

Prof. dr Milan Milošević
Dr Vladimir Urošević

Pregledni naučni rad
UDK: 343.9.018(44)

BORBA PROTIV VISOKOTEHNOLOŠKOG KRIMINALA U REPUBLICI FRANCUSKOJ

Republika Francuska je jedna od najrazvijenijih država Evropske Unije. U martu 2008. godine Internet je u Republici Francuskoj koristilo 58.1% stanovništva, a broj korisnika je od tada u stalnom porastu. Tokom 2008. i 2009. godine borba protiv visokotehnološkog kriminala od strane Ministarstva unutrašnjih poslova Republike Francuske postavljena je kao prioritet radi očuvanja informacione strukture kao osnove savremenog informacionog društva. Francuski zakoni se konstantno prilagođavaju savremenoj praksi vezanoj za visokotehnološki kriminal, a struktura državnih organa Francuske namenjena borbi protiv ovog fenomena predstavlja primer efikasnog sistema za borbu protiv visokotehnološkog kriminala. Krivično pravna regulativa u Republici Francuskoj pruža efikasne okvire za sprečavanje ove pojave. Oštra kaznena politika koje se ogleda u visini zatvorskih kazni koje su zaprećene, kao i zaprećenim novčanim kaznama predstavlja i svojevrsan faktor odvraćanja od izvršenja krivičnih dela iz ove oblasti.

Ključne reči: *Republika Francuska, visokotehnološki kriminal, zloupotreba informacionih tehnologija, zloupotrebe podataka*

1. UVOD

Republika Francuska je jedna od ekonomski najrazvijenijih država Evropske Unije. Sa ukupno 65.073.482 stanovnika (prema procenama iz 01.01.2009. godine), 2.867 triliona američkih dolara BDP-a, površinom teritorije od 674.843 km² i povoljnim geostrateškim položajem predstavlja, pored Nemačke, najuticajnijiu državu u Evropskoj Uniji.

Sa tehničko-tehnološkog aspekta Republika Francuska je takođe među najnaprednijim državama u svetu. Broj korisnika Interneta na teritoriji Republike Francuske je procenjen na 36.153.327 korisnika u martu 2008. godine (58,1% ukupne populacije). Radi poređenja, može se

uzeti činjenica da je u Republici Srbiji broj korisnika u septembru 2006. godini bio 1.400.000 korisnika ili 13.9% ukupne populacije, a da je te iste godine broj korisnika u Republici Francuskoj bio 30.837.595 ili 50.3% ukupne populacije.¹

Tokom 2008. i 2009. godine borba protiv visokotehnološkog kriminala od strane Ministarstva unutrašnjih poslova Republike Francuske postavljena je kao prioritet upravo zbog činjenice da ugrožava osnovne temelje savremenog društva koje počiva na razmeni informacija, elektronskoj trgovini i drugim aktivnostima koje se odvijaju putem informacione infrastrukture koja je veoma ranjiva, a koja je neophodna da bi društvo kakvo danas poznajemo moglo da opstane i da se dalje progresivno razvija.

2. ORGANIZACIJA DRŽAVNIH ORGANA ZA BORBU PROTIV VISOKOTEHNOLOŠKOG KRIMINALA U REPUBLICI FRANCUSKOJ

Poznato je da je osamdesetih godina prošlog veka došlo do nakon nagle ekspanzije visokotehnološkog kriminala u Republici Francuskoj. Kao odgovor na tu pretnju bezbednosti, formirana je prva nacionalna jedinica za borbu protiv visokotehnološkog kriminala u okviru „Brigada Tigrova“ (Brigades du Tigre), jedne od elitnih jedinica francuske policije. Ova jedinica je osnovana 1994. godine i nosila je naziv Centralna brigada za sprečavanje informatičkog kriminaliteta (Vrigade Centrale de Répression de la Criminalité Informatique - B.C.R.C.I.). Tokom 1996. godine formirana je Brigada za sprečavanje zloupotreba i falsifikovanja industrijske svojine i umetničkih dela (Brigade Centrale pour la Répression des Contrefaçons Industrielles et Artistiques - B.C.R.C.I.A.).

