

**Prof. dr. sc. Leo Cvitanović\***  
**Dr. sc. Ivan Glavić\*\***

## **UZ PROBLEMATIKU SIGURNOSNE MJERE ZABRANE PRISTUPA INTERNETU**

*Problematika sigurnosnih mjera, tog genezom sekundarnog kaznenopravnog kolosijeka, općenito implicira dva temeljna kriminalnopolitička aspekta. U prvome redu, već tradicionalno – aspekt zaštite temeljnih ljudskih prava i sloboda: povijest sigurnosnih mjera, napose njihove praktične primjene, jedno je od “sivih” poglavlja novije kaznenopravne povijesti. Drugi aspekt odnosi se na problem ostvarenja njihove inicijalne kaznenopravne naravi odnosno svrhe na razini odnosa forme i sadržaja: u ovoj su se kaznenopravnoj formi, naime, nerijetko pojavljivali (i pojavljuju se) čisti represivni sadržaji. S tih načelnih pozicija zanimljivo je zakonodavno oblikovanje sigurnosne mjere zabrane pristupa internetu iz čl. 75. Kaznenog zakona, primarno u kontekstu njezine razmjernosti ograničenju osuđenikovih temeljenih prava, učinkovitosti i odnosa prema posebnim obvezama uz uvjetnu osudu, prema radu za opće dobro i prema uvjetnom otpustu. Problematika odnosa između legitimnog interesa za otklanjanjem uvjeta koji omogućuju ili poticajno djeluju na počinjenje novog kaznenog djela i stupnja zadiranja u temeljna prava i slobode potencirana je time što navedena kaznenopravna sankcija onemogućuje korištenje širokog opsega usluga koje nemaju utjecaja na recidivizam, a istovremeno su zabačene manje intruzivne, ali jednako učinkovite mjere ograničenja pristupa internetu. Također se daje prikaz poredbenih pravnih sustava i načina na koji je u njima uređeno ograničenje pristupa toj mreži te u kojoj mjeri imaju dodirnih točaka s hrvatskim rješenjem.*

---

\* Dr. sc. Leo Cvitanović, redoviti profesor pri Katedri za kazeno pravo Pravnog fakulteta Sveučilišta u Zagrebu

\*\* Dr. sc. Ivan Glavić, zamjenik općinskog državnog odvjetništva u Općinskom državnom odvjetništvu u Zagrebu

## I. UVOD

Priroda svake kaznenopravne sankcije, osim admonitivne, jest zadiranje u neko od temeljnih prava i sloboda čovjeka i građanina, kod sigurnosne mjere zabrane pristupa internetu u slobodu izražavanja, koja uključuje i pravo na primanje informacija. Člankom 38. st. 4. Ustava određeno je da zadiranje u potonje pravo mora biti propisano zakonom, razmjerno naravi potrebe za ograničenjem u svakom pojedinom slučaju te nužno u slobodnom i demokratskom društvu. Analogne odredbe sadržavaju i međunarodni izvori koji uređuju temeljna ljudska prava, pa i izričitim normiranjem da pravo slobode izražavanja obuhvaća primanje i širenje informacija ili ideja.<sup>1</sup>

Recentni nacrt Rezolucije Vijeća UN-a za ljudska prava o promicanju, zaštiti i uživanju ljudskih prava na internetu potvrđuje da ista prava koje ljudi uživaju mimo njega (offline) moraju biti zaštićena i na toj komunikacijskoj mreži (online).<sup>2</sup> Takvo je i stajalište američkih sudova pri donošenju odluka vezanih uz kaznenopravno ograničenje pristupa internetu;<sup>3</sup> a načela izražena u prijašnjim presudama Europskog suda za ljudska prava, vezano uz pravo na slobodu izražavanja i primanje informacija, primjenjuju i na internet.<sup>4</sup> Dapače, francuski Ustavni sud<sup>5</sup> i specijalni izvjestitelj UN-a za promicanje i zaštitu prava i slobode mišljenja i izražavanja<sup>6</sup> produbljuju problematiku te značenje temeljnog ljudskog prava na primanje informacija, upravo u kontekstu restrikcije pristupa internetu, potenciraju činjenicom da je ono temelj za uživanje drugih prava i sloboda (pravo na obrazovanje, sudjelovanje u kulturnom životu, uživanje u prednostima znanstvenog napretka i sl.).

Dikcija čl. 75. Kaznenog zakona pokazuje da se pri propisivanju sigurnosne mjere zabrane pristupa internetu zakonodavac odlučio za iznimno rigoroznu varijantu potpune zabrane korištenja usluga koje ovise o toj mreži, bez obzira na težinu počinjenog i eventualnog budućeg kaznenog djela u apstraktnom (s obzirom na propisanu kaznu) i konkretnom (s obzirom na izrečenu kaznu)

---

<sup>1</sup> Čl. 19. st. 2. i 3. Međunarodnog pakta o građanskim i političkim pravima, čl. 10. st. 1. i 2. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda.

<sup>2</sup> United Nations, Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13 od 29. lipnja 2012.

<sup>3</sup> Gillett, G., A world without Internet: A new framework for analyzing a supervised release condition that restricts computer and Internet access, *Fordham Law Review*, vol. 79, br. 1/2010, str. 254.

<sup>4</sup> Usp. European Court of Human Rights, Research division, Internet: case-law of the European Court of Human Rights, 2011., str. 11. - 17., 20. - 24., dostupno na [www.echr.coe.int](http://www.echr.coe.int) (5. rujna 2012.)

<sup>5</sup> Conseil Constitutionnel, odluka br. 2009-580 od 10. lipnja 2009., odjeljak 15.

<sup>6</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27 od 16. svibnja 2011., odjeljak 22.

pogledu. Premda to ograničenje prava na pristup informacijama ima legitimni cilj, specijalnu prevenciju i zaštitu društva,<sup>7</sup> postavlja se pitanje u kojoj je mjeri doista i nužno radi njegova ostvarivanja uvesti sigurnosnu mjeru sa širokim zabranama za počinitelja.

Kazneni zakon u čl. 67. sadržava, doduše, načelnu odredbu određujući da sigurnosna mjera mora biti u razmjeru s težinom počinjenog kaznenog djela i kaznenih djela koja se mogu očekivati te sa stupnjem počiniteljeve opasnosti. Potonja je kategorija shvaćena kao temelj za primjenu sigurnosne mjere, a načelo razmjernosti kao temelj za njihovo odmjeravanje.<sup>8</sup> Sudeći prema obrazloženju danom uz sigurnosnu mjeru obveznog psihijatrijskog liječenja, zakonodavac smatra da se potreba „*preciznijeg definiranja*“ sigurnosne mjere u Kaznenom zakonu pokazuje onda kada se pojave „*nedoumice i lutanja*“ u sudskoj praksi.<sup>9</sup> Međutim, sukladno shvaćanju Europskog suda za ljudska prava, ujednačena sudska praksa doduše može precizirati zakon, ali pod uvjetom da je takav rezultat predvidiv.<sup>10</sup> Stoga sud koji izriče kaznenopravnu sankciju nije jedini adresat ustavnog načela razmjernosti i zakonodavac ne može istodobno kreirati nedovoljno jasnu normu koja ostavlja mogućnost povrede tog načela za određenu kategoriju kaznenih djela ili počinitelja, očekujući da je sud u budućnosti neće na taj način primijeniti u konkretnom predmetu. Načelo razmjernosti ujedno pretpostavlja i da se neka sigurnosna mjera ne izrekne ako se ista svrha može postići i blažom sigurnosnom mjerom.<sup>11</sup> Međutim, kako će sud, kršeći načelo zakonitosti iz čl. 2. Kaznenog zakona, izreći blažu sigurnosnu mjeru ako ju nije predvidio zakonodavac? Stoga sama načelna odredba o razmjernosti tih kaznenopravnih sankcija nije dovoljna, dapače, Ustavni je sud još povodom ocjene ustavnosti odredaba „starog“ Kaznenog zakona naveo: „*Primijenjeno na svaku, pa i na ovu sigurnosnu mjeru, načelo razmjernosti nalaže da se kod propisivanja i izricanja sigurnosne mjere mora ispitati je li ista primjerena ostvarenju zakonske svrhe... Takvim propisivanjem istovremeno su zanemareni zahtjevi ustavnog načela razmjernosti koje Ustavni sud smatra na području propisivanja i primjene sigurnosnih mjera u kaznenom pravu to važnijim što kod njih, za razliku od propisivanja i primjene kazni kao vrste kaznenih sankcija, ne postoji ograničenje krivnjom počinitelja kao njihovom mjerom.*“<sup>12</sup>

<sup>7</sup> Bačić, F., Pavlović, Š., Komentar Kaznenog zakona, Zagreb, 2004., str. 373.; Novoselec, P., Opći dio kaznenog prava, Zagreb, 2004., str. 418.

<sup>8</sup> Vlada Republike Hrvatske, Konačni prijedlog Kaznenog zakona, listopad 2011., str. 127.

<sup>9</sup> Ib., str. 152.

<sup>10</sup> Usp. S.W. v. United Kingdom (1995.), zahtjev br. 20166/92.

<sup>11</sup> Novoselec, P., kao u bilješci 7, str. 421.

<sup>12</sup> Ustavni sud RH, odluka br. U-I-1162/2008 od 28. lipnja 2011.

U očekivanju načina na koji će biti implementirano u sudskoj praksi, ovaj rad analizira aspekte načela razmjernosti sigurnosne mjere zabrane pristupa internetu u odnosu prema zakonskom sadržaju predmetne kaznenopravne sankcije – odgovara li opseg zadiranja u temeljna ljudska prava zakonom predviđenoj svrsi, reflektira li krug obuhvaćenih kaznenih djela potrebu otklanjanja opasnosti počinitelja, postoje li drugi učinkoviti načini za otklanjanje uvjeta koji omogućuju ili poticajno djeluju na počinjenje novog kaznenog djela, te u odnosu prema uvjetnoj osudi, radu za opće dobro ili uvjetnom otpustu s posebnom obvezom ograničenja pristupa internetu.

