. E., Measures of Blocking, Filtering and Take-Down of Illegal Internet Content: The Netherlands – Report for the Council of Europe (Legal Opinion), November 16, 2015, dostupno na: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2732764](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732764) (11. 8. 2024.).

nih djela propisanih Kaznenim ili drugim zakonom, već na kaznenopravne inkriminacije zajedničkog prava Europske unije ili međunarodnih konvencija. Zaštitne mjere naloga za djelovanje protiv nezakonitog sadržaja također nisu kaznenopravne prirode. Obveza da izdavalatelj obrazloži zašto su informacije nezakonit sadržaj s upućivanjem na konkretnu normu (što može biti i odredba posebnog dijela Kaznenog zakona), kao i pravo na učinkovit pravni lijek, prvenstveno su u funkciji zaštite slobode izražavanja. U praksi Europskog suda za ljudska prava zabrana pristupa, filtriranje i blokiranje sadržaja na internetu razmotreno je u kontekstu čl. 10. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda,<sup>53</sup> odnosno slobode izražavanja, koja obuhvaća pravo širenja informacija, kao i pravo drugih korisnika da ih prime. Zbog sveobuhvatne prirode takve zabrane, da bi se ostvario uvjet nužnosti u demokratskom društvu, ne samo da odluka nadležnog tijela mora imati dostatno obrazloženje<sup>54</sup> već se prethodno mora ispitati može li se isti učinak postići manje opterećujućom mjerom, a radi izbjegavanja zlouporaba osigurati i učinkovita sudska zaštita.<sup>55</sup> Sama zabrana mora biti strogo usmjerena prema nezakonitom sadržaju te ne smije proizvesti proizvoljni ili ekscesivni učinak, odnosno kolateralnu štetu za zakoniti sadržaj ili *web*-stranice.<sup>56</sup>

U svakom slučaju, nalog za djelovanje protiv nezakonitog sadržaja koji predstavlja kazneno djelo fleksibilna je mjera trenutačnog domaćeg i (li) prekograničnog učinka, reducirana na utvrđivanje objektivnih obilježja inkriminacije, uz osiguranje ravnoteže u odnosu na zaštitu slobode izražavanja. Navedena odluka može se izdati i postoje li stvarne ili pravne zapreke za kazneni progon, primjerice zbog nemogućnosti utvrđivanja počinitelja, primjene imuniteta, nedostatka prijedloga oštećenika ili ako je zakonska obilježja kaznenog djela ostvarilo dijete. Bez obzira na to što se nalogom posredno postiže prevencija kaznenih djela i zaštita žrtve, sam za sebe ne ostvaruje svrhu kažnjavanja u smislu čl. 41. Kaznenog zakona jer nedostaju elementi izražavanja društvene osude, jačanja svijesti o pogibeljnosti kaznenih djela i pravednosti kažnjavanja počinitelja te omogućavanja počinitelju ponovnog uključivanja u društvo. Budući da izdavanje naloga također nema za posljedicu izricanje kazne primatelju usluge, na njega se ne nadovezuju mehanizmi zaštite prava okrivljenika u kaznenom postupku.

Kazneni postupak, s druge strane, podrazumijeva protek vremena do pravomoćne odluke, dokazivanje subjektivnih obilježja kaznenog djela, osiguranje prava obrane i tek djelomično učinkovite mjere prisile prema pružatelju

---

<sup>53</sup> Narodne novine, Međunarodni dio, br. 18/1997, 6/1999, 14/2002, 13/2003, 9/2005, 1/2006, 2/2010, 13/2017.

<sup>54</sup> Usp. Ooo Flavus i drugi protiv Rusije, 2020.

<sup>55</sup> Usp. Ahmet Yildirim protiv Turske, 2012.

<sup>56</sup> Usp. Vladimir Kharitanov protiv Rusije, 2020.

usluga, kada se kumulativno radi o domaćem poslovnom subjektu te sadržaju prenesenom ili pohranjenom na poslužitelju koji se fizički nalazi u Hrvatskoj. U tom smislu istodobno vođenje dva odvojena, paralelna postupka ima svoje prednosti jer se jednim trenutačno otklanja protupravno stanje, a drugim odlučuje o kaznenopravnoj odgovornosti onoga koji je takvo stanje prouzročio. Osigura li se pritom primjeren i pravovremen protok informacija na relaciji tijelo otkrivanja i progona kaznenih djela – izdavatelj naloga za djelovanje protiv nezakonitog sadržaja te obratno, kazneni postupak i navedeni instrument Akta o digitalnim uslugama mogu biti kompatibilni i međusobno nadopunjujući.

## 2.4. Provedba Akta o digitalnim uslugama

Provedbenim propisima u Njemačkoj,<sup>57</sup> Austriji<sup>58</sup> i Francuskoj<sup>59</sup> nalozi za djelovanje protiv nezakonitog sadržaja, kao i ostali pravni instituti Akta o digitalnim uslugama, normirani su odvojeno od kaznenoprocenog prava. Ovlaštenim izdavateljima određene su centralizirane agencije nadležne za nadzor mrežnih djelatnosti, ujedno i nacionalni koordinatori za digitalne usluge. Iznimno, u Austriji su nalozi dodatno integrirani u sumarni građanski postupak normiran Zakonom o suzbijanju mržnje na internetu. U tom ih slučaju izdaje sud nadležan za odlučivanje o tužbi oštećenika. Prema obrazloženju prijedloga Popratnog zakona uz Akt o digitalnim uslugama,<sup>60</sup> smisao navede-

---

<sup>57</sup> Zakon o digitalnim uslugama, Digitale-Dienste-Gesetz, <https://www.gesetze-im-internet.de/ddg/BJNR0950B0024.html> (25. 8. 2024.).

<sup>58</sup> Popratni zakon uz Akt o digitalnim uslugama, Bundesgesetz, mit dem das Koordinator-für-digitale-Dienste-Gesetz erlassen und das KommAustria-Gesetz, das E-Commerce-Gesetz, das Allgemeine bürgerliche Gesetzbuch, das Urheberrechtsgesetz, das Gerichtsgebührengesetz, das Mediengesetz, die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz, das EU-JZG, das Auslieferungs- und Rechtshilfegesetz und das Telekommunikationsgesetz 2021 geändert werden (DSA-Begleitgesetz – DSA-BegG) [https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA\\_2023\\_I\\_182/BGBLA\\_2023\\_I\\_182.html](https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2023_I_182/BGBLA_2023_I_182.html) (26. 7. 2024.).

<sup>59</sup> Zakon o sigurnosti i regulaciji digitalnog prostora, Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, [https://www.legifrance.gouv.fr/download/pdf?id=1kWAYP9AsPTUa6nbDcb3Sq3PzXyh2U2x\\_naRfEud\\_Wg=](https://www.legifrance.gouv.fr/download/pdf?id=1kWAYP9AsPTUa6nbDcb3Sq3PzXyh2U2x_naRfEud_Wg=) (15. 8. 2024.).

<sup>60</sup> Ministerialentwurf betreffend Bundesgesetz, mit dem das Koordinator-für-digitale-Dienste-Gesetz erlassen und das KommAustria-Gesetz, das E-Commerce-Gesetz, das Allgemeine bürgerliche Gesetzbuch, das Urheberrechtsgesetz, das Gerichtsgebührengesetz, das Mediengesetz, die Strafprozeßordnung 1975, das Staatsanwaltschaftsgesetz, das EU-JZG, das Auslieferungs- und Rechtshilfegesetz und das Telekommunikationsgesetz 2021 geändert werden (DSA-Begleitgesetz – DSA-BegG), 302/ME XXVII. GP – Ministerialentwurf – Erläuterungen, str. 3, [https://www.parlament.gv.at/dokument/XXVII/ME/302/fname\\_1590553.pdf](https://www.parlament.gv.at/dokument/XXVII/ME/302/fname_1590553.pdf) (26. 7. 2024.).

nog jest potreba brzog uklanjanja nezakonitog sadržaja na internetu, što nije bilo ostvarivo dostavom sudske odluke inozemnom pružatelju usluge prema postojećem pravu Europske unije. Zbog nedavnog početka obavljanja ovlasti zasad nisu dostupni podaci o načinu interakcije nadležnih centraliziranih agencija s redarstvenim i pravosudnim tijelima.

Različito od naprijed navedenog poredbenog prava, Nacrtom prijedloga Zakona o provedbi Akta o digitalnim uslugama izdavanje naloga za djelovanje protiv nezakonitog sadržaja koji predstavlja kazneno djelo (i prekršaj) u nadležnosti je državnog odvjetništva i policije, dok o (nesuspenzivnom) prigovoru pružatelja i primatelja usluge posredovanja u žurnom postupku odgovarajućom primjenom Prekršajnog zakona u prvom stupnju odlučuje Općinski prekršajni sud u Zagrebu, a u drugom Visoki prekršajni sud Republike Hrvatske.