Najzad, Centralna jedinica za borbu protiv kriminala u oblasti informacioninih i komunikacionih tehnologija (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication - O.C.L.C.T.I.C), koja i danas funkcioniše, formirana je tokom 2000. godine. Trenutno se u okviru pomenute Centralne nalaze dve službe, i to:

¹ <http://www.internetworldstats.com/eu/fr.htm> (06.01.2010. god.).

- Služba za borbu protiv visokotehnološkog kriminala nadležna za čitavu teritoriju Republike Francuske (Enquêteurs Spécialisés en Criminalité Informatique – ESCI),
- Služba za sprečavanje prevara izvršenih pomoću informacionih tehnologija (La Brigade d 'Enquête sur les Fraudes aux technologies de l 'Information - BEFTI).

Pored ove dve službe u sastavu jedinice nalaze se i službenici Direkcije za javnu bezbednost (Direction departementale de la securite publique – DDSP), kao i službenici Nacionalne žandarmerije – specijalisti za oblast Interneta i komunikacija.

Inače je Centralna jedinica za borbu protiv kriminala u oblasti informacionih i komunikacionih tehnologija osnovana Dekretom broj 2000-405 od 14. maja 2000. godine koji je usvojio Parlament Republike Francuske. Ovim dekretom jedinica je osnovana kao međuresorna institucija koja objedinjuje službe iz dva ministarstva, tj. iz Ministarstva unutrašnjih poslova i iz Nacionalne žandarmerije, koja je oficijelno vojna formacija. Članovima od 15 do 18 Dekreta ovoj jedinici (O.C.L.C.T.I.C) u nadležnost povereni su sledeći poslovi:

- Prikupljanje i obrada podataka o visokotehnološkom kriminalu
- Operativni poslovi
- Sprečavanje visokotehnološkog kriminala
- Statističke analize
- Borba protiv specifičnih kriminoloških fenomena i kriminoloških fenomena koji imaju međunarodnu dimenziju (saradnja i rad u okviru Interpola, Šengena i Europa).

Na nacionalnom planu poslovi koji su povereni ovoj jedinici su:

- Prikupljanja informacija o visokotehnološkom kriminalu i koordinacija rada službi koje se bave sprečavanjem ove pojave
- Angažovanje službenika sudske policije i stručnih službenika policije u osetljivim slučajevima na nacionalnom i međunarodnom planu
- Pružanje tehničke pomoći centralnim i lokalnim jedinicama policije u slučajevima kada je ona potrebna.²

² <http://www.securiteinfo.com/legal/OCLCTIC.shtml>, (06.01.2010. god.).

Prema tome, jedinica O.C.L.C.T.I.C na međunarodnom planu ima veoma značajne zadatke koji su joj Dekretom poverene u nadležnost. Na tom planu joj je poveren kontakt i saradnja sa Interpolom po pitanjima visokotehnološkog kriminala, grupom koja je u okviru G8 zadužena za visokotehnološki kriminal, ekspertskom grupom Evropske komisije i grupom Europol za visokotehnološki kriminal, itd.

U ovoj jedinici ukupno je zaposleno oko 60 policijskih službenika, 12 vojnih službenika (pripadnici Nacionalne žandarmerije), kao i jedan inženjer telekomunikacija koji je nezavisno lice zaposleno u preduzeću Telekom Francuske. Ostalo, pomoćno osoblje se angažuje iz javnog i privatnog sektora u zavisnosti od potrebe.

Druge jedinice koje se bave sprečavanjem visokotehnološkog kriminala na nacionalnom nivou su Brigada za sprečavanje zloupotreba u oblasti industrijske i intelektualne svojine (La Brigade Centrale pour la Répression des Contrefaçons Industrielles et Artistiques- BCRCIA) i Nacionalno odeljenje za sprečavanje prekršaja protiv ljudi i imovine (La Division Nationale pour la Répression des Atteintes aux Personnes et aux Biens - DNRAPB).

Pored navedenih centralnih jedinica na nacionalnom nivou u policijskim prefekturama na teritoriji Republike Francuske postoji i 19 grupa za intervencije u slučajevima visokotehnološkog kriminala raspoređenih po administrativnim oblastima, kao i tri regionalne grupe sa istom namenom. U svim jedinicama na teritoriji Francuske postoje pripadnici policije i žandarmerije koji su prošli osnovnu obuku za borbu protiv visokotehnološkog kriminala, nakon koje su na korišćenje dobili i opremu za primarne intervencije u slučajevima krivičnih dela iz ove oblasti kriminala.