Naposljetku, komentar zaslužuje i poredbenopravno ograničavanje pristupa internetu te je li riječ o istim konotacijama kao u našem zakonodavstvu. Obrazlažući tu sigurnosnu mjeru predlagatelj Kaznenog zakona poziva se na trend u „*sudskoj praksi nekih država SAD-a (od 2000. godine nadalje)... francuskom Zakonu o distribuciji i zaštiti autorskih i srodnih djela na internetu N°2009-669 od 12. lipnja 2009. (tzv. HADOPI zakon) te irskom zakonodavstvu (uz uvjet da je najmanje tri puta počinjeno – načelo ‘three strikes and you are out’*“.<sup>13</sup> Da je pri izradi Kaznenog zakona izostao ozbiljniji komparativni pristup, pokazuju već sljedeće činjenice – u SAD-u sudska praksa nije započela nakon 2000. i nije riječ samo o odlukama sudova saveznih država,<sup>14</sup> problematika nije riješena isključivo sudskom praksom, već pojedine države imaju kaznenopravnu legislativu;<sup>15</sup> u Francuskoj tu materiju odavno regulira Zakon o kaznenoj zaštiti literarnog i umjetničkog vlasništva na internetu N°2009-1311 od 28. listopada 2009. (tzv. HADOPI 2 zakon), dok je u Irskoj riječ samo o razmatranju sličnog zakona.<sup>16</sup>

## II. OPSEG ZADIRANJA U TEMELJNA LJUDSKA PRAVA

Oslanjajući se na obrazloženje Konačnog prijedloga Kaznenog zakona i na sam zakonski tekst, teško da bi se moglo zaključiti na što se ciljalo pri

---

<sup>13</sup> Vlada Republike Hrvatske, Konačni prijedlog Kaznenog zakona, listopad 2011., str. 157.

<sup>14</sup> Usp. odluke federalnog Prizivnog suda SAD-a (U.S. Court of Appeals) u predmetima U.S. v. Mitnick, No. 97-50365, 1998 WL255343 (9.th Cir. May 20,1998) i U.S. v. Crandon, 173F.3d122 (3d Cir. 1999).

<sup>15</sup> Usp. pregled zakonskih tekstova pojedinih saveznih država u: LaMagna, R.C., Berejka, M., Remote Computer Monitoring: Managing Sex Offenders' Access to the Internet (dodatak Sex Offender Computer Use: Relevant State Statutes), The Journal of Offender Monitoring, vol. 21, br. 1/2009, str. 27. - 29.

<sup>16</sup> Boardman, M., Digital Copyright Protection and Graduated Response: A Global Perspective, Loyola of Los Angeles International and Comparative Law Review, vol. 33, br. 2/2011, str. 229.

kaznenopravnom uređenju korištenja interneta – jedanput je on usluga koju pružaju telekomunikacijski operatori („...ugovor o elektroničkim komunikacijskim uslugama koji uključuje uslugu interneta“<sup>17</sup>), ponekad samo jedna od usluga baziranih na internetskom protokolu („...putem telefona ili interneta, chatrooms, različitih igara...“<sup>18</sup>), a treći put sam informacijski sustav („informacijski sustavi uključujući i internet“<sup>19</sup>). Ne navodi se da je internet ono što doista i jest - globalna komunikacijska mreža, čija upotreba podrazumijeva širok spektar usluga temeljenih na posebnim protokolima – world wide web, elektroničku poštu, prijenos podataka, chatroom, društvene mreže, telefonske usluge (VoIP), televiziju (IPTV) i sl.

S obzirom na naprijed navedeno, način na koji se namjerava provoditi sigurnosna mjera zabrane pristupa internetu, raskidanjem postojećih i zabranom sklapanja novih ugovora koji uključuju korištenje te mreže,<sup>20</sup> u pojedinim slučajevima podrazumijeva i raskidanje onih ugovornih odnosa kod kojih korištenje usluge ne stoji u kauzalnoj vezi sa svrhom sigurnosne mjere, opasnošću počinitelja. Primjerice, teško da korištenje internetske inačice kabelaške televizije (IPTV)<sup>21</sup> može biti uvjet koji omogućuje ili poticajno djeluje na počinjenje novog kaznenog djela budući da je na taj način moguće gledanje samo legalnih sadržaja, a usluga je tehnički odvojiva od onih koje su bazirane na drugim internetskim protokolima.

Daljnji je problem porast legalnih načina korištenja interneta. Suočavajući se 2001. s pitanjem razmjernosti potpune zabrane pristupa internetu, američki federalni prizivni sud navodi da bi ona onemogućila njegovo korištenje „u knjižnici za bilo kakvo istraživanje, pribavljanje vremenske prognoze ili čitanje novina online“.<sup>22</sup> Samo dvije godine poslije nabrajaju se daleko opsežnija zađiranja u pravo na komunikaciju te izražava stav da „takva zabrana pogađa suvremeni život – u kojem, primjerice, vlada snažno ohrabruje porezne obveznike da podnose svoje zahtjeve elektronički, kada se sve više trgovine odvija online i kada je ogromna većina vladinih informacija postavljena na web stranice“.<sup>23</sup> U međuvremenu, usluge koje su bile ponuđene preko interneta kao alternativa tradicionalnim metodama postale su standardne, a mnoge i dostupne isključivo na taj način (prijava na studij ili posao, mnoge državne usluge).<sup>24</sup>

<sup>17</sup> Vlada Republike Hrvatske, Konačni prijedlog Kaznenog zakona, listopad 2011., str. 157.

<sup>18</sup> Ib., str. 198.

<sup>19</sup> Čl. 185. st. 5. Kaznenog zakona.

<sup>20</sup> Vlada Republike Hrvatske, Konačni prijedlog Kaznenog zakona, listopad 2011., str. 157.

<sup>21</sup> MaxTV, OptiTV, IskonTV, H1TV, AmisTV i sl.

<sup>22</sup> U.S. v. White, 244 F.3d 1199 (10th Cir. 2000).

<sup>23</sup> U.S. v. Holm, 326 F.3d 872 (7th Cir. 2003).

<sup>24</sup> Adkins, J., Unfriended felons: Reevaluating the Internet's role for the purpose of special conditions in sentencing in a post-Facebook world, *Journal on Telecommunications and High Technology Law*, vol. 9, br. 1/2011, str. 272.

Ističe se da porast usluga na internetu pojačava učinkovitost kaznenopravne zabrane u smislu odvracanja potencijalnih počinitelja kada je ograničenje pristupa široko postavljeno,<sup>25</sup> ali sve da je taj zaključak i točan, preneseno na svrhu sigurnosnih mjera kako je definirana u hrvatskom zakonodavstvu, veća dostupnost legalnih sadržaja ne utječe na svrhu sigurnosne mjere zabrane pristupa internetu. Specijalna prevencija kao bitna odrednica sigurnosne mjere ne temelji se na zastrašivanju, već na uklanjanju uvjeta koje omogućuju počinjenje novog kaznenog djela ili mu pogoduju, i opasnost okrivljenika ne može se prosuđivati prema broju legalnih usluga korištenja interneta jer on ne predstavlja prijetnju sigurnosti društva kada se internetom služi na zakonit način. Istovremeno, rast značenja interneta u svakodnevnom životu pri zabranjivanju njegova korištenja pridonosi povećanju zadiranja u pravo na slobodu izražavanja i time utječe na narušavanje načela razmjernosti sigurnosnih mjera.

Posebnu kontroverziju apsolutne zabrane korištenja interneta uzrokuje otežanost, ili čak nemogućnost, rehabilitacije počinitelja, u smislu zapreka pri zapošljavanju i zadržavanju posla,<sup>26</sup> odnosno dostavljanju i primanju liječničkih podataka,<sup>27</sup> nesposobnosti obeštećenja žrtve,<sup>28</sup> sprječavanja pristupa obrazovanju, a dolazi i do stigmatizacije počinitelja koji će u svakodnevnom životu poslodavcu i okolini teško objasniti zašto se ne koristi *online* dostupnim uslugama. Kada je riječ o počiniteljima kojima je izrečena kazna zatvora, ističe se da je zabrana korištenja interneta nakon puštanja na slobodu upitna budući da nemogućnost njegova korištenja za vrijeme izdržavanja kazne ionako oslabljuje učinak odvracanja.<sup>29</sup> Međutim, pogubne posljedice prohibicije korištenja internetom na rehabilitaciju i integraciju u društvenu zajednicu počinitelja puštenog na slobodu nisu oslabljene, jer zadovoljenje njegovih životnih potreba, koje su mu za vrijeme izdržavanja kazne osigurane od zatvorskog sustava, sada pada na njegova leđa. Ne samo da su njegove potrebe boravkom na slobodi povećane već mu je onemogućeno i korištenje onih usluga putem interneta koje je posrednim putem imao čak i za vrijeme oduzimanja slobode, budući

---

<sup>25</sup> *Ib.*, str. 282.

<sup>26</sup> Correll, F. E., „You fall into Scylla in seeking to avoid Charybdis“: The Second Circuit’s pragmatic approach to supervised release for sex offenders, *William and Mary Law Review*, vol. 49, br. 2/2007, str. 706. - 707., Gillett, G., kao u bilješci 3, str. 249., Sullivan, J.L., *Federal courts act as a toll booth to the information super highway – are Internet restrictions too high of a price to pay?*, *New England Law Review*, vol. 44., br. 4/2009-2010, str. 958. - 959.

<sup>27</sup> Krause, C.A., Pazicky, L.A.E., *An Un-Standard Condition: Restricting Internet Use as a Condition of Supervised Release*, *Federal Sentencing Reporter*, vol. 20, br. 3/2008, str. 203., Regina, J.A., *Access Denied: Imposing Statutory Penalties On Sex Offenders Who Violate Restricted Internet Access As a Condition of Probation*, *Seton Hall Circuit Review*, vol. 4, br. 1/2007, str. 198. - 199., Sullivan, J.L., kao u bilješci 26, str. 956.

<sup>28</sup> Krause, C.A., Pazicky, L.A.E., kao u bilješci 27, str. 203.