Premda se može činiti da je sjedinjavanjem funkcija izdavatelja naloga i tijela nadležnih za otkrivanje i progon kaznenih djela ubrzan postupak djelovanja protiv nezakonitog sadržaja koji predstavlja kazneno djelo, nasuprot sjedinjavanju funkcija izdavatelja i nacionalnog koordinatora za digitalne usluge kakvo postoji u poredbenom pravu, tome nije tako. S jedne strane, nacionalni koordinatorsko tijelo je koje isključivo raspolaže podacima o izdanim inozemnim nalogima za djelovanje protiv nezakonitog sadržaja, kao i nalogima za davanje informacija o kojima će biti riječ u narednom poglavlju, te ujedno tijelo koje obavijest o izdanom nalogu mora proslijediti u inozemstvo. Zbog navedenog ne može se izbjeći njegova bitna uloga koordinacije s policijom i državnim odvjetništvom, prije i poslije izdavanja naloga, u svakom pojedinačnom slučaju. Policija i državno odvjetništvo s jedne strane raspolažu boljim znanjem o propisanim kaznenim djelima, ali upitno je ostvaruje li se izdavanjem naloga s njihove strane prednost kod kaznenih djela koja su eklatantna, osobito s obzirom na nedostatak stručnog znanja u području elektroničkih komunikacija i usluga posredovanja. Nadalje, za neometanu suradnju s pružateljem usluga posredovanja presudni su faktori stjecanje rutine i pravna sigurnost tom poslovnom subjektu da komunicira s ovlaštenom osobom, što je lakše ostvarivo putem centraliziranog nacionalnog tijela za izdavanje svih naloga za djelovanje protiv nezakonitog sadržaja.

Naposljetku, osim što provedba planiranog hrvatskog rješenja iziskuje promjenu propisa o organizaciji rada i nadležnosti unutar policije i državnog odvjetništva, ostaju otvorena pitanja prikladnosti državnog odvjetništva i policije kao izdavatelja naloga za kaznena djela koja se progone privatnom tužbom i ona za koja je u tijeku kazneni postupak koji vodi nadležni kazneni sud.

Dodatni problem predstavlja i okolnost da su preostali ovlašteni izdavatelji naloga Agencija za zaštitu osobnih podataka, Carinska uprava (za povredu prava intelektualnog vlasništva), Državni inspektorat i Ministarstvo zdravlja. Unatoč načelnoj obvezi međusobne suradnje nadležnih tijela te ulozi

Hrvatske regulatorne agencije za mrežne djelatnosti kao nacionalnog koordinatora za digitalne usluge, opisana disperzija nije prikladno rješenje s obzirom na preklapanje nadležnosti. Primjerice, prodaja krivotvorenih lijekova putem internetskih platformi istodobno može predstavljati opasnost za zdravlje, intelektualno vlasništvo, slobodu trgovine i prava potrošača, a za njezino suzbijanje nadležni mogu biti policija, državno odvjetništvo, Carinska uprava, Ministarstvo zdravstva i Državni inspektorat. Sam Nacrt prijedloga Zakona o provedbi Akta o digitalnim uslugama ne sadrži odredbe o rješavanju negativnog sukoba nadležnosti, dok su odredbe o pozitivnom sukobu ionako suviše ne raspolažu li sva nadležna tijela podatkom o namjeri izdavanja naloga drugog ovlaštenog izdavatelja. Posljedično, postoji realna opasnost da nijedno tijelo ne izda nalog ne raspolažući podacima iz inozemstva ili smatrajući da ga treba izdati netko drugi, da više tijela izda naloge u odnosu na isti sadržaj i pružatelja usluge ili da izvršenje naloga za djelovanje protiv nezakonitog sadržaja upravnog tijela, uslijed brisanja ili činjenja sadržaja nedostupnim, omete provođenje tekućih i potencijalnih izvida kaznenih djela ili posebnih dokaznih radnji. S obzirom na navedeno, u ovom trenutku boljima se pokazuju norme poredbenog prava o centralizaciji izdavanja tih naloga.

### **3. PRIBAVLJANJE PODATAKA O PRIMATELJU (KORISNIKU) USLUGE**

#### **3.1. Odredbe Akta o digitalnim uslugama**

Nalog za davanje informacija iz čl. 10. Akta o digitalnim uslugama također izdaje nadležno pravosudno ili upravno tijelo (uključujući tijelo za izvršavanje zakonodavstva) države članice i dostavlja ga kontaktnoj točki pružatelja usluga posredovanja za izravnu elektroničku komunikaciju. *Ratio* naloga jest identifikacija određenog primatelja ili određenih primatelja usluge temeljem čijeg je zahtjeva nezakonit sadržaj prenesen, odnosno privremeno ili kroz određeno vrijeme smješten na poslužitelju pružatelja usluge. Kako bi se ostvarila ta svrha, nalog mora sadržavati podatke temeljem kojih pružatelj usluge može utvrditi na kojeg se primatelja odnosi, kao i obrazloženje zašto je nužan i razmjeran<sup>61</sup> za utvrđivanje usklađenosti primatelja usluge s primjenjivim pravom Europske unije ili nacionalnim pravom koje je u skladu s pravom Unije. Normirana je i iznimka o izostanku tog obrazloženja postoje li razlozi povezani sa sprječavanjem, istragom, otkrivanjem i progonom kaznenih djela.

---

<sup>61</sup> U izvorniku na hrvatskom jeziku navedeno kao „potreban i primjeren“ (engl. *necessary and proportionate*, njem. *erforderlich und verhältnismäßig*).

S obzirom na to da je nužnost i razmjernost naloga u funkciji sprječavanja prekomjernog tereta za pružatelja usluge i izbjegavanja neopravdanog učinka na prava i zakonite interese trećih osoba,<sup>62</sup> proizlazi da se time ne otklanja sama obveza izdavatelja da prethodno ispita jesu li ostvareni navedeni uvjeti, već se osigurava očuvanje tajnosti pojedinih faza otkrivanja i progona kaznenih djela koja proizlazi iz pravnih sustava država članica.

U ostalim dijelovima nalog za davanje informacija procesno je istovjetan nalogu za djelovanje protiv nezakonitog sadržaja, primjerice u pogledu obveze izdavatelja da ta odluka sadrži upućivanje na relevantnu pravnu osnovu, informacije o izdavatelju i mehanizmima pravne zaštite dostupnima pružatelju i primatelju usluge; kao i obveze pružatelja usluge posredovanja da obavijesti primatelja usluge o zaprimljenom nalogu, njegovoj provedbi i mogućnosti dostupne pravne zaštite, najkasnije u trenutku provedbe ili, ako je to primjenjivo, u trenutku koji je navelo tijelo koje je izdalo nalog.

### **3.2. Vrste podataka o primatelju usluge i uvjeti njihova pribavljanja**

Sukladno čl. 10. st. 2. toč. b) Akta o digitalnim uslugama, nalogom za davanje informacija mogu se tražiti samo one prikupljene u trenutku pružanja usluge i nad kojima pružatelj ima kontrolu. Ipak, samim Aktom nisu pobliže određene kategorije takvih informacija, kao i pravne osnove držanja podataka od strane pružatelja usluga. Iznimku predstavlja institut sljedivosti trgovca iz čl. 30., prema kojem su pružatelji internetskih platformi kojima se potrošačima omogućuje sklapanje ugovora na daljinu dužni od trgovca prethodno pribaviti te provjeriti ime, fizičku i adresu elektroničke pošte, telefonski broj, presliku identifikacijskog dokumenta ili elektroničku identifikaciju, podatke o računu za plaćanje te podatke iz registra te to zadržati i šest mjeseci nakon isteka ugovornog odnosa s trgovcem. Međutim, teoretski dolaze u obzir i podaci koje je pružatelj usluge prikupio i sačuvao moderirajući nezakonit sadržaj na vlastitu inicijativu ili po prijavi treće osobe; regulirajući ugovorni odnos s klijentom (uključivo ispostavu računa za pružene usluge i rješavanje korisničkih prigovora); ili postupajući prema obvezi preventivnog zadržavanja podataka koja proizlazi iz nacionalnog prava.