U prefekturi Pariza koja, za razliku od drugih prefektura, ima i specijalan status pošto za svoj rad odgovara direktno direktoru policije, funkcionišu Brigada za istraživanje prevara u oblasti informacionih tehnologija (La Brigade d 'Enquête sur les Fraudes aux Technologies de l 'Information - BEFTI) u kojoj radi 30 službenika policije, Brigada za sprečavanje prevara u oblasti sredstava plaćanja (La Brigade des Fraudes aux Moyens de Paiement - BFMP) u kojoj radi 56 službenika i Brigada za sprečavanje zloupotreba u oblasti intelektualne svojine (La Brigade de Répression de la délinquance Astucieuse - BRDA) u kojoj je zaposleno 54 službenika.

Navedene jedinice policije najveću pažnju u svom radu posvećuju zloupotrebama na Internetu, zloupotrebama u savremenim informacionim tehnologijama i falsifikovanju i zloupotrebama platnih kartica. U okviru ovih jedinica nalaze se i službenici koji učestvuju u timu za hitne intervencije (Computer Emergency Responce Team – CERT) Francuske koji se angažuje u urgentnim slučajevima.

Na teritoriji Francuske ove jedinice međusobno blisko saraduju, a posebna saradnja ostvaruje se između Centralne jedinice za borbu protiv kriminala u oblasti informacionih i komunikacionih tehnologija sa Brigadom za zaštitu od prevara u oblasti informacionih tehnologija (La Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information - B.E.F.T.I.), Direkcijom za nadgledanje teritorije (Direction de la Surveillance du Territoire - D.S.T), Nacionalnom žandarmerijom (La Gendarmerie Nationale) i Carinskom službom (Les Douanes).

Brigada za zaštitu od prevara u oblasti informacionih tehnologija osnovana je 1994. godine, i u njenom sastavu se nalazi dvadeset službenika policije. Teritorijalna nadležnost ove brigade proteže se na grad Pariz sa predgrađima. U većini slučajeva, službenici brigade rade na slučajevima povrede autorskog prava (muzika, softveri itd).

Direkcija za nadgledanje teritorije Republike Francuske (Direction de la Surveillance du Territoire - DST) nastala je 1944. godine radi borbe protiv špijunaže i protiv uticaja stranih sila na teritorijama pod francuskim suverenitetom. Do 1970. godine ova direkcija pretrpela je značajne izmene izazvane zbog dva nova fenomena. Naime, špijunaža je ranije bila isključivo vezana za vojne ciljeve, a od tada je proširena na ekonomski i naučno-tehnički aspekt, kao i na terorističke pretnje. Smatra se da je danas sve značajnije da postoji jaka služba unutrašnje bezbednosti čija je primarna funkcija obezbeđivanje sigurnosti i praćenje rada stranih obavještajnih službi na teritoriji Francuske.³

Žandarmerija je konstantno angažovana u poslednjih nekoliko godina u borbi protiv novih oblika kriminala, posebno u vezi sa Internetom. Od 1998. godine Nacionalna žandarmerija je uočila izazov

³ Tokom 2008. godine uspostavljena je Centralna direkcija za unutrašnji obavještajni rad (Direction Centrale du Renseignement Intérieur - DCRI) objedinjavanjem dve bivše službe Ministarstva unutrašnjih poslova, *Direkcije za nadzor teritorije* (DST) i *Direkcije za opšta obavještenja* (Direction des Renseignements Generaux - DRG). Oko 7.000 pripadnika Centralne direkcije za unutrašnji obavještajni rad, organizovano je u okviru *Uprava za zaštitu komunikacija i još pet centralnih uprava*.

postavljen pred policiju naglim porastom zloupotreba savremenih tehnologija i odgovorila je uspostavljanjem adekvatne strukture i odgovarajuće obuke za svoje pripadnike.

U okviru Nacionalne žandarmerije osnovano je Odeljenje za tehnički servis i obradu dokumentacije o sajber kriminalu sudske policije (Département cybercriminalité du service technique de recherches judiciaires et de documentation - STRJD) koje se bavi nadgledanjem Internet mreže u potrazi za krivičnim delima protiv lica i imovine (nadgledaju se Internet sajtovi, IRC, diskusione grupe, socijalne mreže, Peer to Peer mreže). U okviru Instituta za istraživanje kriminala Nacionalne žandarmerije (l'institut de recherche criminelle de la Gendarmerie nationale - IRCGN) nalazi se Katedra za elektroniku i računare koja se bavi razvojem metoda, alata i softvera za automatsku detekciju fotografija sa pedofilskim sadržajem i otkrivanje preuzimanja ovih podataka od strane korisnika Interneta.