<sup>29</sup> Sullivan, J.L., kao u bilješci 26, str. 959. - 960.

da su se djelatnici zatvora koristili tom mrežom kako bi mu osigurali zdravstvenu skrb, zadovoljenje vjerskih potreba, upućivanje predstavki, kontakt s veleposlanstvom, obavještavanje članova obitelji u inozemstvu i sl. Ne čudi da se beziznimna zabrana pristupa internetu shvaća više kao retribucija, s oduzimanjem slobode na posve novoj razini nego što je to psihičko zatvaranje.<sup>30</sup>

Zbog navedenih razloga valjalo bi umjesto o zabrani razmisliti o ograničenju pristupa internetu, koje može biti provedeno funkcionalno, s obzirom na način korištenja interneta, ili sadržajno, s obzirom na mrežne usluge. Najčešći primjer prvog ograničenja u SAD-u predstavlja njegovo korištenje tek uz odobrenje probacijskog službenika,<sup>31</sup> ali postoji mogućnost i da se zabrani pristup internetu uz uporabu kriptacije ili drugog načina sakrivanja identiteta, dopusti njegovo korištenje samo na poslu ili u obrazovnoj ustanovi i sl. S druge strane, ograničenje sadržajne prirode može biti takvo da se korištenje pojedinih usluga zabrani u potpunosti (npr. zabrana počinitelju kaznenog djela mamljenja djece za zadovoljenje spolnih potreba da se koristi društvenim mrežama, zabrana počinitelju kaznenog djela protiv intelektualnog vlasništva da se koristi online trgovinom ili elektroničkom poštom) ili djelomično (npr. zabrana počinitelju kaznenog djela mamljenja djece za zadovoljenje spolnih potreba da se koristi društvenim mrežama koje dopuštaju otvaranje profila djeci, dopuštenje počinitelju kaznenog djela protiv intelektualnog vlasništva da se koristi samo jednom adresom elektroničke pošte).

### III. IZVRŠAVANJE, NADZOR I UČINKOVITOST ZABRANE PRISTUPA INTERNETU

Sukladno čl. 75. st. 4. Kaznenog zakona, sud će o pravomoćno izrečenoj sigurnosnoj mjeri zabrane pristupa internetu obavijestiti regulatorno tijelo nadležno za elektroničke komunikacije koje će osigurati njezino provođenje. To prema obrazloženju predlagatelja Zakona podrazumijeva određivanje nadležnog tijela koje će koordinirati izvršavanje mjere, a to bi bila Hrvatska agencija za poštu i elektroničke telekomunikacije (HAKOM). Ona bi po zahtjevu obavijestila nadležnog suda o pravomoćno izrečenoj mjeri obavijestila sve operatore koji pružaju usluge pristupa internetu da u određenom razdoblju ne smiju sklopiti ugovor o korištenju usluga pristupa internetu odnosno, ako

---

<sup>30</sup> Khilman, V., Can a court lawfully forbid a person access to the internet as a term of his probation?, *International Journal of Baltic Law*, vol. 1, br. 2/2004, str. 66.

<sup>31</sup> Cowin, S., You Don't Have Mail: The Permissibility of Internet-Use Bans in Child Pornography Cases and the Need for Uniformity Across the Circuits, *The George Washington Law Review*, vol. 80, br. 3/2012, str. 898. - 899., Gillett, G., kao u bilješki 3, str. 251.

s počiniteljem već imaju zasnovan pretplatnički odnosno na to da mu moraju obustaviti pružanje usluga u razdoblju određenom mjerom.<sup>32</sup>

Predmetna norma suprotna je već čl. 75. st. 1. Kaznenog zakona, budući da sigurnosna mjera počinje teći izvršnošću presude, a ne njezinom pravomoćnošću. Praktična je posljedica navedene dihotomije isključivanje usluga pristupa internetu prije početka izvršenja sigurnosne mjere ili čak kada se mjera ne bi mogla ni izvršiti zbog nastupa zastare, što predstavlja ograničavanje temeljnih ljudskih prava bez uporišta u zakonu.

Nastojanja zakonodavca da omogući osuđeniku odsluženje kazne zatvora u vlastitom domu, u smislu čl. 44. st. 4. Kaznenog zakona, nisu naišla na odgovarajuće normiranje izvršavanja sigurnosnih mjera koje počinitelju zabranjuju određeno ponašanje. Zabrana pristupa internetu u tom je kontekstu osobito značajna, jer za razliku od drugih sigurnosnih mjera nečinjenja, boravak u vlastitom domu *per se* ne otklanja uvjet koji omogućuje ili poticajno djeluje na počinjenje novog djela (osuđenik može pristupiti internetu iz vlastitog doma). Premda je u čl. 75. st. 2. Kaznenog zakona određeno da se vrijeme provedeno u zatvoru, kaznionici ili ustanovi ne uračunava u vrijeme trajanja zabrane pristupa internetu, ostaje upitno bi li argument *a contrario*, da se izdržavanje kazne u vlastitom domu uračunava u vrijeme trajanja te sigurnosne mjere, bio teleološki opravdan ili je opet riječ o pravnoj praznini. Naime, takvo odsluženje kazne nije predviđeno kao razlog mirovanja sigurnosne mjere zabrane upravljanja motornim vozilom ili zabrane približavanja, iako je notorno da pretpostavlja nemogućnost korištenja vozilom ili približavanja osobi koja nije član kućanstva, pa je upitna ostvarivost svrhe sigurnosne mjere i istodobno se osuđenika neopravdano stavlja u povoljniji položaj od onog koji izdržava kaznu u instituciji. Kada bi se i prihvatilo stajalište da se sigurnosna mjera zabrane pristupa internetu proteže i na razdoblje odsluženja kazne u vlastitom domu, njezino kršenje ne bi imalo kao posljedicu institucionalno zatvaranje jer Kaznenim zakonom nije predviđen opoziv takvog izdržavanja kazne zbog kršenja sigurnosne mjere.

Obrazloženje uz Konačni prijedlog ne sadržava naznake namjere da se izvršavanje sigurnosne mjere zabrane pristupa internetu potanko uredi provedbenim propisom. Ostaje upitno kako u praksi pristupiti pitanju prekida u izvršavanju mjere (npr. početak izdržavanja kazne); ostvariti zaštitu osuđenika od povrede prava na privatnost, budući da će širok krug privatnih osoba znati za njegovu osuđivanost, te koje su posljedice ako pružatelj usluga pristupa internetu nezakonito otkrije tu okolnost. Naposljetku, odluke koje donosi HAKOM upravne su prirode, protiv njih se može pokrenuti upravni spor, pa je jasno da njegova uloga u izvršavanju sigurnosne mjere može biti samo prosljeđivanje sudske obavijesti. Bez obzira na to što se uvodi kaznena odgovornost za službenu

---

<sup>32</sup> Vlada Republike Hrvatske, Konačni prijedlog Kaznenog zakona, listopad 2011., str. 157.-158.



ili odgovornu osobu koja ne izvrši pravomoćnu sudsku odluku koju je bila dužna izvršiti,<sup>33</sup> pod tu odgovornost ne podliježe obrtnik pružatelj usluge pristupa internetu koji zasnjuje ili nastavi ugovorni odnos s osobom za koju traje sigurnosna mjera. Učinkovitost namjeravanog rješenja dodatno je dovedena u pitanje i činjenicom da niti jedna odredba Kaznenog zakona (ili Zakona o kaznenom postupku) ne konstituira obvezu pružatelja usluga pristupa internetu da se pridržava zabrane zasnivanja ili nastavka pretplatničkog odnosa, budući da on nije adresat u kaznenom, već izvršnom postupku.

Hrvatska agencija za poštu i telekomunikacije nije ustanova koja bi mogla uspješno koordinirati izvršavanje sigurnosne mjere, jer nema sredstvo provjere pridržavaju li se pružatelji usluge pristupa internetu dobivene obavijesti, a mogućnost da utvrdi koristi li se osuđenik u kritičnom razdoblju internetom na neki drugi način gotovo je nikakva. Prikladnije tijelo, u svakom slučaju, bio bi Operativno-tehnički centar za nadzor telekomunikacija, koji je ionako nadležan za koordinaciju između osoba koje pružaju pristup internetu i tijela kaznenog progona koja nalažu i izvršavaju mjere tajnog nadzora, ima ovlast nadzora nad radom davatelja telekomunikacijskih usluga te je s njima povezan tehničkim putem.<sup>34</sup>

Sve da se i otklone naprijed navedeni problemi, iluzorno je očekivati da je nemogućnost zadržavanja ili zasnivanja pretplatničkog odnosa dobar način za sprječavanje osuđenika da pristupi internetu, mreži koju ionako karakterizira anonimnost korisnika. Dovoljno je da osim počinitelja još jedna osoba s njim živi u kućanstvu pa da se može nesmetano koristiti priključkom i kršiti sigurnosnu mjeru, budući da se na članove obitelji osuđenika ne može protegnuti ograničenje prava na sklapanje pretplatničkog odnosa. Također, kako se o postojanju sigurnosne mjere ne obavještavaju treće osobe, osuđenik se može nesmetano koristiti i tuđim priključkom (npr. posudba uređaja, pristup na radnom mjestu). Ne samo da postoje mnogobrojni i lako izvedivi nezakoniti načini korištenja internetom skrivanjem identiteta korisnika (prijevarno ugovaranje mobilnog priključka na tuđe ime; zloupotreba tuđeg bežičnog routera i sl.) već mu se bez otkrivanja osobnih podataka može osobno pristupiti na posve legalne načine (kupovina prepaid paketa mobilnog interneta, korištenje usluge bežičnog HotSpot pristupa u ugostiteljskim objektima, knjižnicama, hotelima pa čak i cijelim gradskim zonama).

Isti problemi javljaju se u slučajevima ograničenja pristupa internetu: osuđenik također može pristupiti zabranjenom sadržaju promjenom šifre za

---

<sup>33</sup> Ministarstvo pravosuđa, Nacrt prijedloga zakona o izmjenama i dopunama Kaznenog zakona, srpanj 2012., čl. 73.

<sup>34</sup> Usp. čl. 18. Zakona o sigurnosno-obavještajnom sustavu Republike Hrvatske, čl. 335. st. 2. Zakona o kaznenom postupku

pristup, uporabom tuđeg priključka ili javnog bežičnog pristupa internetu.<sup>35</sup> Međutim, različito od potpunog onemogućavanja korištenja, ipak je probacijskim službenicima pružena mogućnost da računalnim putem provjere pridržava li se počinitelj zabrane korištenja pojedinim uslugama s poznatih točaka pristupa ili čak da instaliranjem posebnih programa na njegovu računalu ograniče korištenje te mreže. Pritom se software za kontroliranje osuđenika može, poredano po razini zadiranja u temeljna ljudska prava, podijeliti na forenzične, nadgledne i filtrirajuće programe.<sup>36</sup> Svi pretpostavljaju osuđenikov pristanak na pristup računalu od treće osobe, bilo da je riječ o kontroli ili instaliranju i ažuriranju programa.