Osim općeg zahtjeva da nalog za davanje informacija mora biti nužan i razmjernan, Akt o digitalnim uslugama ne sadrži referencu o tome mogu li se informacije za utvrđivanje identiteta pribaviti za sav nezakonit sadržaj, neovisno o pravnoj osnovi zbog koje ih pružatelj usluge drži. Djelomičan odgovor vezano uz nezakonit sadržaj kod usluga prijenosa podataka i privremenog

---

<sup>62</sup> Odjeljak 31. uvoda Akta o digitalnim uslugama.

smještaja informacija na poslužitelju nalazi se u Direktivi 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama)<sup>63</sup> i pripadajućim stajalištima Suda Europske unije. Tumačeći čl. 15. st. 1. Direktive, Sud je izdvojio dvije kategorije podataka relevantnih za identifikaciju korisnika elektroničkih komunikacijskih sredstava putem pružatelja usluga. Prvi su oni o građanskom identitetu (ime, prezime, fizička adresa i dr.), za koje se u nacionalnom pravu država članica može propisati obveza pružatelja usluga da ih preventivno zadrže bez vremenskog ograničenja, u svrhu borbe protiv kaznenih djela i zaštite javne sigurnosti općenito; a drugi IP adrese dodijeljene izvoru veze, za koje se može propisati da ih pružatelji usluga preventivno zadrže za razdoblje vremenski ograničeno na ono što je strogo nužno, u svrhu borbe protiv teških kaznenih djela i sprečavanja ozbiljnih prijetnji javnoj sigurnosti.<sup>64</sup>

Podaci o građanskom identitetu primatelja usluge pritom se sadržajno preklapaju s pojmom pretplatničkih podataka iz čl. 18. st. 3. Konvencije o kibernetičkom kriminalu, za koje zbog niske razine miješanja u pravo na privatnost i slobodu komunikacije i ranije nije bilo prijeporno da ih tijekom izvida može prikupiti policija bez posebnih ograničenja u pogledu težine kaznenog djela.<sup>65</sup> Navedena ovlast policije proizlazi i iz čl. 263. st. 1. u svezi s čl. 261. st. 2. hrvatskog Zakona o kaznenom postupku. S druge strane, odlukom Suda Europske unije doneseno je stajalište da IP adrese dodijeljene izvoru veze predstavljaju dio podataka o prometu komunikacije, manje osjetljiv od ostalih jer same za sebe nisu podobne da otkriju bilo kakvu informaciju o trećim osobama koje su bile u kontaktu s osobom na izvoru komunikacije. Ipak, njihovo prikupljanje i obveza pružatelja usluga da ih zadrže kroz određeno vrijeme doseže razinu ozbiljnog zadiranja u prava na privatnost i zaštitu osobnih podataka, jer su tada podobne za iscrpno praćenje tijeka pregledavanja i internetske aktivnosti primatelja usluge.<sup>66</sup>

Posljedično, nema zapreke da se pretplatnički podaci pribave nalogom za davanje informacija iz Akta o digitalnim uslugama za sva kaznena djela, neovisno o tome jesu li prikupljeni i sačuvani uslijed reguliranja poslovnog odnosa ili obveze preventivnog zadržavanja koja proizlazi iz nacionalnog pra-

---

<sup>63</sup> Službeni list Europske unije, br. L 201/37, 31. srpnja 2002., izmijenjena Direktivom 2009/136/EZ od 25. studenoga 2009., Službeni list Europske unije, br. L 337/11, 18. prosinca 2009.

<sup>64</sup> Usp. Sud Europske unije, br. C511/18, C512/18 i C520/18 (La Quadrature du Net i dr. protiv Premier ministre i dr.) od 6. listopada 2020.; Glavić, I., *op. cit.* (bilj. 41), str. 445–446.

<sup>65</sup> Odjeljak 171. Council of Europe, Explanatory report to the Convention on Cybercrime, 23. XI. 2001.; Sud Europske unije, br. C-207/16 (Ministerio fiscal) od 2. listopada 2018., odjeljci 58., 63.

<sup>66</sup> Usp. Sud Europske unije, C511/18, C512/18 i C520/18 (La Quadrature du Net i dr. protiv Premier ministre i dr.) od 6. listopada 2020., odjeljci 152.–156.

va ili instituta sljedivosti trgovca. Različito od navedenog, taj nalog može se izdati u odnosu na IP adrese dodijeljene izvoru veze bez ograničenja u težini kaznenog djela ako su prikupljene i sačuvane radi reguliranja poslovnog odnosa s klijentom, a samo za teška kaznena djela određena nacionalnim pravom ako su predmetom obveznog preventivnog zadržavanja. Vezano uz hrvatsko pravo, preventivno zadržavanje navedenih IP adresa normirano je čl. 53. i 54. Zakona o elektroničkim komunikacijama,<sup>67</sup> ali još uvijek sjedinjeno s drugim podacima o prometu za koje se prema tumačenju Suda Europske unije ne može propisivati preventivno zadržavanje. S obzirom na navedeno, kao i s obzirom na duljinu roka zadržavanja od čak dvanaest mjeseci, postoji potreba za reformom prava elektroničkih komunikacija, kao i čl. 339.a Zakona o kaznenom postupku temeljem kojeg se takvi podaci od pružatelja javnih komunikacijskih usluga pribavljaju kao dokaz u kaznenom postupku, odnosno čl. 68. Zakona o policijskim poslovima i ovlastima<sup>68</sup> temeljem kojeg se pribavljaju kao izvor saznanja tijekom izvida.<sup>69</sup>

### **3.3. Korelacija s europskim nalogom za dostavljanje elektroničkih dokaza**

Nepunih godinu dana od Akta o digitalnim uslugama donesena je Uredba (EU) 2023/1543 Europskog parlamenta i Vijeća od 12. srpnja 2023. o europskim nalogima za dostavljanje i europskim nalogima za čuvanje elektroničkih dokaza u kaznenim postupcima i za izvršenje kazni zatvora nakon kaznenog postupka,<sup>70</sup> s primjenom od 18. kolovoza 2026. Premda su osnovna načela i uvjeti izdavanja naloga za dostavljanje elektroničkih dokaza preslikani po uzoru na europski istražni nalog, taj institut predstavlja suštinski brži i učinkovitiji način prikupljanja dokaza zbog činjenice da se upućuje izravno pružateljima usluga u drugoj državi članici, kao i kratkoće rokova te reduciranosti osnova za odbijanje izvršenja.<sup>71</sup> U obuhvatu primjene europski nalog za dostavljanje elektroničkih dokaza preklapa se s nalogom za davanje informacija jer su njime obuhvaćeni svi pružatelji usluga posredovanja,<sup>72</sup> a prema pratećoj

---

<sup>67</sup> Narodne novine, br. 76/2022, 14/2024.

<sup>68</sup> Narodne novine, br. 76/2009, 92/2014, 70/2019.

<sup>69</sup> Usp. Vrhovni sud Republike Hrvatske, I Kž 290/17-4 od 1. lipnja 2017., I Kž-Us 21/2020-4 od 27. veljače 2020., Kzz 2/2020-3 od 8. svibnja 2020.

<sup>70</sup> Službeni list Europske unije, br. L 191/118 od 28. srpnja 2023. (u daljnjem tekstu Uredba o europskim nalogima za dostavljanje i čuvanje elektroničkih dokaza).

<sup>71</sup> Čl. 7., čl. 10., čl. 12. Uredbe o europskim nalogima za dostavljanje i čuvanje elektroničkih dokaza.

<sup>72</sup> Usp. definiciju pružatelja usluga iz čl. 3. st. 3. Uredbe o europskim nalogima za dostavljanje i čuvanje elektroničkih dokaza.

direktivi oni subjekti izvan Europske unije, nude li usluge na njezinu području i pritom postoji bitna veza, dužni su u jednoj od država članica imenovati zastupnika za primanje i postupanje po izdanim nalogima.<sup>73</sup>

Analogno pravnom shvaćanju Suda Europske unije normirane su dvije kategorije informacija relevantnih za identifikaciju primatelja usluge. Prva su pretplatnički podaci, koji uključuju ime i prezime, datum rođenja i kontaktne podatke, nadnevak prve registracije, podatke o vrsti i trajanju usluge, identifikatore korištene pri njezinoj aktivaciji (*telefonski broj, MAC adresa, broj SIM kartice...*), profilne podatke (*korisničko ime, ime na ekranu, profilna fotografija...*), podatke o kreditnoj ili debitnoj kartici te preslike ugovora i dostavljene dokumentacije.<sup>74</sup> Druga su kategorija podaci zatraženi isključivo u svrhu identifikacije korisnika, a uključuju IP adresu dodijeljenu izvoru veze te, ako je ona istovremeno dodijeljena većem broju osoba, dodatne identifikatore, kao što su izvorišni portovi i vremenski žigovi.<sup>75</sup>

Europski nalog za dostavljanje elektroničkih dokaza kao pravosudnu mjeru prekograničnog prikupljanja dokaza, ovisno o nacionalnom pravu, može izdati sud ili državno odvjetništvo, a policija samo uz prethodnu ili u hitnim slučajevima naknadnu potvrdu tih tijela.<sup>76</sup> Premda u pogledu pretplatničkih podataka i podataka zatraženih isključivo u svrhu identifikacije korisnika nalog načelno nije ograničen vrstom i težinom kaznenog djela, može se izdati samo pod uvjetom da bi sličan nalog mogao biti izdan pod istim uvjetima u usporedivom domaćem slučaju.<sup>77</sup> Posljedično, izdavatelj naloga vezan je ograničenjima propisanim domaćim kaznenoprocenim pravom, osobito katalogom teških kaznenih djela za koja se mogu zatražiti preventivno zadržane IP adrese dodijeljene izvoru veze.