U oktobru 2003. godine, Nacionalna žandarmerija je bila zadužena da u saradnji sa Nacionalnom policijom osnuje Nacionalni centar za slike sa pedopornografskim sadržajem (le centre national d'images pédopornographiques - CNAIP). U ovom centru prikupljaju se i klasifikuju u baze podaci o svim slikama (do danas ih ima preko 470 000) i video materijalima oduzetim prilikom krivičnih istraga. Ove baze podataka su značajne za dalje istrage, sudske postupke i sl.

Od 2002. godine Nacionalna žandarmerija organizuje je i specijalne obuke u oblasti savremenih tehnologija radi specijalizacije svojih službenika. Ova obuka poznata je kao „N-Tech“ i sprovodi se u Nacionalnom centru za obuku sudske policije (Centre national de formation de police judiciaire - CNFPJ) koji se nalazi u gradu Fontenblou (Fontenblou). Svake godine u Centru oko 30 istražitelja prolazi ovu obuku, a krajem 2008. godine ukupno je obučeno 190 istražitelja koji su raspoređeni u specijalizovane jedinice širom blike Francuske.

U Francuskoj postoje i teritorijalne jedinice Nacionalne žandarmerije. Kada su suočeni sa ovom vrstom kriminala, istražitelji iz teritorijalnih jedinica, koje su opšte po svojoj nameni, koriste pomoć stručnjaka specijalno obučenih za istrage vezane za visokotehnološki kriminal.

Odseci istražitelja (Les sections de recherches - SR), bave se specifičnim krivičnim delima u oblasti informacionih sistema. Ovi odseci

su namenjeni za ciljane nadzore Internet mreže koje obavljaju u saradnji sa Odeljenjem za tehnički servis i obradu dokumentacije o visokotehnološkom kriminalu sudske policije (STRJD).

U sastavu Brigade za sudske obaveštajne poslove sudske policije (Les Brigades Départementales de Renseignements et d'Investigations Judiciaires - BDRIJ) nalaze se forenzički eksperti (veštaci u krivičnim istragama, treneri za n-Tech obuke, kriminalistički analitičari itd) čija je uloga da, između ostalog, olakšaju razmenu iskustva i održavaju potrebni nivo tehničkih znanja i veština neophodnih za rad jedinica Nacionalne žandarmerije.⁴

U saradnji policije i žandarmerije stvorena je 13.04.2005. godine i Nacionalna platforma za prijavljivanje nedozvoljenog sadržaja na Internetu kojom se uspostavlja mogućnost za *On line* prijavljivanje slučajeva iz oblasti visokotehnološkog kriminala, kao i za međusobnu saradnju sa komercijalnim sektorom i drugim zainteresovanim stranama i pojedincima. Ova platforma efektivno funkcioniše od 01.01.2009. godine. Uvođenje nacionalne platforme za izveštavanje o ilegalnom sadržaju na Internetu je omogućilo:

- Efikasno izveštavanje o Internet sajtovima sa nezakonitim sadržajem (ksenofobija, pedofilija, terorizam, podsticanje na korišćenje droga, prostitucija, krađe, izazivanje rasne mržnje i neizvinjenje za zločine protiv čovečnosti itd).
- Centralizaciju podataka i prosleđivanje izveštaja nadležnim službama.

Uvedena je i telefonska platforma "prevare Info" za besplatno informisanje građana o prevarama na Internetu, koja je dostupna od ponedeljka do petka od 9 do 18 sati besprekidno.⁵

U Krivičnom zakoniku Republike Francuske u članu 113-1 navedeno je da se francuski zakoni primenjuju na celoj teritoriji Republike. Prema članu 113-2 Krivičnog zakona smatra se da je krivično delo počinjeno na teritoriji Republike Francuske ukoliko je samo jedna komponenta krivičnog dela izvršena na njenoj teritoriji. Dana 26.02.2002. godine sud najviše instance u Parizu (17. Veće) podsetio je da "francuske sudije imaju nadležnost u slučajevima kada su poruke ili

⁴<http://www.gendarmerie.interieur.gouv.fr/fr/sites/Gendarmerie/Presentation/PJ/PJ/Cybercriminalite> (06.01.2009. god.)