Forenzični programi omogućuju prikupljanje i povrat izbrisanih računalnih podataka radi analize korisnikove aktivnosti na računalu. Budući da su u početku zahtijevali fizičku zapljenu računala kako bi se iz njegove memorije kroz više sati kopirala veća količina računalnih podataka, smatrani su najdetaljnijima, ali i najopsežnijim zadiranjem u privatnost osuđenika,<sup>37</sup> dok noviji programi omogućuju (zaštićeni) virtualni pristup počiniteljevom računalnom sustavu korištenjem mreže.<sup>38</sup> Nadzorni programi razlikuju se od forenzičnih po tome što u određenim vremenskim razmacima prate i bilježe aktivnost na računalu u realnom vremenu, oponašajući funkciju nadzornih kamera,<sup>39</sup> prikazom zaslona monitora ili prikupljanjem podataka s tipkovnice. Aktivni nadzorni programi šalju rezultate elektroničkom poštom probacijskom službeniku i ne zahtijevaju njegov fizički pristup računalu, dok pasivni spremaju rezultate na korisnikovu računalu.<sup>40</sup> Naposljetku, filtrirajući programi onemogućuju pristup određenim sadržajima na internetu, sukladno ograničenjima zadanim kaznenopravnom sankcijom, bilo da je riječ o pojedinim web stranicama, društvenim mrežama, chatroomovima i sl. S obzirom na to da nemaju nadzornu funkciju, smatraju se najmanje intruzivnima.<sup>41</sup>

Sadašnja tehnologija programa za kontroliranje osuđenikove aktivnosti na internetu, bez obzira na to o kojoj je kategoriji riječ, omogućuje i zadovoljavajuću ravnotežu s potrebom zaštite privatnosti osuđenika. Oni se mogu prilagoditi ne

---

<sup>35</sup> Usp. Curphey, S., *United States v. Lifshitz: Warrantless Computer Monitoring and the Fourth Amendment*, *Loyola of Los Angeles Law Review*, vol. 38, br. 5/2005, str. 2266. - 2267., Regina, J.A., kao u bilješci 27, str. 204. - 205., Sullivan, J. L., kao u bilješci 26, str. 962., Winton, J.S., *Myspace, yourspace, but not theirs: The constitutionality of banning sex offenders from social networking sites*, *Duke Law Journal*, vol. 60, br. 8/2010 - 2011, str. 1901.

<sup>36</sup> Curphey, S., kao u bilješci 35, str. 2263. - 2266., Regina, J.A., kao u bilješci 27, str. 201.- 204.

<sup>37</sup> Curphey, S., kao u bilješci 35, str. 2263.

<sup>38</sup> Regina, J.A., kao u bilješci 27, str. 201.

<sup>39</sup> *Ib.*, str. 202.

<sup>40</sup> Curphey, S., kao u bilješci 35, str. 2264.

<sup>41</sup> *Ib.*, str. 2265.

samo tako da nadziru pristupa li korisnik zabranjenim uslugama na internetu već i tako da pretražuju korištenje samih usluga prema određenim parametrima, kao što je korištenje pojedinih softwera na računalu ili korištenje ključnih riječi (npr. ime žrtve, izrazi povezani s dječjom pornografijom i sl.).<sup>42</sup> Fleksibilnost koja je time dopuštena, nažalost, povezana je s određenim poteškoćama – probacijski službenici koji prate aktivnost osuđenika na internetu moraju biti dobro informatički educirani, dok svakodnevni porast opsega zabranjenih sadržaja iziskuje učestale nadogradnje programa, a učinkovitost je i dalje upitna budući da se promjena parametara filtrirajućih programa ne može dovoljno brzo prilagoditi velikoj količini zabranjenih sadržaja koji se svakodnevno pojavljuju i mijenjaju.<sup>43</sup>

Zaključno, da se *de lege ferenda* uvede sigurnosna mjera ograničavanja pristupa internetu, stvarna mogućnost njezina nadzora i fizičkog (ili virtualnog) sprječavanja osuđenika da pristupi zabranjenim sadržajima bila bi upitna – baš kao što je to s postojećom sigurnosnom mjerom zabrane pristupa internetu. Međutim, isto je s bilo kojom drugom mjerom koja okrivljeniku nameće zabranu (u SAD-u se povlači paralela sa zabranom korištenja droge<sup>44</sup>) te sudu preostaje osloniti se na povjerenje u osuđenika. Otežavajući faktor kod zabrane korištenja internetom predstavlja okolnost da će se redarstvene vlasti pri nasumičnoj kontroli suočiti s osuđenikom koji može lakše iskoristiti anonimnost i privatnost nego osuđenik kojem je izrečena druga sigurnosna mjera (zabrana upravljanja motornim vozilom, zabrana približavanja i sl.). Očigledno da se sve svodi na *ex post facto* reakciju odnosno hipotetičku prijetnju naknadnom represijom.

#### IV. OBUHVAĆENA KAZNENA DJELA

Ograničavanje počiniteljevih temeljnih prava najčešće je prilagođeno tako da eliminira opasnost od ponovnog počinjenja određenog kruga potencijalnih kaznenih djela koja stoje u kauzalnoj vezi s pravom koje se ograničava (npr. sigurnosna mjera zabrane obavljanja određene dužnosti ili djelatnosti izriče se za kaznena djela počinjena u obavljanju dužnosti, sigurnosna mjera zabrane upravljanja motornim vozilom za ugrožavanje prometa, dok se sigurnosna mjera zabrane pristupa internetu izriče za kaznena djela počinjena putem interneta).

---

<sup>42</sup> Usp. Curphey, S., kao u bilješci 35, str. 2265. - 2266., LaMagna, R.C., Berejka, M., kao u bilješci 15, str. 15, Regina, J.A., kao u bilješci 27, str. 200. - 203.,

<sup>43</sup> Cowin, S., kao u bilješci 31, str. 913 - 914., Regina, J.A., kao u bilješci 27, str. 203.

<sup>44</sup> Curphey, S., kao u bilješci 35, str. 2249., Sullivan, J.L., kao u bilješci 26, str. 964. - 965.

Na prvi pogled može se činiti da je zadaća zakonodavca pri definiranju te kaznenopravne sankcije isključiti od njezina izricanja ona kaznena djela kod kojih ograničavanje temeljnih prava po samoj prirodi nije podobno otkloniti opasnost od njihova možebitnog počinjenja (npr. zabrana upravljanja motornim vozilom nije podobna za otklanjanje opasnosti od počinjenja kaznenog djela protiv spolne slobode). Ipak, propisivanjem sigurnosne mjere ne samo da se od njezina izricanja isključuju kaznena djela za koja uopće ne postoji opasnost od počinjenja već i ona djela kod kojih ona nije specifična i dovoljno ozbiljna ili kauzalna veza između prava počinitelja koje se ograničava i postojanja opasnosti nije dovoljno čvrsta. Potonje stajalište implementirano je u sudsku praksu SAD-a; ograničenje pristupa internetu smatra se (pre)opterećujućim kada tehnologija nije integralni dio kaznenog djela, primjerice u slučaju poštanske prijave u kojoj je e-mail bio tek način korespondencije.<sup>45</sup>

Preneseno na ostale sigurnosne mjere propisane Kaznenim zakonom, zabrana upravljanja motornim vozilom izriče se kod opasnosti da će biti počinjeno ugrožavanje prometa, ali ne i krađa vozila; zabrana obavljanja određene dužnosti ili djelatnosti samo kod opasnosti od zlorabe dužnosti ili djelatnosti, ali ne i za pronevjeru, utaju poreza ili nehajno djelo; udaljenje iz zajedničkog kućanstva kod opasnosti od počinjenja kaznenog djela nasilja, ali ne i uvrede ili rodoskvrnuća.

Kada se upozorava na apsurdnost zabrane pristupa internetu za preširok krug kaznenih djela, u američkoj se sudskoj praksi i doktrini odavno povlači paralela s počinjenjem prijave i drugih kaznenih djela upotrebom „tradicionalnih“ sredstava komunikacije, kao što su telefon ili pošta, na što se kaznenopravno ne reagira zabranom pristupa telefonu ili poštanskim uslugama.<sup>46</sup> Slično tome, zloraba čeka i platne kartice može se počinuti uporabom bankomata, krivotvorenje isprave uporabom računala, povreda autorskog prava uporabom fotokopirnog uređaja, prijetnja uporabom noža, uvreda objavljivanjem knjige, ali zakonodavac očigledno zbog toga ne smatra prihvatljivim uvesti sigurnosne mjere zabrane pristupa bankomatu, računalu, fotokopirnom uređaju ili nožu odnosno zabrane posjedovanja platne kartice ili objavljivanja knjige. Zašto bi bilo prihvatljivo zabraniti pristup internetu kada su ta ista kaznena djela počinjena uporabom te mreže?

Jedine sigurnosne mjere primjenjive na sva kaznena djela su one kod kojih se opasnost, strogo vezana uz ličnost počinitelja, ne može otkloniti nečinjenjem, već njegovim aktivnim sudjelovanjem (podvrgavanje liječenju ili zaštitnom nadzoru). Kod ostalih sigurnosnih mjera (osim zabrane pristupa internetu) zakonodavcu je ipak uspjelo ograničiti primjenu pobližim određivanjem da se

---

<sup>45</sup> Gillett, G., kao u bilješki 3, str. 249., U.S. v. Silvious 512 F.3d 364, 371 (7th Cir. 2008).

<sup>46</sup> Cowin, S., kao u bilješki 31, str. 899, Gillett, G., kao u bilješki 3, str. 253. - 254., Sullivan, J.L., kao u bilješki 26, str. 957. - 958., Wynton, J.S., kao u bilješki 35, str. 1866.

otklanja opasnost od počinjenja kaznenih djela s određenim obilježjem koje tvori biće kaznenog djela (npr. nasilje kod sigurnosne mjere obveznog psihosocijalnog tretmana ili udaljenja iz zajedničkog kućanstva), kaznenih djela kojima se zaštićuju određena pravna dobra (npr. sigurnost prometa kod sigurnosne mjere zabrane upravljanja motornim vozilom, spolna sloboda kod sigurnosne mjere zabrane približavanja) ili čak taksativno navedenih kaznenih djela (kod sigurnosne mjere zabrane obavljanja određene dužnosti ili djelatnosti iz čl. 71. st. 3. Kaznenog zakona).