Osnovna razlika između europskog naloga za dostavljanje elektroničkih dokaza i naloga za davanje informacija iz Akta o digitalnim uslugama izdanim inozemnom pružatelju usluga sastoji se u njihovoj dokaznoj snazi. Naime, podaci dobiveni temeljem Akta o digitalnim uslugama nisu upotrebljivi kao dokaz u kaznenom postupku uslijed izostanka prethodne ocjene neovisnog

---

<sup>73</sup> Direktiva (EU) 2023/1544 Europskog parlamenta i Vijeća od 12. srpnja 2023. o utvrđivanju usklađenih pravila za imenovanje imenovanih subjekata koji imaju poslovni nastan i za imenovanje pravnih zastupnika za potrebe prikupljanja elektroničkih dokaza u kaznenim postupcima, Službeni list Europske unije, br. L 191/181, 28. srpnja 2023.

<sup>74</sup> Odjeljak F(a) priloga I. Uredbe o europskim nalogima za dostavljanje i čuvanje elektroničkih dokaza.

<sup>75</sup> Usp. čl. 3. st. 10. Uredbe o europskim nalogima za dostavljanje i čuvanje elektroničkih dokaza.

<sup>76</sup> Usp. čl. 4. st. 1. Uredbe o europskim nalogima za dostavljanje i čuvanje elektroničkih dokaza.

<sup>77</sup> Usp. čl. 5. st. 2., 3. Uredbe o europskim nalogima za dostavljanje i čuvanje elektroničkih dokaza.

pravosudnog tijela o dopustivosti takva prikupljanja informacija u svrhu dokazivanja u sličnom domaćem slučaju, kao i nemogućnosti djelovanja nadležnog tijela države članice u kojoj pružatelj usluge ima poslovni nastan ili zastupnika pojavi li se sumnja u zadiranje u imunitete i povlastice te slobodu izražavanja u medijima u toj državi.<sup>78</sup>

Nalozi za davanje informacija stoga će poslužiti redarstvenim vlastima ponajprije kao inicijalne informacije o postojanju osnova sumnje na počinitelja kaznenog djela koji djeluje na njihovu području bez obzira na to jesu li sama inicirala izdavanje takvih naloga ili su im dostavljeni podaci pribavljeni nalogom drugog nadležnog domaćeg ili inozemnog tijela. U tom smislu predstavljaju izvor saznanja za identifikaciju osumnjičenika s posljedičnim prekidanjem protupravnog stanja njegovim uhićenjem i(li) pokretanjem kaznenog postupka daljnjim dokaznim radnjama, uključujući i sam europski nalog za dostavljanje elektroničkih dokaza.

Nalozi za davanje informacija imaju vrijednost i kada su upućeni pružatelju usluge posredovanja sa sjedištem u državi članici koja je izdala nalog. Različito od klasičnih naloga za dostavu podataka domaćim poslovnim subjektima otprije normiranih nacionalnim pravom, nalozi iz Akta o digitalnim uslugama zajedno sa zaprimljenim informacijama dostavljaju se nacionalnom koordinatoru za digitalne usluge, koji ih je dužan dalje proslijediti ostalim nacionalnim koordinatorima putem jedinstvenog informacijskog sustava čija je uspostava u nadležnosti Europske komisije.<sup>79</sup> Navedeno omogućuje da nadležna tijela u svakoj državi članici utvrde osobu za koju postoji sumnja da je radnju dostavljanja nezakonitog sadržaja pružatelju usluge ostvarila na njezinoj teritoriji. Pored toga, analizom informacija o primatelju usluge koji je bio predmet većeg broja domaćih ili inozemnih naloga može se utvrditi i sumnja na namjernu disperziju nezakonitog sadržaja putem raznih pružatelja usluga, a poduzetu u cilju prikrivanja kaznenog djela ili okolnosti pod kojima je ono počinjeno.

---

<sup>78</sup> Usp. čl. 10. st. 5. Uredbe o europskim nalogima za dostavljanje i čuvanje elektroničkih dokaza.

<sup>79</sup> Usp. Provedbena uredba Komisije (EU) 2024/607 od 15. veljače 2024. o praktičnim i operativnim rješenjima za funkcioniranje sustava za razmjenu informacija u skladu s Uredbom (EU) 2022/2065 Europskog parlamenta i Vijeća („Akt o digitalnim uslugama“), Službeni list Europske unije, serije L, 16. veljače 2024.

#### **4. OBVEZA PRUŽATELJA USLUGA SMJEŠTAJA INFORMACIJA NA POSLUŽITELJU DA PRIJAVI KAZNENO DJELO**

##### **4.1. Odredbe Akta o digitalnim uslugama**

Člankom 18. Akta o digitalnim uslugama normirano je da, sazna li pružatelj usluge smještaja informacija na poslužitelju za bilo koji podatak koji dovodi do sumnje da je počinjeno, ili da je vjerojatno da će biti počinjeno, ili je u tijeku počinjenje kaznenog djela koje uključuje prijetnju životu ili sigurnosti osobe, o svojoj sumnji odmah obavješćuje tijela za izvršavanje zakonodavstva<sup>80</sup> ili pravosudna tijela i dostavlja im sve dostupne relevantne informacije. Smatrat će se da je nadležna za zaprimanje prijave ona država članica za koju postoji sumnja da je u njoj počinjeno kazneno djelo, ili je počinjenje u tijeku, ili je vjerojatno da će biti počinjeno; odnosno država članica u kojoj boravi ili se nalazi osumnjičenik ili žrtva. Ne može li s dovoljnom sigurnošću utvrditi nadležnu državu članicu, pružatelj usluge smještaja informacija na poslužitelju o svojoj sumnji obavješćuje redarstveno tijelo države članice u kojoj ima poslovni nastan, ili u kojoj njegov pravni zastupnik ima boravište ili poslovni nastan, ili obavješćuje Europol ili oboje.

Kao primjeri kaznenih djela u odnosu na koja postoji obveza podnošenja kaznene prijave u uvodu Akta o digitalnim uslugama navedena su ona koja proizlaze iz zajedničkog prava Europske unije o inkriminiranju kaznenih djela terorizma, trgovanja ljudima te seksualnog zlostavljanja ili iskorištavanja djece i dječje pornografije.<sup>81</sup> Prije Akta o digitalnim uslugama institut obvezne prijave terorističkog sadržaja, ali u užem opsegu, jer je morao uključivati neposrednu opasnost za život, bio je normiran člankom 14. stavkom 5. Uredbe (EU) 2021/784 Europskog parlamenta i Vijeća od 29. travnja 2021. o borbi protiv širenja terorističkog sadržaja na internetu.

Najznačajniji izvor saznanja o sumnji na kazneno djelo koje uključuje prijetnju životu ili sigurnosti osoba predstavlja institut pouzdanih prijavitelja iz čl. 22. Akta o digitalnim uslugama, čijim obrazloženim prijavama pružatelji internetskih platformi moraju dati prioritet te ih obraditi i o njima odlučiti bez nepotrebne odgode. Riječ je o neovisnim subjektima certificiranim od nacionalnih koordinatora za digitalne usluge, koji posjeduju posebno stručno znanje i sposobnost za potrebe otkrivanja, utvrđivanja i prijavljivanja nezakonitog sadržaja. Ipak, svaki pružatelj usluga smještaja informacija na poslužitelju dužan je sukladno čl. 16. Akta o digitalnim uslugama omogućiti bilo kojem pojedincu ili subjektu da ga obrazloženom i potkrijepljenom izjavom obavijesti o prisutnosti

---

<sup>80</sup> Pod tim pojmom podrazumijevaju se redarstvena tijela.

<sup>81</sup> Usp. odjeljak 56. uvoda Akta o digitalnim uslugama.

određenih informacija u njegovoj usluzi za koje smatra da predstavlja nezakonit sadržaj, ali obrada takvih prijava nije deklarirana prioritonom.

Samo propisivanje upravne, prekršajne ili kaznenopravne odgovornosti pružatelja usluga smještaja informacija na poslužitelju koji postupe protivno obvezi podnošenja kaznene prijave na zakonodavcima je država članica. Člankom 52. Akta o digitalnim uslugama općenito je određeno da nacionalne sankcije za povredu neke odredbe moraju biti djelotvorne, proporcionalne i odvraćajuće, ali pritom najviši iznos novčane kazne zbog nepostupanja u skladu s nekom od obveza iz Akta može doseći 6 % godišnjeg svjetskog prihoda pružatelja usluga posredovanja u prethodnoj financijskoj godini (odnosno 1 % za dostavljanje netočnih, nepotpunih ili obmanjujućih informacija).