⁵ Minister De L'Interieur, De L'Outre-Mer Et Des Collectivites Territoriales La lutte contre la cybercriminalité De L'Interieur, De L'Outre-Mer Et Des Collectivites Territoriales, France, 2009, p.2-3.

sadržaj Internet sajta dostupni preko Interneta, na teritoriji Francuske.“⁶ Na čitavoj teritoriji Republike Francuske postoje specijalizovane sudije koje prolaze obuku vezanu za visokotehnoški kriminal.

Za krivična dela iz oblasti visokotehnoškog kriminala nadležno je Republičko tužilaštvo (Procureur de la République) koje se nalazi pri Vrhovnom sudu (Tribunal de Grande Instance). Tužiocima takođe prolaze posebne obuke za visokotehnoški kriminal radi specijalizacije za ovu oblast.

3. KRIVIČNO PRAVNI PROPISI I VISOKOTEHNOŠKI KRIMINAL U REPUBLICI FRANCUSKOJ

Francuski zakoni se konstantno prilagođavaju savremenoj praksi vezanoj za visokotehnoški kriminal. Obaveza čuvanja podataka od strane Internet provajdera u roku od godinu dana u Republici Francuskoj uvedena je zbog toga što je čuvanje logova postalo gorući problem, posebno kada se uzme u obzir porast broja otvorenih pristupa Internet mreži. Napredna rešenja u zakonodavstvu vezana za daljinski pristup podacima od strane sudije u slučajevima terorizma i organizovanog kriminala predstavljaju savremena administrativna rešenja vezana za efikasno sprovođenje zakona u ovoj oblasti.⁷

Republika Francuska je dana 23.11.2001. godine potpisala Konvenciju o visokotehnoškom kriminalu i ratifikovala je 10.01.2006. godine, sa dodatnim Protokolom o ksenofobiji i rasizmu. Pravni propisi su usklađeni sa ovom Konvencijom, a problematika visokotehnoškog kriminala je regulisana Krivičnim zakonikom (Code Penal), Zakonom o intelektualnoj svojini (Code de la Propriete Intellectuelle) i Zakonikom o krivičnom postupku (Code de Procedure Penal).

Krivični zakonik Republike Francuske u oblasti zaštite automatske obrade podataka u članu 323 stav 1 (tekst se nalazi u zakonu pod nazivom Loi Godfrain od 05.1.1998. godine) inkriminiše radnje menjanje i brisanje računarskih podataka, a zaprećena je kazna do jedne godine zatvora i novčana kazna u iznosu do 15.000 eura. Uništavanje

⁶ Ministère de la justice, direction des affaires criminelles et des grâces: Le traitement judiciaire de la cybercriminalité „Guide méthodologique“, France, 2002, p.23.

⁷ C. Aghroum: L'Europe, un atout pour la France dans la lutte contre la cybercriminalité, Cahiers de la sécurité No 6, l'Institut national des hautes études de sécurité, France, 2008, p.94.

podataka inkriminisano je u čl. 323-1 stav 2 a zaprećena je kazna zatvora do dve godine i novčana kazna do 30.000 eura. Ometanje funkcionisanja obrade podataka inkriminisano je u čl. 323-2 a propisana je kazna zatvora do tri godine i kazna do 45.000 eura. U čl. 323-3 inkriminiše se protivpravna prodaja podataka kaznom do tri godine zatvora i novčanom kaznom do 45.000 eura. Protivpravno umnožavanje podataka u čl. 323-4 sankcionisano je identičnom kaznom.

Pokušaj uticaja na sistem automatske obrade podataka u čl. 323-7 takođe je sankcionisan kaznom do tri godine zatvora. Unošenje štetnih podataka, skrivanje podataka, nuđenje na prodaju neovlašćeno prikupljenih podataka, pravljenje, prodaja i davanje na upotrebu programa i informatičke opreme za unošenje štetnih podataka i drugo, sankcionisani su u čl. 323-3-1 (u tekstu zakona LCEN od 9.IV 2004 član. 34). Zaprećena kazna za navedena krivična dela je do tri godine zatvora i novčana kazna do 45.000 eura.