Isto je valjalo napraviti i sa zabranom pristupa internetu sigurnosnom mjerom koja zahtijeva nečinjenje, ograničavajući je na tzv. računalni kriminalitet, kako je i prihvaćen u međunarodnom pravu,<sup>47</sup> obuhvaćajući kaznena djela protiv računalnih sustava, programa i podataka (glava XXV. Kaznenog zakona), kaznena djela protiv intelektualnog vlasništva (glava XXVII.) i kaznena djela seksualnog iskorištavanja djece. Uostalom, pri obrazlaganju te sigurnosne mjere predlagatelj je (egzemplifikativno) nabrojio upravo takva kaznena djela – „*hacking*, dječja pornografija, objavljivanje piratskih sadržaja i sl.“<sup>48</sup>

*Ratio* svođenja zabrane pristupa internetu za naprijed navedena kaznena djela predstavlja okolnost da su zbog značajki njegova korištenja (anonimnost, dostupnost ogromne količine sadržaja, mogućnost jednostavnog uklanjanja tragova, brzina, nepostojanje prostorne ograničenosti, povezivanje i dostupnost iznimno velikog broja supočinitelja i potencijalnih žrtvi, neadekvatni okviri međunarodne pravne pomoći, olakšana ponuda ilegalnih sadržaja za osobe koji nisu računalni stručnjaci) upravo ona postala teško ostvariva (iako ne nemoguća) bez pomoći interneta, uzrokuju iznimno teške posljedice, a pojačana opasnost počinitelja potencirana je njihovim jednostavnim ostvarenjem i otežanim otkrivanjem (primjerice, do sredine 1980-tih distribucija dječje pornografije u SAD-u bila je gotovo eliminirana, sve do masovne uporabe interneta<sup>49</sup>). Time opasnost da će počinitelj upravo ta protupravna ponašanja pokušati ponovo ostvariti putem interneta postaje doista ozbiljna, ali pod uvjetom da je dostupnost interneta bila odlučujući faktor za počinjenje kaznenog djela. Konkretno, kod povrede prava intelektualnog vlasništva nije svejedno je li počinitelj putem interneta pribavio ili distribuirao objekt kaznenog djela ili je elektroničkim putem samo ispunio obrazac prodajnog oglasa u novinama.

Načelo razmjernosti iz čl. 67. Kaznenog zakona predviđa proporcionalnost sigurnosne mjere i prema počinjenom kaznenom djelu, premda ono samo za sebe ne upućuje na stupanj opasnosti od počinjenja budućeg kaznenog dje-

---

<sup>47</sup> Usp. čl. 2.- 10. Konvencije o kibernetičkom kriminalu Vijeća Europe.

<sup>48</sup> Vlada Republike Hrvatske, Konačni prijedlog Kaznenog zakona, listopad 2011., str. 157.

<sup>49</sup> Sullivan, J.L., kao u bilješci 26, str. 943.

la i unatoč tome što sigurnosna mjera ima sasvim drugu svrhu nego kazna. Samo je za dvije sigurnosne mjere predviđeno da se mogu izreći tek kada je počinjeno kazneno djelo određene težine, i to apstraktne težine (propisana kazna zatvora od najmanje jedne godine) kod sigurnosne mjere obveznog psihijatrijskog liječenja odnosno konkretne težine (izrečena kazna u trajanju od najmanje dvije ili pet godina zatvora) kod sigurnosne mjere zaštitnog nadzora nakon punog izvršenja kazne zatvora. Premda se može činiti da je kod većine sigurnosnih mjera namjerno izostavljeno da se izriču uz oslobođenje od kazne,<sup>50</sup> ipak se ne radi o odrazu načela da one moraju biti razmjerne počinjenom kaznenom djelu, već o tome da je pri izradi Zakona „zaboravljeno“ da se mogu izreći i u takvim slučajevima.<sup>51</sup> Neka strana zakonodavstva ipak ograničavaju i sigurnosne mjere s obzirom na izrečenu kaznu, pa je tako za primjenu zabrane obavljanja određene dužnosti ili djelatnosti, koja također u bitnoj mjeri zadire u temeljna prava i slobode, sukladno čl. 67. st. 1. švicarskog Kaznenog zakona potrebno izricanje kazne zatvora preko šest mjeseci ili novčane kazne preko 180 dnevnih iznosa. Ta problematika kod sigurnosne mjere zabrane pristupa internetu u hrvatskom zakonodavstvu ipak je samo sporedne prirode – da nije neopravdano uvedena potpuna zabrana korištenja interneta i da su uže određena kaznena djela za koja se izriče, ograničenje temeljnih ljudskih prava ne bi bilo tako teško da bi načelo razmjernosti podrazumijevalo neprimjenu sigurnosne mjere na propisanu ili izrečenu kaznu određene težine.

## V. OGRANIČENJE PRISTUPA INTERNETU KAO POSEBNA OBVEZA

Uvjetna osuda, rad za opće dobro i uvjetni otpust prema novom Kaznenom zakonu mogu se izreći uz dodatnu posebnu obvezu. Kako su u čl. 62. st. 2. nabrojene samo egzemplifikativno, zasigurno ima mjesta da se počinitelju kaznenog djela tim putem ograniči pristup internetu, čime se otvara problematika odnosa prema sigurnosnoj mjeri zabrane pristupa toj mreži s aspekta načela razmjernosti, u dijelu koji se odnosi na primjenu jednako učinkovite, a manje intruzivne kaznenopravne sankcije. Tome svakako pogoduje okolnost da je jedna od svrha posebnih obveza iz čl. 63. st. 2. Kaznenog zakona (pored zaštite žrtve kaznenog djela) istovjetna svrsi sigurnosnih mjera i odnosi se na otklanjanje okolnosti koje pogoduju ili poticajno djeluju na počinjenje novog kaznenog djela. Međutim, kada je zakonodavcu, umjesto ograničavanja, prihvatljivija sigurnosna mjera potpune zabrane pristupa internetu čak i kod lakog

---

<sup>50</sup> Čl. 68. st. 2., čl. 69. st. 2., čl. 70. st. 2., čl. 73. st. 2. i čl. 74. st. 2. Kaznenog zakona.

<sup>51</sup> Usp. obrazloženje uz čl. 68. st. 2., Vlada Republike Hrvatske, Konačni prijedlog Kaznenog zakona, listopad 2011., str. 153.

protupravnog ponašanja koje za kaznenopravnu posljedicu ima oslobođenje od kazne, u kojoj je mjeri prihvatljivo zabraniti pristup internetu kada je riječ o posebnoj obvezi?

Generalna klauzula iz čl. 63. st. 1. Kaznenog zakona, u dijelu koji se odnosi na zabranu primjene nerazumnih posebnih obveza, preuzeta je iz njemačkog, dok je u dijelu koji se odnosi na zabranu povrede dostojanstva okrivljenika preuzeta iz španjolskog zakonodavstva.<sup>52</sup> Prema njemačkoj pravnoj doktrini smatra se da se nerazumnost tiče ne samo sadržaja obveze već i njezine mjere, primjerice ako je riječ o obvezi koja onemogućuje zadržavanje zaposlenja ili o nerazmjerno teškom ograničavanju prava osuđenika zbog lakšeg kaznenog djela.<sup>53</sup> To nesumnjivo upućuje na promicanje posebne obveze ograničavanja pristupa internetu umjesto njegove potpune zabrane, pogotovo kada je riječ o uvjetnoj osudi i radu za opće dobro kojima se nastoji izbjeći izvršavanje lakše kazne. Situacija je nešto drugačija kada se radi o uvjetnom otpustu ili djelomičnoj uvjetnoj osudi, kada su i njemački sudovi skloni ne samo stavljati posebnu obvezu potpune zabrane pristupa internetu već i zbog njezina „teškog i upornog“ kršenja donositi odluke o opozivu. U tom su slučaju, ipak, temelj zaključku da probatorni uvjet nije nerazuman (navedeno je i da osuđenik ima raspoložive „tradicionalne“ načine pristupa informacijama) izrazito teške okolnosti kaznenog djela (osuda na zatvorsku kaznu za seksualno zlostavljanje djece i distribucija dječje pornografije trećim osobama putem računala), a kršenje probatornog uvjeta prelazi granice nužne uporabe interneta (administriranje web stranica i korištenje društvenih mreža).<sup>54</sup> U španjolskoj sudskoj praksi nije se primjenjivala generalna klauzula kako bi se kao dodatna obveza uz uvjetnu osudu stavilo ograničenje ili zabrana pristupa internetu, ali se smatra da bi razvojem legislative i institucija izvršnog sustava restrikcija (ali ne i prohibicija) prava na pristup tehnologiji, uz pripadajući nadzor, mogla postati prihvatljiva u okviru probacije kod visokog rizika od recidivizma za najteža kaznena djela (određene kategorije seksualnih prijestupnika i opasni počinitelji kibernetičkih kaznenih djela).<sup>55</sup>

---

<sup>52</sup> Vlada Republike Hrvatske, Konačni prijedlog Kaznenog zakona, listopad 2011., str. 150.

<sup>53</sup> Illert, H., *Aspekte einer Implementierung des elektronisch überwachten Hausarrest in das deutsche Recht*, Göttingen, 2005., str. 95. - 96., Schlömer, U., *Der elektronisch überwachte Hausarrest*, Frankfurt a/M, 1998., str. 194. - 196., Schneider, K., *Electronic Monitoring (Alternativer Strafvollzug oder Alternative zum Strafvollzug?)*, Baden - Baden, 2003., str. 115. - 116.

<sup>54</sup> OLG Frankfurt, 3. Strafsenat, 3 Ws 839/10 od 7. rujna 2010.

<sup>55</sup> Felip i Saborit, D., *¿Poner puertas al campo? Sobre la posibilidad de prohibir penalmente el uso de las tecnologías de la información y la comunicación*, *Revista catalana de dret públic*, br. 35, 2007 (ed. web), str. 16. - 18., 20. - 21., dostupno na [http://www10.gencat.net/eapc\\_revistadret/](http://www10.gencat.net/eapc_revistadret/) (5. rujna 2012.)