Ono što je propisano čl. 6. i čl. 16. st. 3. tog izvora zajedničkog prava Europske unije te je neposredno primjenjivo u državama članicama jest izuzeće od „svih vrsta“<sup>82</sup> odgovornosti pružatelja usluga smještaja informacija na poslužitelju, uključujući i kaznenopravnu,<sup>83</sup> ako nakon stjecanja saznanja ili spoznaje o nezakonitom sadržaju pohranjenom na zahtjev primatelja usluge žurno djeluje kako bi ga uklonio ili mu onemogućio pristup. Obavijesti trećih osoba dovest će do stjecanja takva stvarnog znanja ili spoznaje ako savjesnom pružatelju usluga omogućuju da bez detaljnog pravnog ispitivanja utvrdi nezakonitost relevantne aktivnosti ili informacija.

Pružatelj usluga smještaja informacija na poslužitelju saznanje o nezakonitoj prirodi sadržaja načelno može crpiti i iz istraga provedenih na vlastitu inicijativu.<sup>84</sup> Kako bi se spriječilo odvrćanje od poduzimanja takvih dobrovoljnih mjera, člankom 7. Akta o digitalnim uslugama, po uzoru na pravo Sjedinjenih Američkih Država, normirana je tzv. klauzula „Dobrog samaritanca“, tj. imunitet osobe koja u dobroj vjeri i bez pravne obveze pomaže drugome,<sup>85</sup> kojom se sprječava da spoznaja proizašla iz predmetnih *bona fide* aktivnosti dovede do gubitka izuzeća od odgovornosti. Stoga je konstituiranje kaznenopravne odgovornosti pružatelja usluga bitno suženo ako mu sumnja na kazneno djelo nije ukazana inicijativom trećih osoba te će postojati samo utvrdi li se neki od općih uvjeta neprihvatljivosti oslobođenja od odgovornosti (primjerice, namjerna suradnja s primateljem usluga radi poduzimanja neza-

---

<sup>82</sup> Odjeljak 17. uvoda Akta o digitalnim uslugama.

<sup>83</sup> Usp. Wilman, F., The EU's system of knowledge-based liability for hosting service providers in respect of illegal user content – between the e-Commerce Directive and the Digital Services Act, JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law, vol. 12, br 3/2021, str. 321.

<sup>84</sup> Usp. odjeljak 22. uvoda Akta o digitalnim uslugama.

<sup>85</sup> Usp. G'sell, F., The Digital Services Act: a General Assessment, u von Ungern-Sternberg, A. (ur.), Content Regulation in the European Union – The Digital Services Act, Schriften des IRDT – Trier Studies On Digital Law, Volume 1, Trier 2023, str. 90–92.

konitih aktivnosti,<sup>86</sup> djelovanje primatelja usluge na temelju ovlaštenja ili pod kontrolom pružatelja usluge iz čl. 6. st. 2. Akta o digitalnim uslugama).

#### 4.2. Posljedice Akta o digitalnim uslugama na poredbeno pravo

Mandatorno prijavljivanje kaznenih djela od strane privatnih subjekata u poredbenom pravu i teoriji nije općeprihvaćeno, a gdje postoji, normira se radi prevencije ozbiljne i neposredne opasnosti, produljenja dužnosti pojedinih osoba da brinu o ranjivim kategorijama žrtava ili potrebe povećanog obraćanja redarstvenim vlastima u slučajevima rijetko prijavljivanih kaznenih djela u odnosu na koja, s obzirom na prirodu i prouzročene posljedice, država ima pojačanu dužnost djelovanja.<sup>87</sup>

Vezano konkretno za pružatelje usluga smještaja na poslužitelju, obveza da podnesu kaznenu prijavu za sadržaj koji je dostavio primatelj usluge pretežito se odnosi na nacionalne sustave nekih europskih i izvan europskih država o suzbijanju dječje pornografije te iskorištavanja i zlostavljanja djece na internetu.<sup>88</sup> Nešto šireg dometa bila je novela njemačkog Zakona o zaštiti prava na društvenim mrežama iz 2021.,<sup>89</sup> kojom su velike platforme bile obvezane podnijeti prijavu Saveznom uredu za kriminalitet za pojedina teška kaznena djela – samo da bi iduće godine, povodom tužbi *Googlea* i *Mete*, Upravni sud u Kölnu donio interimnu odluku da takva odredba predstavlja kršenje načela zemlje podrijetla iz čl. 3. st. 2. Direktive o elektroničkoj trgovini, odnosno da države članice normiranjem obveze prijavljivanja kaznenih djela ne mogu ograničiti slobodu pružanja usluga informacijskog društva pružatelju iz druge države članice (konkretno Irske, u kojoj je bilo europsko sjedište tužitelja).<sup>90</sup> Kao posljedica izravne primjene čl. 18. Akta o digitalnim uslugama takvo zakonsko rješenje postalo je suvišno i stavljeno je izvan snage time da se obavijesti o sumnji na kazneno djelo koje uključuje prijetnju životu i sigurnosti osobe opet podnose Saveznom uredu za kriminalitet, koji je u tu svrhu kreirao posebnu *web*-stranicu s poveznicom na portal za *online*-registraciju pružate-

---

<sup>86</sup> Odjeljak 20. uvoda Akta o digitalnim uslugama.

<sup>87</sup> Usp. Pivaty, A., Wolters, P. T. J., The obligation to notify suspicions of criminal offences in the Digital Services Act under scrutiny, *Boom Strafbblad*, br. 5/2022, str. 188–189, 191.

<sup>88</sup> Usp. OECD Digital Economy Papers No. 357, Transparency Reporting on Child Sexual Exploitation and Abuse Online, September 2023, str. 36–39.

<sup>89</sup> Čl. 7. Zakona o borbi protiv desnog ekstremizma i zločina mržnje, *Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität*, [https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/BGBl/Bgbl\\_Bekaempfung\\_Rechtsextremismus\\_Hasskriminalitaet.pdf?\\_\\_blob=publicationFile&v=3](https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/BGBl/Bgbl_Bekaempfung_Rechtsextremismus_Hasskriminalitaet.pdf?__blob=publicationFile&v=3) (24. 8. 2024.).

<sup>90</sup> Usp. VG Köln, Beschluss vom 1. 3. 2022 – 6 L 1354/21.

lja usluga.<sup>91</sup> Prema obrazloženju uz prijedlog provedbenog zakona, pružatelj usluge smještaja informacija na poslužitelju nije obavezan provoditi kaznenu istragu, ali mora pružiti sve relevantne podatke koji su mu dostupni. Ovlašćivanje centraliziranog tijela da zaprimi sve kaznene prijave normirano je radi izbjegavanja udvostručenja posla i stvaranja uvjeta za žurno poduzimanje hitnih radnji jer će ono provjerama utvrditi mjesnu nadležnost i proslijediti predmet nadležnoj ustrojstvenoj jedinici.<sup>92</sup>

Različito od njemačkog provedbenog propisa, kojim nisu određene kazne za propust pružatelja usluge da podnese kaznenu prijavu, u Austriji je povreda čl. 18. Akta o digitalnim uslugama sankcionirana upravnom kaznom maksimalnog iznosa dopustivog člankom 52. Akta o digitalnim uslugama,<sup>93</sup> dok se u Francuskoj radi o kaznenom djelu *sui generis* s propisanom kaznom zatvora do jedne godine i novčanom kaznom od 250 000 eura, koja se za pravnu osobu s obrascem kršenja obveze može uvećati do 6 % godišnjih prihoda ostvarenih na svjetskoj razini u protekloj godini.<sup>94</sup>

#### **4.3. Kaznena odgovornost za neprijavljivanje kaznenog djela u hrvatskom pravu?**

Kazneno djelo neprijavljivanja pripremanja kaznenog djela iz čl. 301. Kaznenog zakona čini tko zna da se priprema počinjenje kaznenog djela s propisanom kaznom zatvora od najmanje pet godina i to ne prijavi u vrijeme kad je još bilo moguće spriječiti njegovo počinjenje, a djelo bude pokušano ili počinjeno. Smatra se da je navedenom normom obuhvaćeno i neprijavljivanje započetog kaznenog djela postoji li mogućnost sprječavanja njegova dovršenja.<sup>95</sup>

---

<sup>91</sup> [https://www.bka.de/EN/OurTasks/Remit/CentralAgency/DigitalServicesAct/DigitalServicesAct\\_node.html](https://www.bka.de/EN/OurTasks/Remit/CentralAgency/DigitalServicesAct/DigitalServicesAct_node.html) (26. 7. 2024.).

<sup>92</sup> Usp. Deutscher Bundestag, 20. Wahlperiode, Drucksache 20/10031, 15. 1. 2024, Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze, str. 72–73.