U Krivičnom zakoniku štiti se takođe i automatska obrada ličnih podataka. Neodgovorno postupanje sa ličnim podacima sankcionisano je u čl. 226-16 a sankcija za navedeno krivično delo je do tri godine zatvora i novčana kazna do 45.000 eura. Tekst ovog člana nalazi se u zakonskom aktu pod nazivom „Loi Informatique et Libertés 06 I 1978“.

Neosiguravanje baze podataka je krivično delo predviđeno u čl. 226-17 a kazna koja je predviđena je do pet godina zatvora i novčana kazna od 300.000 eura. Identične kazne predviđene su i za prikupljanje podataka o konkurenciji (nelojalnu konkurenciju), koje je inkriminisano u čl. 226-18, kao i za neovlašćeno prikupljanje poverljivih podataka, koje je inkriminisano u čl. 226-19.

Prikupljanje istorijskih, statističkih i naučnih podataka bez ovlašćenja od strane njihovih vlasnika kao krivično delo predviđeno je u čl. 226-20, sa zaprećenom sankcijom do tri godine zatvora i novčanom kaznom do 45.000 eura. Zloupotreba podataka u svrhe za koje nisu dati kao krivično delo regulisana je članom 226-21 sa kaznom zatvora do pet godina i novčanom kaznom do 300.000 eura. Prodaja ličnih podataka krivično delo je po čl. 226-22 a predviđena je kazna zatvora do jedne godine i novčana kazna do 15.000 eura. Javno objavljivanje ličnih podataka bez ovlašćenja, neobezbeđivanje poverljivih tehničkih podataka i fabrikovanje lažnih podataka je krivično delo predviđeno u zakonu

„Code des P&T“ u čl. L. 39-31, za koje je predviđena kazna zatvora do jedne godine i novčana kazna do 75.000 eura⁸.

Krivična dela vezana za zloupotrebu i falsifikovanje platnih kartica nalaze se u Zakonu o monetarnoj politici i finansijama (Code monétaire et Financier), u tekstu akta pod nazivom LSQ od 15 XI 2001, u članovima od 35 do 39 i u članu 40. Za ova krivična dela predviđena je kazna zatvora do sedam godina. Neovlašćena enkripcija podataka predviđena je kao krivično delo u Krivičnom zakoniku u čl. 434-15-2, a kazna koja je zaprećena iznosi do jedne godine zatvora i novčano do 45.000 eura.

Odbijanje predaje ključa za dekripciju (predaja šifre) predviđeno je kao kažnjivo u čl.11 Zakona o telekomunikacijama (L. Télécom 29. XII.1990. godina) sa modifikacijama od 10.07.1991. godine, za šta je zaprećena je kazna do dve godine zatvora. Odbijanje predaje šifre kojom se može izbeći ili ograničiti krivična istraga kao samostalno krivično delo predviđeno je članom 434-15-2 stav 2. Ukoliko se radi o pokušaju izbegavanja predaje šifre radi izbegavanja istrage zaprećena kazna je do 30 000 eura i pet godina zatvora, a u slučaju pokušaja ograničavanja istrage kazna je do 75.000 eura a i takođe pet godina zatvora.

Zloupotreba dece u pornografske svrhe u zakonskim propisima regulisana je u nekoliko članova. U članu 227-23 Krivičnog zakonika gledanje dečije pornografije i registracija u nameri pripavljanja sadržaja sa dečijom pornografijom predviđeno je kao delo koje se kažnjava kaznom od tri godine zatvora i 45.000 eura. Širenje pornografskog materijala putem mreže je kao krivično delo predviđeno u članu 227-23 stav 3 sa zaprećenom kaznom do pet godina zatvora i novčanom kaznom do 75.000 eura.

Posedovanje fotografija sa sadržinom dečije pornografije je kao krivično delo predviđeno 227-3 stav 4, a zaprećena kazna je takođe do pet godina zatvora i novčana kazna do 75.000 eura, Nasuprot tome, za organizovani kriminal u ovoj oblasti predviđena je kazna do 10 godina zatvora i do 500.000 eura novčane kazne. Krivično delo širenja pornografskih predstava u kojima učestvuju lica koja se predstavljaju kao maloletna regulisano je u čl. 227-4 Krivičnog zakonika, a za to je predviđena kazna do tri godine zatvora i novčano 75.000 eura.