Različito od sadržajnog ograničenja pristupa internetu, pod koje se može podvesti i obveza instaliranja programa koji korisniku računala blokira pristup određenim uslugama, upitno je mogu li se pod posebnu obvezu podvesti nadzorni softveri koji prate korisnikovu aktivnost i slučajeve potencijalnih zlouporaba dojavljuju probacijskom službeniku. Premda u dijelu njemačke pravne doktrine postoji mišljenje da je elektronički nadzor neodgovarajući da bude obveza uz uvjetnu osudu, bilo zato što se sagledava kao kontrola bez sadržaja ili što nadzorna komponenta prevladava nad pružanjem pomoći i resocijalizacijom počinitelja,<sup>56</sup> prevladavaju drugačija mišljenja.<sup>57</sup> Premda su pobornici opravdanosti elektroničkog nadzora uz uvjetnu osudu suglasni da bi njegova primjena samo zbog kontrole i(li) kažnjavanja bila neprihvatljiva, ostaje činjenica da integraciju počinitelja u društvo ne stavljaju u izravni kontekst sa sadržajem nadzora, već obvezom koja se nadzire. Postavlja se stoga pitanje nije li riječ o nespretnom miješanju materijalnog i izvršnog kaznenog zakonodavstva te napuštanju smisla upute kao materijalnopravne obveze počinitelja, sve kako bi se opravdala mogućnost uvođenja elektroničkog nadzora uz uvjetnu osudu. Unatoč dugogodišnjoj primjeni u Hesseu, niti jedna druga pokrajina nije ga uvela u praksu.

Predvidivo je, dakle, da će posebna obveza iz čl. 62. Kaznenog zakona u sudskoj praksi potisnuti sigurnosnu mjeru zabrane pristupa internetu, iz više razloga. Različito od sigurnosnih mjera čije je izvršavanje statično, posebne obveze su elastične i mogu se skratiti, ukinuti ili zamijeniti drugima, što preneseno na ograničenje pristupa internetu znači da se osuđenikova obveza može kontinuirano prilagođavati razvoju tehnologije. Nadalje, zakonodavac je isključio primjenu sigurnosnih mjera obveznog psihosocijalnog tretmana, zabrane približavanja i udaljenja iz zajedničkog kućanstva kod uvjetne osude i rada za opće dobro baš zbog sadržajnog preklapanja s odgovarajućim posebnim obvezama,<sup>58</sup> pa nema razloga da se isto shvaćanje ne reflektira i na sigurnosnu mjeru zabrane pristupa internetu. Isto tako, budući da ograničenje pristupa internetu, umjesto potpune zabrane, može biti jednako učinkovito za odvratanje osuđenika od počinjenja kaznenih djela, primjena načela razmjernosti nalaže odabir posebne obveze kod koje je takvo, manje intruzivno, zadiranje u njegova prava moguće. Dapače, zbog činjenice da se može primijeniti kod djelomične uvjetne osude i uvjetnog otpusta, posebna obveza ograničenja pristupa internetu mogla bi potisnuti sigurnosnu mjeru i za slučaj institucionalnog zatvaranja počinitelja.

---

<sup>56</sup> Usp. Illert, H., kao u bilješki 53, str. 91.- 92.

<sup>57</sup> Illert, H., kao u bilješki 53, str. 93.- 94., Schlömer, U., kao u bilješki 53, str. 186.- 191., Schneider, K., kao u bilješki 53, str. 113.- 118.

<sup>58</sup> Čl. 70. st. 2., čl. 73. st. 2. i čl. 74. st. 2. Kaznenog zakona; usp. obrazloženje uz čl. 70. st. 2. Kaznenog zakona, Vlada Republike Hrvatske, Konačni prijedlog Kaznenog zakona, listopad 2011., str. 155.



Naposljetku, za razliku od sigurnosne mjere, izvršenje posebnih obveza može se kumulirati uz zaštitni nadzor. Time nije dovedeno u pitanje načelo razmjernosti, bez obzira na to što je takva kontrola za počinitelja teža nego nenadzirana sigurnosna mjera. Naime, navedeno načelo pretpostavlja odabir blaže kaznenopravne posljedice koja je jednako učinkovita, što ovdje nije slučaj, budući da se zaštitni nadzor primjenjuje samo ako bi nenadziranim posebnim obvezama bila dovedena u pitanje specijalna prevencija i integracija počinitelja u društvo. Upravo zato što potpuna zabrana korištenja interneta ima mjesta eventualno kod počinitelja izrazito teških kaznenih djela (i što nemogućnost sklapanja pretplatničkog odnosa ne predstavlja uspješnu kontrolu), može se dogoditi da će sudovi biti skloniji odrediti je uz dulje trajanje i dodatni nadzor, što je moguće jedino kroz posebne obveze uz djelomičnu uvjetnu osudu ili uvjetni otpust kumulirane sa zaštitnim nadzorom.

## VI. POREDBENO PRAVO

### a) Francuska

Prvotni, u Skupštini i Senatu usvojeni prijedlog Zakona o distribuciji i zaštiti autorskih i srodnih djela na internetu, nazvan HADOPI prema akronimu državne agencije koja ga je izvršavala, uključivao je izmjene propisa o intelektualnom vlasništvu uvođenjem isključivo administrativnih sankcija.<sup>59</sup> Bio je utemeljen na trofaznom „postupnom odgovoru“, prema kojem se konceptu navedena agencija, postupajući po obavijesti dobivenoj od predstavnika nositelja prava ili državnog odvjetnika, smatrajući da postoji ozbiljna sumnja na kršenje autorskog djela, mogla (putem pružatelja usluga pristupa internetu) porukom elektroničke pošte obratiti pretplatniku s upozorenjem da se internetska veza koristi za povredu autorskog djela te ga obavijestiti o njegovim obvezama, dostupnim legalnim izvorima autorskog djela, načinu na koji može zaštititi svoj priključak od neovlaštenog korištenja i mogućim posljedicama u slučaju daljnje povrede autorskog djela. Kod ponovljene sumnje na kršenje autorskog prava putem istog priključka u roku od šest mjeseci nakon primitka prvog e-maila, agencija je ponovo slala sličnu poruku elektroničkom poštom, s naznakom mjesta i vremena u kojem se dogodila povreda autorskog djela te svojim kontaktnim podacima. Konačno, ako bi se povreda i unatoč tome nastavila u roku od godine dana od nespornog primitka druge poruke, agencija je mogla nakon saslušanja stranaka, ovisno o stupnju protupravnosti, naložiti administrativne mjere, uključivo suspenziju pristupa komunikacijskoj mreži u

---

<sup>59</sup> *Projet de loi favorisant la diffusion et la protection de la création sur internet*, Assemblée nationale, n° 275 od 12. svibnja 2009.; *Sénat* n° 395 od 13. svibnja 2009.

trajanju od dva mjeseca do godine dana, s posljedičnom nemogućnošću sklapanja novog ugovora s bilo kojim pružateljem usluge pristupa internetu. Treba naglasiti da primjena takvih mjera nije polazila od premise da je korisnik priključka osobno kršio autorska prava, već da je propustio osigurati da se njegov priključak ne koristi u tu svrhu. Odlukom Ustavnog suda<sup>60</sup> primjena potonjih mjera proglašena je nedopustivim izricanjem kazne od tijela koje ne pripada sudbenoj vlasti, kao i kršenjem presumpcije nevinosti, budući da je teret dokaza bio neosnovano prebačen na vlasnika priključka. Kao posljedica utvrđivanja neustavnosti pojedinih odredaba, proglašen je oklaštteni zakonski tekst, bez propisanih zakonskih posljedica kršenja autorskih prava nakon primitka druge poruke elektroničkom poštom od agencije.<sup>61</sup>

Paradoksalno, kaznenopravna sankcija zabrane pristupa internetu uslijedila je kao odgovor na potrebu jače zaštite prava okrivljenika. Naime, nakon svega nekoliko mjeseci, u listopadu 2009., prvi je propis zamijenjen novim Zakonom o kaznenoj zaštiti literarnog i umjetničkog vlasništva na internetu (tzv. HA-DOPI 2).<sup>62</sup> Njime se Zakon o intelektualnom vlasništvu mijenja tako da agencija u posljednjoj fazi, umjesto samostalne primjene administrativnih sankcija, tužiteljstvu proslijeđuje spis radi eventualnog vođenja kaznenog postupka. On u konačnici može rezultirati novčanom i zatvorskom, ali i dodatnom kaznom suspenzije pristupa javnoj mrežnoj komunikaciji. Izvorno, ta se kazna mogla izreći, u trajanju do godine dana, za klasična kaznena djela povrede autorskih prava (čl. L 335-2 do L 335-4-2 Zakona o intelektualnom vlasništvu), a naknadnim zakonskim izmjenama<sup>63</sup> i za novo kazneno djelo grubog nemara u zaštiti autorskih i srodnih djela. Počinitelj potonjeg ne krši osobno tuđa prava, već je bez opravdanog razloga, nakon nespornog osobnog primitka druge poruke od agencije, propustio zaštititi svoj priključak u javnoj mrežnoj komunikaciji, a on je u roku od godine dana upotrijebljen za neovlašteno iskorištavanje prava intelektualnog vlasništva. Za to kazneno djelo mjera dodatne kazne suspenzije pristupa javnoj mrežnoj komunikaciji iznosi jedan mjesec.

Pretpostavka je navedene dodatne kazne počinjenje kaznenog djela putem javne mrežne komunikacije, uključuje suspenziju mrežnog priključka i zabranu ugovaranja sličnih usluga s drugim pružateljem usluga, njezina primjena ne može dovesti do nemogućnosti korištenja usluga telefona ili televizije, troškovi izvršavanja padaju na teret osuđenika, a provodi se tako da agencija,

---

<sup>60</sup> Conseil Constitutionnel, odluka br. 2009-580 od 10. lipnja 2009.

<sup>61</sup> LOI n° 2009-669 favorisant la diffusion et la protection de la création sur internet od 12. lipnja 2009.

<sup>62</sup> LOI n° 2009-1311 relative à la protection pénale de la propriété littéraire et artistique sur internet od 28. listopada 2009.

<sup>63</sup> Décret n° 2010-695 instituant une contravention de négligence caractérisée protégeant la propriété littéraire et artistique sur internet od 25. lipnja 2010.

pod prijetnjom novčane kazne od 5.000 eura, obavještava pružatelja usluga da je dužan u roku od 15 dana prekinuti pretplatnički odnos s osuđenikom (čl. L 335-7 i L335-7-1 Zakona o intelektualnom vlasništvu). Članak L 335-7-2 Zakona sadržava smjernice sudu za primjenu te dodatne kazne i određivanje njezina trajanja, određujući da u obzir mora uzeti prirodu i težinu kaznenog djela te ličnost počinitelja, a osobito njegovu društvenu i poslovnu aktivnost te socio-ekonomski status. Trajanje kazne mora odražavati ravnotežu između zaštite intelektualnog vlasništva i poštovanja prava na slobodu izražavanja i komunikacije, osobito iz vlastitog doma.