<sup>93</sup> Usp. čl. 5. st. 2. toč. 8., čl. 6. Popratnog zakona uz Akt o digitalnim uslugama, DSA-Begleitgesetz – DSA-BegG, *op. cit.* (bilj. 58).

<sup>94</sup> Usp. čl. 48. Zakona o sigurnosti i regulaciji digitalnog prostora, Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, *op. cit.* (bilj. 59).

<sup>95</sup> Pavlović, Š., Kazneni zakon (zakonski tekst, obrazloženje, poveznice, komentar, sudska praksa), Rijeka, 2012, str. 648.

Kazneno djelo neprijavljivanja počinjenog kaznenog djela iz čl. 302. Kaznenog zakona čini tko zna da je počinjeno kazneno djelo za koje je propisana kazna zatvora od najmanje deset godina i to ne prijavi iako zna da bi takvom prijavom bilo omogućeno ili znatno olakšano otkrivanje djela ili počinitelja. Prema stavku 2. istog članka kaznenopravno odgovara i službena ili odgovorna osoba ne prijavi li počinjenje kaznenog djela za koje je saznala obavljajući svoju dužnost radi li se o kaznenom djelu za koje pokretanje kaznenog postupka nije prepušteno privatnoj tužbi ili progonu po prijedlogu.

Tekst Kaznenog zakona upućuje na to da navedena kaznena djela nečinjenja konstituiraju kaznenopravnu odgovornost pružatelja usluga smještaja informacija na poslužitelju i njihovih odgovornih osoba za povredu obavješćivanja nadležnog tijela o sumnji na kazneno djelo. Međutim, ona je pritom ograničena odredbama Akta o digitalnim uslugama kao izvora zajedničkog prava Europske unije izravno primjenjivog u državama članicama. U tom smislu presudno je smatra li se da je odgovorna fizička osoba pružatelja usluge imala stvarno znanje ili spoznaju da se radi o kaznenom djelu koje uključuje prijetnju životu ili sigurnosti osobe, odnosno sukladno čl. 16. st. 3. Akta o digitalnim uslugama da u objektivnom smislu za donošenje istog zaključka nije bilo potrebno detaljno pravno ispitivanje. Kaznenopravna odgovornost moguća je i ostane li identitet odgovorne fizičke osobe pružatelja usluge nepoznat. Premda je tijekom donošenja Zakona o odgovornosti pravnih osoba za kaznena djela to bilo sporno pitanje, prevladavajući je stav u hrvatskoj pravnoj teoriji i sudskoj praksi kako je odgovornost pravne osobe moguća i ne uspije li se utvrditi o kojoj bi konkretnoj fizičkoj osobi bila riječ.<sup>96</sup>

Prema pružatelju usluge smještaja informacija na poslužitelju kao pravnoj osobi za kaznena djela neprijavljivanja pripremanja i počinjenog kaznenog djela neće se moći primijeniti čl. 10. st. 5. Zakona o odgovornosti pravnih osoba za kaznena djela o zapriječenju novčanoj kazni u iznosu do 10 % ukupnog godišnjeg prihoda ostvarenog u poslovnoj godini koja prethodi godini

---

<sup>96</sup> Usp. Novoselec, P., Odgovornost pravnih osoba za kaznena djela - značajna novost u hrvatskom pravnom sustavu, *Pravo u gospodarstvu* br. 4/2002, str. 118; Đurđević, Z., Kaznena odgovornost i kazneni postupak prema pravnim osobama u Republici Hrvatskoj, *Hrvatski ljetopis za kazneno pravo i praksu*, vol. 10, br. 2/2003, str. 754; Novosel, D., Zakon o odgovornosti pravnih osoba za kaznena djela u primjeni, u *Aktualna pitanja kaznenog zakonodavstva*, Zagreb 2008, str. 133–135; Moslavac, B., Kaznenopravna odgovornost pravnih osoba, *Hrvatska pravna revija*, vol. 9, br. 4/2009, str. 91–92; Vuletić, I., Novokmet, A., Tomićić, Z., Izazovi posebnog dijela kaznenog prava zbog razvoja umjetne inteligencije uz poseban osvrt na hrvatsko kazneno pravo, *Zbornik Pravnog fakulteta u Zagrebu*, vol. 74, br. 1/2024, str. 20–21; Županijski sud u Varaždinu – Stalna služba u Koprivnici, br. Kž-662/11 od 7. rujna 2011.; Županijski sud u Varaždinu, br. Kž-401/2019 od 26. studenog 2019.; suprotno u Derenčinović, D., Zakon o odgovornosti pravnih osoba za kaznena djela (s uvodnim napomenama, komentarskim bilješkama, pojmovnim kazalom i prilogima), Zagreb 2003, str. 54–55; Vrhovni sud Republike Hrvatske, broj IV Kž-32/08-3 od 1. travnja 2008.

donošenja presude, budući da je norma protivna maksimalnom iznosu novčane kazne od 6 % godišnjeg svjetskog prihoda pružatelja usluga u prethodnoj financijskoj godini, koji se, sukladno čl. 52. st. 3. Akta o digitalnim uslugama, može propisati zakonodavstvom države članice Europske unije.

Ipak, sam Kazneni zakon te općenito način na koji se kaznena djela iz čl. 301. i čl. 302. tumače u pravnoj teoriji i praksi pridonose objektivnim teškoćama i praktički krajnje reduciranom prostoru za kazneni progon odgovorne fizičke osobe, a posljedično i pružatelja usluga smještaja informacija na poslužitelju kao pravne osobe. Naime, neprijavljivanje pripremanja kaznenog djela iz čl. 301. Kaznenog zakona predstavlja *delicta communia* prilagođena kaznenopravnoj odgovornosti privatnih osoba. Posljedično, kako bi bilo počinjeno, nužno je da počinitelj „zna“ da se priprema počinjenje kaznenog djela. Smatrat će se da takvo subjektivno obilježje nije ispunjeno ako netko na temelju dostupnih mu informacija samo sumnja da se priprema počinjenje kaznenog djela ili je to mogao saznati da je bio pažljiviji i zainteresiraniji.<sup>97</sup> Subjektivno obilježje „zna“ sastavni je dio i osnovnog oblika kaznenog djela neprijavljivanja počinjenog kaznenog djela iz čl. 301. st. 1. Kaznenog zakona. Budući da pružatelji usluga smještaja informacija na poslužitelju, odnosno njihove odgovorne osobe, mahom ne poznaju i nemaju osobnih kontakata s primateljem usluge koji je pohranio sporni sadržaj, kako uopće dokazivati trenutak u kojem sumnja (koja je i kriterij za nastanak obveze obavješćivanja nadležnih tijela prema čl. 18. Akta o digitalnim uslugama) prerasta u znanje da se priprema ili da je počinjeno kazneno djelo?

Za nastanak kaznenopravne odgovornosti u smislu čl. 302. st. 2. Kaznenog zakona dovoljno je postojanje svojstva (službene ili) odgovorne osobe te da saznanje o počinjenom kaznenom djelu potječe iz obavljanja dužnosti. Navedena *delicta propria* tradicionalno su se vezivala uz kaznenoprocесnu normu da bi građani trebali, a da bi tijela državne vlasti i pravne osobe bila dužna prijaviti kazneno djelo koje se progona po službenoj dužnosti.<sup>98</sup> Nakon što je novelom iz 2013.<sup>99</sup> članak 204. Zakona o kaznenom postupku preoblikovan tako da je svatko dužan prijaviti kazneno djelo za koje se postupak pokreće po službenoj dužnosti, tumači se kako službene i odgovorne osobe imaju garantnu obvezu skrbi za zaštićena pravna dobra (konkretno pravosuđe) u svim slučajevima kada za to postoji javni interes.<sup>100</sup>

<sup>97</sup> Pavlović, Š., *op. cit.* (bilj. 95), str. 648; Derenčinović, D. u Cvitanović, L. i dr., Kazneno pravo (posebni dio), Zagreb 2018, str. 429.

<sup>98</sup> Mrčela, M., Kaznena djela protiv pravosuđa, Hrvatski ljetopis za kazneno pravo i praksu, vol. 10, br. 2/2003, str. 598; Derenčinović, D., Marginalije uz Glavu XXII. Kaznenog zakona (kaznena djela protiv pravosuđa), Pravo i porezi, vol. 14, br. 11/2005, str. 52; Pavlović, Š., *op. cit.* (bilj. 95), str. 651–652.

<sup>99</sup> Zakon o izmjenama i dopunama Zakona o kaznenom postupku, Narodne novine, br. 145/2013.

<sup>100</sup> Usp. Derenčinović, D., *op. cit.* (bilj. 97), str. 434.