⁸ Tekst ovog člana nalazi se u aktu pod nazivom LSQ 15 XI 2001 u čl. 29.

Krivična dela vezana za širenje rasne, verske i etničke mržnje i netrpeljivosti takođe su regulisana u Krivičnom zakoniku. U članovima 23 i 24 kao krivično delo predviđeno je podsticanje na izvršenje ovih krivičnih dela, a kazna je novčano do 45.000 eura i zatvorska kazna do pet godina zatvora. Negiranje ratnih zločina i pozivanje na terorizam predviđeno je u članu 24 u stavovima 3 i 4, a zaprećena je kazna istovetna kazna - do pet godina zatvora i novčana kazna do 45.000 eura.

Izazivanje rasne mržnje predviđeno je kao krivično delo u čl. 24 stav 6 Krivičnog zakonika sa predviđenom kaznom zatvora do jedne godine i novčanom kaznom do 45.000 eura. Izazivanje zločina protiv čovečnosti je predviđeno takođe u čl. 24 sa zaprećenom kaznom do jedne godine zatvora i 45.000 eura. Kleveta na osnovu rasnih razlika kao krivično delo nalazi se u članovima od 29 do 32, a uvreda na osnovu rasnih razlika u članovima od 29 do 33. Kazne za ova krivična dela kreću se do jedne godine zatvora i 45.000 eura novčano.

Krivična dela protiv ličnosti i dostojanstva takođe se nalaze u Krivičnom zakoniku. Krađa identiteta predviđena je kao krivično delo članom 434-23, a zaprećena kazna je do pet godina zatvora i 75.000 eura. Obične pretnje i pretnje smrću inkriminisane su članom 222-17, sa predviđenom kaznom od šest meseci do tri godine zatvora, kao i novčanom kaznom od 45.000 do 75.000 eura.

Iznošenje privatnih podataka o ličnosti je krivično delo po članu 226 u stavu 1 i 2 sa predviđenom kaznom do jedne godine zatvora i 45.000 eura novčano. Narušavanje ugleda je krivično delo po čl. 226-8 sa istovetno predviđenom kaznom. Nasuprot tome, kleveta je kao krivično delo predviđena u čl. 226-10 sa kaznom zatvora do pet godina i novčanom kaznom do 45.000 eura. Najzad, otkrivanje poslovne tajne je krivično delo po članu 226-13, a predviđena je kazna zatvora do jedne godine i novčana kazna do 45.000 eura.

Krivična dela protiv imovine takođe se sadrže u Krivičnom zakoniku, a najznačajnije krivično delo za visokotehnološki kriminal predstavlja pretnja oštećenjem ili uništenjem imovine, koje se nalazi u čl. 322-12, sa predviđenom kaznom do 6 meseci zatvora i novčanom kaznom do 7.500 eura. Krivična dela vezana za prevare sa platnim karticama inkriminisana su u čl. 313-1, kao prevare vezane za korišćenje lažnih platnih kartica i plaćanja na Internetu, a zaprećene kazne za takve aktivnosti iznose do pet godina zatvora i 350.000 eura.

U francuskom Zakonu o zaštiti intelektualne svojine sadrže se krivična dela vezana za zaštitu intelektualne svojine u koje spadaju različiti programi, žigovi, dizajn i sl. Takođe je dodatno sankcionisano i ponavljanje (izvršenje u povratu) krivičnih dela iz ove oblasti, kao i kvalifikovan oblik ukoliko počinitelj krivičnog dela koristi neki specifičan poslovni ili privatni odnos sa žrtvom. Ova krivična dela nalaze se u članovima 335-1, 335-2 i 335-3, zatim u članu 716-9, i u članu 521-4. Za njih su zaprećene kazne do tri godine zatvora i novčane kazne do 300.000 eura. Članom 335-9 se predviđa sankcionisanje povratništva ili korišćenje specifičnog položaja ili odnosa koji počinitelj koristi, a kazne se u tom slučaju udvostručuju. Kazna za organizovane kriminalne grupe u ovoj oblasti je do pet godina zatvora i 375.000 eura.