Francusko rješenje nije naišlo na osobit odjek u međunarodnim okvirima – „postupni odgovor“ u Europi postoji samo u engleskom zakonodavstvu, isključivo u administrativnim granicama;<sup>64</sup> pokušaj implementacije prilikom revizije telekomunikacijske regulative Europske unije završio je na općenitom određivanju smjernica za primjenu načela razmjernosti kod ograničavanja prava na pristup uslugama;<sup>65</sup> specijalni izvjestitelj UN-a za promicanje i zaštitu prava i slobode mišljenja i izražavanja, osvrćući se na francusko i englesko rješenje, naveo je da uskrata pristupa internetu, „bez obzira na opravdanje, uključujući i utemeljenost na kršenju prava o intelektualnom vlasništvu“ predstavlja povredu Međunarodnog pakta o građanskim i političkim pravima,<sup>66</sup> a izričite odredbe o tom konceptu izostavljene su čak i iz konačnog teksta sporazuma ACTA.<sup>67</sup>

\* \* \*

Razlike između francuskog i hrvatskog kaznenopravnog rješenja su mnogobrojne (francusko zakonodavstvo detaljnije određuje načelo razmjernosti; primjenjuje sankciju na uski krug kaznenih djela; pretpostavlja formiranje agencije sa širokim ovlastima u svezi s prikupljanjem podataka o identitetu korisnika, njegovim upozoravanjem, certifikacijom programa za zaštitu računala od povrede autorskih prava te koordinacije izvršenja kaznenopravne sankcije), ali ključne su dvije:

– suspenzija mrežnog pristupa u francuskom zakonodavstvu nije sigurnosna mjera, već dodatna kazna, što pretpostavlja i punitivni, a ne isključivo rehabilitativni karakter kaznenopravne sankcije, kao i ostvarenje ciljeva koji

---

<sup>64</sup> Digital Economy Act 2010 (c.24), čl. 2. - 18.

<sup>65</sup> Boardman, M., kao u bilješci 16, str. 232. - 234., Lucchi, N., Access to network services and protection of constitutional rights: recognizing the essential role of internet access for the freedom of expression, *Cardozo Journal of International & Comparative Law*, vol. 19., br. 3/2011, str. 655. - 657.

<sup>66</sup> Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27 od 16. svibnja 2011., odjeljak 49, 78, 79.

<sup>67</sup> *Ib.*, odjeljak 50.

premašuju puko otklanjanje uvjeta koji omogućuju ili poticajno djeluju na počinjenje novog kaznenog djela (npr. izražavanje društvene osude, generalna prevencija). To svojstvo osobito dolazi do izražaja zbog toga što se navedena kaznenopravna sankcija javlja kao reakcija na oglašivanje vlasnika priključka na višekratna upozorenja o kršenju autorskih prava i mogućim posljedicama, sa sistemskog gledišta nevezana uz težinu počinjenog kaznenog djela. Naime, postoje i teža s internetom povezana kaznena djela (npr. dječja pornografija, računalna prijevarena), njihovu počinitelju ne daje se druga i treća prilika prije pokretanja kaznenog postupka, ali isto tako ne povlače za sobom dodatnu kaznu suspenzije mrežnog pristupa. To je selektivno kažnjavanje prihvatljivo ako se ta kaznenopravna posljedica promatra kao kazna, ali ne i kada je riječ o sigurnosnoj mjeri za čiju je primjenu relevantna opasnost počinitelja, pa bi eventualno prethodno upozoravanje počinitelja imalo vrijednost tek kao jedan od mnogobrojnih indikatora takve opasnosti;

– paradoksalno, francuska kazna niti izbliza se ne kosi s ostvaranjem ciljeva rehabilitacije kao kada je riječ o hrvatskoj „rehabilitativnoj“ sigurnosnoj mjeri. Raskidanje postojeće pretplate obveza je pružatelja usluga i jedina je zabrana za počinitelja suzdržavanje od sklapanja pretplatničkog odnosa za mrežnu uslugu, s time da njezino kršenje ne povlači opoziv uvjetne osude ili rada za opće dobro vezanog uz glavnu kaznu, već novu kaznu (čl. L 335-7-1 Zakona o intelektualnom vlasništvu). Posljedično, osuđenik se može koristiti internetom s tuđe točke pristupa, na radnom mjestu, u internet-kafićima i sl., pri čemu nije nevažno da je vlasnik svakog priključka dužan osigurati ga tako da njegovim korištenjem ne dođe do kršenja intelektualnog vlasništva (u suprotnom, mogao bi počinuti kazneno djelo grubog nemara u zaštiti autorskih i srodnih prava). Takva reducirana zabrana pristupa internetu zasigurno ne može poslužiti kao sadržaj sigurnosne mjere u hrvatskom zakonodavstvu, budući da uvjet koji omogućuje ili mu počinjenje novog kaznenog djela pogoduje nije puko posjedovanje vlastitog priključka, već činjenica da se počinitelj koristio internetom. Uostalom, materijalna pretpostavka za primjenu sigurnosne mjere zabrane pristupa internetu nije postojanje opasnosti od počinjenja novog kaznenog djela putem vlastitog priključka, već opća uporaba interneta.

## **b) Sjedinjene Američke Države**

Sudska praksa federalnog Prizivnog suda u odnosu na zabranu ili ograničenje pristupa internetu kao obveze uz nadzirani otpust (nadzirana obveza osuđenika koji je izdržao dosuđenu kaznu zatvora, čiji se sadržaj i trajanje određuju već pri samom izricanju kazne) ravna se prema Smjernicama za kažnjavanje. Prema njima, obveza uz nadzirani otpust može se odrediti ako je razumno povezana s prirodom i okolnostima kaznenog djela te prijašnjim

životom i karakteristikama počinitelja, kada se poštuje pravni poredak i osigurava pravično kažnjavanje, pruža primjereno odvracanje od kažnjivog ponašanja, štiti javnost od daljnjih kaznenih djela osuđenika, pruža potrebna edukacija i drugi tretman; sve pod uvjetom da se osuđeniku ne ograničava sloboda više nego što je nužno.<sup>68</sup>

Prvi slučaj u kojem je na federalnoj razini primijenjeno ograničenje pristupa internetu odnosi se na notornog hackera Kevina Mitnicka, kojemu je još 1988. godine zbog federalnih kaznenih djela kao uvjet uz nadzirani otpust nakon odsluženja kazne zatvora od 12 mjeseci određena i zabrana neovlaštenog pristupa računalu ili komunikacijskoj mreži, u trajanju od tri godine. Nakon što ju je prekršio i kao bjegunac počinio više kaznenih djela, naposljetku mu je 1998. godine određena zabrana upotrebe računala, programa ili druge elektroničke opreme koja bi mogla omogućiti pristup računalu ili telekomunikacijskoj mreži bez odobrenja probacijskog službenika. Takva obveza postavljena je kao uvjet uz nadzirani otpust nakon odsluženja četverogodišnje kazne zatvora.<sup>69</sup> Dakle, iako je bila riječ o recidivistu u počinjenju najtežih računalnih kaznenih djela, sud mu ipak nije u potpunosti zabranio pristup internetu.

Nakon toga, federalna se praksa kaznenopravnog reguliranja pristupa internetu svela isključivo na slučajeve iskorištavanja djece preko interneta,<sup>70</sup> pri čemu nije nepoznato ni izricanje potpune zabrane pristupa internetu. Ističe se da su pojedini okruzi prizivnog suda skloniji izricanju (apsolutne) zabrane, a drugi ograničenju pristupa internetu,<sup>71</sup> ili da isti okrug zna odstupati od vlastitih precedenata u pogledu obrazlaganja načela razmjernosti.<sup>72</sup> Ipak, smatra se da je sudskoj praksi zajedničko to da za izricanje (potpune) zabrane pristupa internetu nije dovoljno puko posjedovanje dječje pornografije, već počiniteljevo ponašanje mora predstavljati osobito teško kazneno djelo (distribuiranje ili proizvodnja dječje pornografije, mamljenje djeteta na seksualne odnose ili snimanje pornografske predstave i sl.).<sup>73</sup> To, međutim, nije garancija da će počiniteljima tih najtežih kaznenih djela takav uvjet uz nadzirani otpust biti izrečen. Dapače, dolazi do paradoksa da se onome koji je samo posjedovao dječju pornografiju stavi funkcionalno ograničenje pristupa internetu, a da se

---

<sup>68</sup> 18 U.S.C. § 3583(d) u svezi s 18 U.S.C. § 3553(a).

<sup>69</sup> Krause, C.A., Pazicky, L.A.E., kao u bilješki 27, str. 201.-202.

<sup>70</sup> *Ib.*, str. 202.

<sup>71</sup> Adkins, J., kao u bilješki 24, str. 264.-270., Correll, F.E., kao u bilješki 26, str. 692 - 697., Sullivan, J.L., kao u bilješki 26, str. 949.-955.

<sup>72</sup> CRIMINAL LAW – SUPERVISED RELEASE – THIRD CIRCUIT APPROVES DECADE-LONG INTERNET BAN FOR SEX OFFENDER. – *United States v. Thielemann*, 575 F.3d 265 (3d Cir.2009), *Harvard Law Review*, vol. 123, br. 3/2009-2010, str. 778.-779.