Stajališta o općoj garantnoj obvezi svih službenih i odgovornih osoba da prijave počinjenje svakog kaznenog djela koje se progoni po službenoj dužnosti (osim onih za koje je potreban prijedlog oštećenika) su sporna. Premda su načelno pojmom odgovorne osobe u smislu čl. 87. st. 6. Kaznenog zakona obuhvaćene i one koje djeluju unutar pravnih osoba bez prenesenih javnih ovlasti, kakvi su i pružatelji usluga smještaja informacija na poslužitelju, ne postoji opravdani razlog zašto bi one samom činjenicom da rade u pravnoj osobi imale pojačanu dužnost zaštite pravosuđa u odnosu na druge fizičke osobe. Da službena ili odgovorna osoba počinu kazneno djelo neprijavljivanjem, saznanje o počinjenom kaznenom djelu druge osobe mora steći „obavljajući svoju dužnost“, što podrazumijeva povredu dva zaštićena pravna dobra – pravosuđa i urednog obavljanja službe ili drugog posla, zbog čega i odgovara u širem opsegu od običnih građana. *Ratio* takva dodatnog obvezivanja službenih ili odgovornih osoba da prijave počinjena kaznena djela u tome je da one s obzirom na prirodu dužnosti (u pravilu ispitivanje i pregled žrtve ili utvrđivanje nezakonitosti) stječu saznanja o kaznenim djelima i počiniteljima koje policija redovito ne bi mogla otkriti. Kako se to ne odnosi na djelatnost svih službenih ili odgovornih osoba i svako kazneno djelo koje se progoni po službenoj dužnosti, zasebnim propisima mora se pobliže odrediti o kojim je osobama riječ te kako i u odnosu na koja kaznena djela moraju podnijeti kaznenu prijavu.<sup>101</sup> U tom kontekstu, kazneno djelo neprijavljivanja počinjenog kaznenog djela iz čl. 302. st. 2. Kaznenog zakona, radi li se o odgovornoj osobi pružatelja usluga smještaja informacija na poslužitelju, može se odnositi samo na propuštanje prijavljivanja kaznenih djela koja uključuju prijetnju životu ili sigurnosti osobe. Ipak, načelna mogućnost kaznenopravne odgovornosti ne znači da će se hrvatsko kazneno zakonodavstvo moći primijeniti. Naime, propusti li kaznenu prijavu prema čl. 18. Akta o digitalnim uslugama podnijeti inozemni subjekt, neće se u smislu čl. 9. Kaznenog zakona raditi o kaznenom djelu počinjenom u Republici Hrvatskoj budući da je njegova odgovorna osoba bila dužna djelovati iz mjesta u kojem se nalazi. Primjena hrvatskog kaznenog zakonodavstva na djela počinjena u inozemstvu moguća je tek teoretski utvrdi li se u smislu čl. 14. Kaznenog zakona hrvatsko državljanstvo odgovorne osobe pružatelja usluga.

Prekršajna odgovornost za nepostupanje u skladu s čl. 18. Akta o digitalnim uslugama Nacrtom prijedloga Zakona o provedbi Akta o digitalnim uslugama nije predviđena.

---

<sup>101</sup> Npr. čl. 22. Zakona o liječništvu, Narodne novine, br. 121/03, 117/08; čl. 12. u svezi s čl. 3. st. 5. Pravilnika o postupanju i izvještavanju o nepravilnostima u upravljanju sredstvima institucija u javnom sektoru, Narodne novine, br. 78/2020; čl. 217. st. 1. u svezi s čl. 204. st. 1. te čl. 231. st. 3. Zakona o zdravstvenoj zaštiti, Narodne novine, br. 100/18, 125/19, 147/20, 119/22, 156/22, 33/23, 36/24; čl. 38. Zakona o provedbi Opće uredbe o zaštiti podataka, Narodne novine, br. 42/2018.

## 5. ZAKLJUČNA RAZMATRANJA

Nacionalnim zakonodavstvom država članica Europske unije i ranije se moglo učinkovito obvezivati domaće pružatelje usluga da surađuju s redarstvenim i pravosudnim tijelima u cilju sprječavanja, otkrivanja, progona i suzbijanja posljedica kaznenih djela počinjenih uporabom interneta. Problem je predstavljalo nametanje takvih zadaća inozemnim poslovnim subjektima, što nije bilo ostvarivo putem rascjepkanih pravnih sustava. Konvencija o kibernetičkom kriminalu pridonijela je harmonizaciji nacionalnih prava u pogledu prikupljanja dokaza o kaznenim djelima počinjenim putem računalnog sustava od domaćih pružatelja usluga posredovanja, ali njome nije obuhvaćena problematika uklanjanja ili onemogućavanja pristupa sadržaju koji predstavlja kazneno djelo mimo dokazne radnje pretrage, upućivanja neposrednih naloga za prikupljanje podataka stranim fizičkim i pravnim osobama ili obvezivanja pružatelja usluga posredovanja da prijave kazneno djelo koje namjerava počiniti ili je počinio primatelj usluge.

Dugotrajnost postupka međunarodne pravne pomoći, ali i europskih istražnih naloga, neproporcionalna potrebi žurnog djelovanja radi otkrivanja i progona kaznenih djela, uz stalan rast njihova broja i težine prouzročenih posljedica, stvorili su preduvjete da se zajedničkim europskim pravom uspostave mehanizmi izravne prekogranične suradnje pružatelja usluga posredovanja, uključujući i obvezu da, i kad kazneno djelo nije počinjeno u državi iz koje dolaze, nadležnim tijelima podnesu kaznenu prijavu ili postupe po nalogima za otkrivanje podataka nužnih za identifikaciju počinitelja, kao i za sprječavanje daljnjih posljedica uklanjanjem ili činjenjem nedostupnim spornog sadržaja.

Suradnja iz Akta o digitalnim uslugama, različito od europskih naloga za dostavljanje elektroničkih dokaza, pozicionirana je u ranu fazu, kada policija ili državno odvjetništvo tek stječu početna saznanja da se kazneno djelo uopće dogodilo i(li) tko dolazi u obzir kao osumnjičenik. Međutim, kako njihove aktivnosti već i tada zadiru u prava primatelja usluge posredovanja na privatnost komuniciranja i slobodu izražavanja, kao i u prava pružatelja usluge na obavljanje gospodarske djelatnosti, bilo je potrebno osigurati da mogu učinkovito pristupiti sudu i osporavati da se radi o kaznenom djelu.

Odredbe Akta o digitalnim uslugama pritom samo predstavljaju pravnu podlogu za ostvarivanje razmjernosti između legitimnog cilja i prava uključenih subjekata, a na nacionalnim je zakonodavcima određivanje nadležnih izdavatelja naloga i postupka učinkovite pravne zaštite koji stoji na raspolaganju primateljima i pružateljima usluga posredovanja. Na operativnoj razini nužna je uspostava sustava koordinacije kojim bi se spriječilo da prijevremeno osiguravanje tih prava ne omete postojeći ili potencijalni kazneni postupak. Osiguraju li se navedeni uvjeti, pravni instituti Akta o digitalnim uslugama omogućuju da se,

usprkos međunarodnoj prirodi digitalnih usluga i interneta, počinitelji kaznenih djela otkriju i osude, a postojeće ili potencijalne žrtve zaštite.

Premda je državama članicama bilo raspoloživo više od jedne godine za osiguranje provedbe prije nego što započne izravna primjena Akta o digitalnim uslugama, navedeni proces uglavnom se odvijao sa zakašnjenjem, a u Hrvatskoj je pred dovršenjem, barem u odnosu na određivanje nadležnih izdavatelja naloga za djelovanje protiv nezakonitog sadržaja i za davanje informacija te propisivanje načina osiguranja sudske zaštite pružatelja i primatelja usluga posredovanja. Nacrtom prijedloga Zakona o provedbi Akta o digitalnim uslugama isključivim izdavateljima naloga za djelovanje protiv nezakonitog sadržaja i za davanje informacija određeni su policija i državno odvjetništvo radi li se o kaznenim djelima. Prihvatljivost navedenog rješenja sporna je kada navedena tijela ujedno nisu nadležna za njihovo otkrivanje i progon (kod kaznenih djela koja se progone privatnom tužbom ili u odnosu na koja je u tijeku kazneni postupak koji provodi nadležni sud). Predstavlja li nezakonit sadržaj, pored kaznenog djela, povredu prekršajne, građanske ili upravne norme, posljedica predmetnog nacrta postojanje je većeg broja nadležnih izdavatelja naloga, bez konkretnih normi o načinu rješavanja sukoba nadležnosti i međusobne razmjene podataka kojom bi se spriječilo da izdavanje naloga omete tekući ili predstojeći kazneni postupak. Zaštita pružatelja i primatelja usluge nominalno je omogućena njihovim pravom da protiv izdanog naloga podnesu prigovor nadležnom prekršajnom sudu, ali je upitno hoće li to pravo u sudskoj praksi biti iluzorno ili stvarno s obzirom na to da se način na koji se može ostvariti svodi na općenito pozivanje na procesne odredbe Prekršajnog zakona, bez uzimanja u obzir da podnositelj prigovora nije u svojstvu okrivljenika. Sama povreda obveze pružatelja usluga smještaja informacija na poslužitelju da obavijeste policiju ili državno odvjetništvo o sumnji na kazneno djelo koje uključuje prijetnju životu ili sigurnosti osobe pritom nije popraćena realnom mogućnošću kaznenog progona, osobito radi li se o inozemnim poslovnim subjektima.