Najzad, neovlašćeno organizovanje igara na sreću sankcionisano je članom 1 Zakona Paraben II sa modifikacijom broj 1 od 12.07.1983. godine, a predviđena je kazna do tri godine zatvora i novčana kazna do 45.000 eura. Za organizovane kriminalne grupe koje se bave izvršenjem ovih krivičnih dela kazna zatvora je sedam godina zatvora i novčana kazna do 100.000 eura. Reklamiranje neovlašćenih igara na sreću je takođe predviđeno kao krivično delo u čl. 23 navedenog zakona, a kazna je novčana i iznosi 4.500 eura.⁹

4. ZAKLJUČAK

Analiza strukture i organizacije državnih organa Republike Francuske u čijoj nadležnosti se nalazi sprečavanje i suzbijanje visokotehnološkog kriminala, kao i krivično-materijalnih propisa koji u Francuskoj regulišu ovu oblast, sama po sebi je značajna, pošto se radi o od državi u kojoj su začete ideje o slobodi, jednakostima i pravima čoveka i zemlji koja je u mnogo čemu „kolevka demokratije“.

Republika Francuska je danas država u kojoj se neguje ovo istorijsko nasleđe i istovremeno konstantno razvija savremeno društvo, a sprečavanje i suzbijanje visokotehnološkog kriminala i zaštita informacionog sistema u toj zemlji su regulisani uz puno uvažavanje ovih principa.

Struktura državnih organa koji se bave sprečavanjem visokotehnološkog kriminala ustanovljena je na sistematičan način i

⁹ T. Breton: Chantier sur la lutte contre la cybercriminalite, Ministère de l'intérieur, Paris 2005. p 22

pruža adekvatan okvir za uspešnu borbu protiv ovog fenomena na teritoriji Republike Francuske. Osim toga, uloga Republike Francuske i njenih državnih organa u borbi protiv ove vrste kriminala jasno je uočljiva i na međunarodnom planu.

Krivičnopravna regulativa takođe pruža efikasne okvire za sprečavanje ove pojave. Oštra kaznena politika koje se ogleda u visini zatvorskih kazni koje su zaprećene, kao i zaprećenim novčanim kaznama predstavlja i svojevrsan faktor odvraćanja od izvršenja krivičnih dela iz ove oblasti.

5. LITERATURA

1. C. Aghroum: L'Europe, un atout pour la France dans la lutte contre la cybercriminalité, Cahiers de la sécurité No 6, l'Institut national des hautes études de *sécurité*, France, 2008.
2. J. Baud, Encyclopédie du Renseignement et des Services Secetes, Lavauzelle, Paris, 1998.
3. T. Breton: Chantier sur la lute contre la cybercriminalite, Ministère de l'intérieur, Paris 2005.
4. Ministère de la justice, direction des affaires criminelles et des grâces: Le traitement judiciaire de la cybercriminalité „Guide méthodologique“, 2002.
5. Minister De L'Interieur, De L'Outre-Mer Et Des Collectivites Territoriales La lutte contre la cybercriminalité De L'Interieur, De L'Outre-Mer Et Des Collectivites Territoriales, France, 2009.
6. P.J. Stead, The Police of France, Macmillan Publishing Company, New York, 1983.
7. <http://www.securiteinfo.com/legal/OCLCTIC.shtml>, (06.01.2010. god.).
8. <http://www.internetworldstats.com/eu/fr.htm>, (06.01.2010. god.).
9. <http://www.gendarmerie.interieur.gouv.fr/fre/sites/Gendarmerie/Presentation/PJ/PJ/Cybercriminalite>, (06.01.2009. god.)

Prof. Milan Milošević, PhD
Vladimir Urošević, PhD

THE FIGHT AGAINST THE CYBER CRIME IN FRANCE

Republic of France is one of the most developed countries of the European Union. In the Republic of France 58.1% of the population used Internet by statistic data from march 2008. The number of users growing steadily since then. Fight against cyber crime was set as a priority in the years 2008 and 2009 by the Ministry of Internal Affairs of the Republic of France in order to preserve the information structure as the basis of modern information society. French laws are constantly adapting modern practices related to high-tech crime suppression. Structure of government bodies intended to fight against this phenomenon in France is an example of an effective system for combating cyber crime. Criminal legal regulations in the Republic of France provide an effective framework for preventing this criminal phenomenon. Harsh sentencing policies that are reflected in the amount of prison sentences, and high fines could be a kind of deterrent factor for crime prevention in this area.

Key words: *Republic of France, high-tech crime, misuse of information technology, misuse of data.*