<sup>73</sup> Cowin, S., kao u bilješki 31, str. 901.-902., Krause, C.A., Pazicky, L.A.E., kao u bilješki 27, str. 202., Wynton, S., kao u bilješki 35, str. 1863.- 1865.

počinitelju koji je takav sadržaj i distribuirao isto ograničenje odbacuje kao preopterećujuće.<sup>74</sup>

Federalni precedent U.S. v. Lifshitz<sup>75</sup> odredio je pravne standarde za slučaj ograničenja pristupa internetu. Automatasko, na instaliranom računalnom programu zasnovano nadziranje i dojavljivanje probacijskom službeniku o možebitnom kršenju zabrane nije ograničeno pravnim standardom osnovanosti sumnje (suprotno, za pretragu računala potrebno je pribaviti informacije koje upućuju na zaključak o pristupanju internetu na nedopušteni način). Međutim, kako se nadziranje ne bi kosilo s opravdanim očekivanjem osuđenika na privatnost, ono mora biti usko prilagođeno, a niži sudovi moraju odlučiti koje su metode dopustive. Konkretno, osuđenik se za vrijeme nadziranog otpusta može obratiti sudu sa zahtjevom za promjenu obveze ako postoje novi načini računalnog nadziranja koji mu manje narušavaju privatnost, a ne dovode u pitanje učinkovitost kontrole (pritom se mora uzeti u obzir i stupanj tehnološkog znanja osuđenika). Posljedično, sudovi su obvezni kontinuirano revidirati pristup nadziranju, ovisno o dostupnoj tehnologiji i karakteristikama počinitelja.<sup>76</sup>

Prema praksi saveznih sudova pojedinih država, osim na nadzirani otpust, ograničenje pristupa internetu primjenjivo je i na uvjetnu osudu anglo-američkog tipa te na uvjetni otpust. Budući da je u pravilu riječ o lakšim kaznenim djelima, reduciranje osuđenikovih prava pojavljuje se u znatno blažem obliku nego u federalnim precedentima. Primjerice, maloljetniku koji je putem društvene mreže stupio u kontakt s prodavateljem i pribavio ukradeni motocikl, nerazmjernim i preopterećujućim ocijenjeni su probatorni uvjeti uporabe računala samo u svrhu povezanu sa školovanjem te zabrana pristupa chatroomovima, forumima i društvenim mrežama. Ostavljen mu je samo probatorni uvjet zabrane upotrebe računala za koje zna da ima instaliranu enkripciju, steganografiju ili maliciozni program.<sup>77</sup>

Reguliranje kaznenopravnog ograničenja pristupa internetu kao uvjeta uz probaciju ili uvjetni otpust nije zastalo na precedentnom pravu. Savezne države donijele su zakone u tom smjeru, najčešće za zlostavljачe djece i ostale seksualne prijestupnike (Florida, Georgia, Illinois, Indiana, New York, Teksas),<sup>78</sup> premda ima primjera normiranja tog uvjeta na računalni kriminalitet općenito

---

<sup>74</sup> Usp. Cowin, S., kao u bilješci 31, str. 887.-888.

<sup>75</sup> U.S. v. Lifshitz, 369 F.3d 173 (2d Cir. 2004).

<sup>76</sup> Curphey, S., kao u bilješci 35, str. 2262.

<sup>77</sup> In re J.J., Case No. D055603 (Cal. Ct. App., Oct. 15, 2010).

<sup>78</sup> Florida Statutes §948.30 (5 g,h); Georgia Code §42-8-35; 730 Illinois Compiled Statutes §5-6-3; Indiana Code §35-38-2-2.2; New York Penal Law §65.10 (4-a, 5); Texas Government Code §508.1861.

(Kalifornija, Minesota).<sup>79</sup> Riječ je mahom o ograničavanju pristupa internetu – obvezom podvrgavanja nadzoru, zabranjivanjem pristupa određenim sadržajima i(li) pristupa bez prethodnog dopuštenja od probacijskog službenika ili druge osobe. Iznimka je Nevada gdje se najtežim seksualnim prijestupnicima mandatorno, a ostalim počiniteljima kaznenih djela koja uključuju računalo, računalni sustav ili mrežu fakultativno, uz uvjetnu osudu ili otpust primjenjuje rigorozna „zabrana posjedovanja računala, uključivo, bez ograničenja, upotrebu elektroničke pošte, chatrooma ili interneta“<sup>80</sup> Pored toga, legislativa pojedinih država (Sjeverna Karolina, Indiana, Nebraska) predviđa zasebna kaznena djela za registrirane seksualne prijestupnike koji pristupe društvenim mrežama (u slučaju Nebraske i forumima te chatroomovima), čak i nakon što su odslužili punu kaznu i ne nalaze se u režimu nadziranog otpusta.<sup>81</sup>

\* \* \*

Usporedba hrvatske sigurnosne mjere zabrane pristupa internetu s američkim zakonodavstvom i sudskom praksom nezahvalna je, iz sljedećih razloga:

– pravo na pristup internetu u Sjedinjenim Američkim Državama od osobitog je značenja za slobodu govora te je njegova (potpuna) zabrana iznimka „rezervirana“ za najteža kaznena djela seksualnih prijestupnika iz sfere kaznenopravne zaštite djece. Dapače, legislativa većine saveznih država takva je da je samo na tu kategoriju počinitelja primjenjivo kaznenopravno uređenje pristupa internetu, ali gotovo uvijek (osim u Nevadi) kao puko ograničenje koje se ne kosi s integracijom osuđenika u društvo. Obrazlažući uvođenje sigurnosne mjere u hrvatsko zakonodavstvo,<sup>82</sup> radna skupina niti riječ nije posvetila značenju interneta za ostvarenje temeljnih ljudskih prava, pa ne čudi da formirano rješenje ne odražava potrebu restriktivnog određivanja kruga kaznenih djela za koje je prihvatljiva zabrana iz sigurnosne mjere;

– obrazlaganje svrhe (potpune) zabrane pristupa internetu u američkoj sudskoj praksi nespojivo je s ciljevima koji se nastoje ostvariti hrvatskom sigurnosnom mjerom. Prvo valja naglasiti da precedenti upućuju na nespojivost zabrane pristupa internetu s alternativnim kaznenim sankcijama te ona ostaje u okvirima nadziranog otpusta. U tim ekstremnim slučajevima gotovo uvijek dolazi do (pre)naglašavanja svrha iz Smjernica za kažnjavanje koje se odnose na utvrđivanje potrebe zaštite javnosti i odvratanja počinitelja, bez

---

<sup>79</sup> California Penal Code §1203.047; Minnesota Statutes §243.055.

<sup>80</sup> Nevada Revised Statutes §176a.413.

<sup>81</sup> North Carolina General Statutes §14-202.5; Indiana Code §35-42-4-12; Nebraska Revised Statutes §28-322.05

<sup>82</sup> Vlada Republike Hrvatske, Konačni prijedlog Kaznenog zakona, listopad 2011., str. 157. - 158.

daljnijeg obrazlaganja.<sup>83</sup> Stoga cilj zaštite društva od počinitelja potiskuje potrebu otpuštenog zatvorenika za reintegraciju u društvenu zajednicu.<sup>84</sup> Dapače, nadzirani otpust uz onemogućavanje pristupa internetu opravdava se tako „da bi bez tih zabrana sud mogao biti prisiljen izreći dulju zatvorsku kaznu kada je prisutan rizik ponavljanja kaznenog djela“,<sup>85</sup> što nije argument koji bi se mogao upotrijebiti kod sigurnosne mjere koja ne samo da nije vezana uz vrstu i mjeru izrečene kazne nego se može izreći i kada se primijeni institut oslobođenja od kazne.

## VII. ZAKLJUČAK

Paradoksalno, to što sigurnosna mjera zabrane pristupa internetu predstavlja „inovaciju“ u poredbenim okvirima, ne znači da hrvatsko zakonodavstvo ide ukorak sa svojim vremenom, a kamoli da je ispred svoga vremena. Uostalom, uvođenjem te kaznenopravne sankcije nastojao se slijediti navodni međunarodni trend obuhvatnog kaznenopravnog zahvata u korištenje internetom. Apsurd leži u tome što je u fokusu strane doktrine i zakonodavstva zapravo kako što više zabaciti zabranu korištenja te mreže, sadržajno i u odnosu na kaznena djela na koja bi se primjenjivala.

Cijeneći značenje interneta u kontekstu pristupa i prosljeđivanja informacija, onemogućavanje njegova korištenja nema osobit rehabilitativni potencijal te je zadržka koju strana zakonodavstva i sudska praksa imaju prema njegovu kaznenopravnom onemogućavanju u potpunosti opravdana. Stoga apsolutna zabrana u poredbenim okvirima isključivo, iako ne prečesto, predstavlja ekstremnu reakciju na ekstremno kazneno djelo, i to ne bilo koje – uvijek se nadovezuje na izdržanu zatvorsku kaznu za najteže oblike seksualnog iskorištavanja djece. S obzirom na prevladavajuće nastojanje da se društvo zaštiti od osuđenika, osnovna svrha takve kaznenopravne reakcije i ne može postati integracija osuđenika u zajednicu, već izolacija od nje.

Između preostalih alternativa, ostaviti osuđenicima neometano korištenje internetom ili to pravo ograničiti, zasigurno se za uski krug kaznenih djela ponajbolja opcija može dovesti u vezu sa svrhom sigurnosnih mjera, a da pritom ne poprimi karakter kazne (premda uvođenje takve mogućnosti ima svoju cijenu – doslovno). Ipak, nužna fleksibilnost u kontinuiranom prilagođavanju trajanja, sadržaja i intenziteta takvog ograničenja potrebama osuđenika nije ostvariva primjenom neelastične sigurnosne mjere, već posebnih obveza uz uvjetnu osudu, rad za opće dobro i uvjetni otpust.

---

<sup>83</sup> Cowin, S., kao u bilješci 31, str. 898.

<sup>84</sup> Correll, F.E., kao u bilješci 26, str. 698.

<sup>85</sup> Adkins, J., kao u bilješci 24, str. 269.



Imaju li se na umu uvodne opaske, nedvojbeno se može zaključiti da je ova nova sigurnosna mjera u hrvatskom kaznenom zakonodavstvu otvorila ne samo niz praktičnih pitanja (za koja će biti interesantno vidjeti kako će ih rješavati sudska praksa) već podjednako dvojbe glede navedenih načelnih kriminalnopolitičkih pitanja povezanih s problematikom tih sankcija.

---

## Summary

### **REGARDING THE ISSUE OF THE SECURITY MEASURE OF PROHIBITION TO ACCESS THE INTERNET**

The issue of security measures, this secondary track in the genesis of criminal law, implies in general two fundamental aspects of criminal policy. In the first place, already traditionally, the aspect of the protection of fundamental human rights and freedoms: the history of security measures, especially of their practical application, is one of the 'grey' chapters of the most recent history of criminal law. The second aspect relates to the problem of achieving their original criminal-law nature or purpose at the level of the relationship between form and content: namely, pure repressive contents have frequently appeared (and still appear) in such criminal-law formats. From such general positions, it is interesting to note that the legislative formation of the security measures of prohibition to access the internet referred to in Article 75 of the Criminal Code, primarily in the context of its proportionality to the limitation of the convicted person's fundamental rights, to efficiency and to its relation with the special obligations accompanying a conditional sentence, community service, and conditional release. The issue of the relationship between legitimate interest to remove the conditions that allow or instigate the commission of a new criminal offence and the degree of touching upon the fundamental rights and freedoms has been intensified by the fact that the stated criminal-law sanction prevents the use of a wide range of services that do not affect recidivism, and, at the same time, the less intrusive, but equally efficient measures of restricting access to the internet are neglected. This paper also presents comparative legal systems and the way in which they regulate the restriction of access to this network, and how many points they have in common with the Croatian solution.