Slijedom navedenog, zasad je neizvjesno hoće li mogućnost izdavanja naloga za djelovanje protiv nezakonitog sadržaja i za davanje informacija na posljetku biti učinkovito iskorištena i komplementarna kaznenom postupku. Prednosti Akta o digitalnim uslugama ionako ne mogu doći do izražaja bez edukacije nadležnih službenika i dužnosnika te uspostave informatičkog sustava i protokola suradnje s nacionalnim koordinatorom za digitalne usluge i svim ostalim izdavateljima.

## LITERATURA

1. Bello, B. G., Tackling online hate speech from a European perspective: Potentials and challenges of inter-legality, *Oñati Socio-Legal Series*, vol. 13, br. 4/2023, str. 1376–1411.
2. Cvitanović, L., i dr., *Kazneno pravo (posebni dio)*, Zagreb, 2018.
3. Derenčinović, D., *Zakon o odgovornosti pravnih osoba za kaznena djela (s uvodnim napomenama, komentarskim bilješkama, pojmovnim kazalom i priložima)*, Zagreb, 2003.
4. Derenčinović, D., Marginalije uz Glavu XXII. Kaznenog zakona (kaznena djela protiv pravosuđa), *Pravo i porezi*, vol. 14, br. 11/2005, str. 50–58.
5. Đurđević, Z., Kaznena odgovornost i kazneni postupak prema pravnim osobama u Republici Hrvatskoj, *Hrvatski ljetopis za kazneno pravo i praksu*, vol. 10, br. 2/2003, str. 719–770.
6. Frosio, G., Geiger, C., Taking fundamental rights seriously in the Digital Services Act's platform liability regime, *European Law Journal*, vol. 29, br. 1–2/2023, str. 31–77.
7. Glavić, I., Neposredna međunarodna suradnja prema Drugom dodatnom protokolu uz Konvenciju o kibernetičkom kriminalu, *Hrvatski ljetopis za kaznene znanosti i praksu*, vol. 29, broj 2/2022, str. 433–460.
8. G'sell, F., The Digital Services Act: a General Assessment, u von Ungern-Sternberg, A. (ur.), *Content Regulation in the European Union – The Digital Services Act*, Schriften des IRDT – Trier Studies On Digital Law, vol. 1, Trier 2023, str. 85–118.
9. Hadas, R., International Internet Jurisdiction; Whose Law is Right? Yahoo!, Inc. v. La Ligue Contr. La Ligue Contre le Racisme et L e le Racisme et L' Antisemitisme, 169 F. Supp. Supp. 2d 1182 (N.D. Cal. 2001), *Florida Journal of International Law*, vol. 15, br. 2/2002, str. 299–309.
10. Kelly, A., Yahoo! Inc. v. La Ligue Contre le Racisme et l' Antisemitisme 379 F.3d 1120 (9TH CIR. 2004), *DePaul Journal of Art, Technology & Intellectual Property Law*, vol. 15, br. 1/2004, str. 257–264.
11. Kooijmans, T., Mevis, P., ICT in the context of criminal procedure: The Netherlands, *Revue électronique de l'AIDP / Electronic Review of the IAPL / Revista electrónica de la AIDP*, 2014, dostupno na: <https://www.penal.org/sites/default/files/files/RA%20-%202011.pdf> (28. 7. 2024.).
12. Lodder, A. R., Sandvliet, K. E., Measures of Blocking, Filtering and Take-Down of Illegal Internet Content: The Netherlands – Report for the Council of Europe (Legal Opinion), November 16, 2015, dostupno na: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2732764](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732764) (11. 8. 2024.).
13. Moslavac, B., Kaznenopravna odgovornost pravnih osoba, *Hrvatska pravna revija*, vol. 9, br. 4/2009, str. 88–103.
14. Mrčela, M., Kaznena djela protiv pravosuđa, *Hrvatski ljetopis za kazneno pravo i praksu*, vol. 10, br. 2/2003, str. 587–624.
15. Novosel, D., Zakon o odgovornosti pravnih osoba za kaznena djela u primjeni, u: *Aktualna pitanja kaznenog zakonodavstva*, Zagreb, 2008, str. 131–184.
16. Novoselec, P., Odgovornost pravnih osoba za kaznena djela – značajna novost u hrvatskom pravnom sustavu, *Pravo u gospodarstvu*, br. 4/2002, str. 104–130.
17. Pavlović, Š., *Kazneni zakon (zakonski tekst, obrazloženje, poveznice, komentar, sudska praksa)*, Rijeka, 2012.
18. Pivaty, A., Wolters, P. T. J., The obligation to notify suspicions of criminal offences in the Digital Services Act under scrutiny, *Boom Strafbblad*, br. 5/2022, str. 187–195.
19. Rojszczak, M., The Digital Services Act and the Problem of Preventive Blocking of (Clearly) Illegal Content, *Institutiones Administrationis – Journal of Administrative Sciences*, vol. 3, br. 2/2023, str. 44–59.
20. Sagar, S., Hoffmann, T., Intermediary Liability in the EU Digital Common Market – from the E-Commerce Directive to the Digital Services Act, *IDP – revista de Internet, derecho y política = revista d'Internet, dret i política*, br. 34/2021, str. 1–12.
21. Tan, Z. Y., Saving the Sinking Ship: How the United States Can Create an Effective Content Moderation Policy by Looking Abroad, *Hastings Law Journal*, vol. 73, br. 2/2022, str. 529–558.

22. Turillazzi, A., Taddeo, M., Floridi, L., Casolari, F., The Digital Services Act: an analysis of its ethical, legal, and social implications, *Law, Innovation and Technology*, vol. 15, br. 1/2023, str. 83–106.
23. Ukrow, J., Core problems of public international law regarding the regulation of the “media sector” with respect to possible tensions with EU law, u: Cole, M.D., Ukrow, J., Etteldorf, C. (ur.), *On the Allocation of Competences between the European Union and its Member States in the Media Sector – Zur Kompetenzverteilung zwischen der Europäischen Union und den Mitgliedstaaten im Mediensektor*, Baden-Baden, 2021, str. 265–330.
24. Vuletić, I., Novokmet, A., Tomičić, Z., Izazovi posebnog dijela kaznenog prava zbog razvoja umjetne inteligencije uz poseban osvrt na hrvatsko kazneno pravo, *Zbornik Pravnog fakulteta u Zagrebu*, vol. 74, br. 1/2024, str. 5–33.
25. Wilman, F., The EU’s system of knowledge-based liability for hosting service providers in respect of illegal user content – between the e-Commerce Directive and the Digital Services Act, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 12, br 3/2021, str. 317–341.
26. Zurth, P., The German NetzDG as Role Model or Cautionary Tale? Implications for the Debate on Social Media Liability, *Fordham Intellectual Property, Media & Entertainment Law Journal*, vol. 31, br. 4/2021, str. 1084–1153.

---

## Summary

Ivan Glavić, PhD\*

### CRIMINAL LAW EFFECTS OF THE DIGITAL SERVICES ACT

The paper analyses the provisions of the Digital Services Act on orders to act against illegal content and to provide information, issued to providers of intermediary services if the content represents a criminal offence. An overview is given of the provisions of the mentioned EU regulation, which refer to the obligation of providers of hosting services to notify the competent law enforcement or judicial authorities of suspicions of a criminal offence involving a threat to the life and safety of persons. Emphasis is placed on the correlation of the mentioned parts of the Digital Services Act with other sources of EU law, as well as the existing legal systems of Croatia and other EU Member States on the detection and prosecution of perpetrators of criminal offences and the obligation to report a crime. The results of the paper indicate that the Digital Services Act represents a legal basis for preventing further crimes, protecting victims and detecting perpetrators of obvious criminal offences on the internet, regardless of the location of the provider of the intermediary services, but under the condition of ensuring in the implementing law the effective exchange of information between law enforcement and judicial authorities and the order issuer and/or the national coordinator for digital services. The criminal responsibility of the provider of hosting services and its responsible persons for a violation of the obligation to report criminal offences involving a threat to the life and safety of persons is theoretically possible, but difficult to achieve in practice.

Keywords: Digital Services Act, order to act against illegal content, order to provide information, European Production Order for electronic evidence, non-reporting of criminal offences

---

\* Ivan Glavić, PhD, Deputy State Attorney at the County State Attorney’s Office in Zagreb; ivan.glavic@zdozg.dorh.hr; ORCID iD: <https://orcid.org/0000-0003-4055-3286>