

Andrej Diligenski

Dragan Prlja

FEJSBUK, ZAŠTITA PODATAKA I SUDSKA PRAKSA

INSTITUT ZA UPOREDNO PRAVO
INSTITUTE OF COMPARATIVE LAW

FEJSBUK, ZAŠTITA PODATAKA I SUDSKA PRAKSA
THE FACEBOOK, DATA PROTECTION AND CASE LAW

Izavač *Published by*
Institut za uporedno pravo
Beograd, Terazije 41
Institute of Comparative Law
Belgrade, Terazije Street 41

Za izdavača *For the Publisher*
Vladimir Čolović
Vladimir Čolović

Recenzenti *Reviewed by*
dr Gordana Gasmi
dr Mario Reljanović
dr Miodrag Savović
Gordana Gasmi Ph. D.
Mario Reljanović Ph. D.
Miodrag Savović Ph. D.

ISBN 978-86-80186-28-3
ISBN 978-86-80186-28-3

Priprema i štampa: *Prepress and Printing:*
Dosije studio, Beograd
Dosije studio, Belgrade

Tiraž: *Copies*
500
500

© INSTITUT ZA UPOREDNO
PRAVO, 2018

© INSTITUTE OF COMPARATIVE
LAW, 2018

Andrej Diligenski
Dragan Prlja

FEJSBUK, ZAŠTITA PODATAKA
I SUDSKA PRAKSA

Institut za uporedno pravo
Beograd, 2018

SADRŽAJ

1. UVOD.....	9
2. FEJSBUK I USAGLAŠENOST SA EVROPSKIM PRAVOM	13
2.1. Uvod	13
2.2. Tužbe protiv Fejsbuka	14
2.2.1. Sakupljanje podataka uz pomoć kolačića i lajk dugme.....	14
2.2.2. Korišćenje podataka bez unapred date saglasnosti „Opt-Out“ ..	17
2.2.3. Prepoznavanje lica	18
2.2.4. Tagovanje	20
2.2.5. Prevelika količina podataka	21
2.2.6. Slike korisnika	24
2.2.7. Friend Finder opcija	25
2.2.8. Politika privatnosti Fejsbuka	27
2.2.9. Aplikacije.....	29
2.3. Postupak u Irskoj protiv Fejsbuka	31
2.4. Postupak u Austriji protiv Fejsbuka	33
3. FEJSBUK I ZAŠTITA PODATAKA	37
3.1. Uvod	37
3.2. Zaštita privatnosti	37
3.3. Razvoj zaštite podataka	39
3.4. Zaštita podataka i pravo EU	40
3.5. Opšta uredba EU o zaštiti podataka	41
3.5.1. Nove kategorije podataka	43
3.5.2. Prava pojedinaca	43
3.5.3. Odgovornost firmi.....	46
3.5.4. Kazne	50
3.5.5. Budućnost i ocene Opšte uredbе o zaštiti podataka.....	53
3.6. Problemi zaštite podataka na Fejsbuku	55
3.6.1. Prikupljanje podataka prilikom registracije	55
3.6.2. Saglasnost korisnika da se njihovi podaci obrađuju	55

3.6.3. Predlozi prijatelja	56
3.6.4. Vidljivost podataka	57
3.6.5. Korišćenje podataka u reklamne svrhe	57
3.6.6. Prikupljanje podataka na osnovu Social Plugin	59
3.6.7. Brisanje profila	61
3.6.8. Mogućnost preuzimanja podataka	62
3.6.9. Skeniranje lica, korišćenje opasnih aplikacija	62
4. SUDSKA NADLEŽNOST I FEJSBUK	65
4.1. Uvod	65
4.2. Međunarodno-privatnopravni odnos sa Fejsbukom	65
4.3. Javnopravni odnos sa Fejsbukom	67
4.4. Međunarodni ugovorni odnos sa Fejsbukom	68
4.4.1. Safe Harbour	68
4.4.2. Tužba zbog afere PRIZMA i uticaj na sporazum Safe Harbour	72
4.4.3. Presuda Evropskog suda slučaj Safe Harbour	74
4.4.4. Privacy Shield	76
5. FEJSBUK I SUDSKA PRAKSA	79
5.1. Fejsbuk zaštita prava ličnosti i autorskih prava	79
5.2. Fejsbuk i zaštita konkurencije	84
5.3. Koordinisane akcije institucija za zaštitu podataka protiv Fejsbuka	93
5.4. Dobijanje otkaza zbog Fejsbuka	100
5.5. Objavljivanje statusa na Fejsbuku	104
5.6. Žurke i pozivi na veselja	110
5.7. Cenzura na Fejsbuku zbog slike Gustava Kurbea „Poreklo sveta“	112
5.8. Zaplena Fejsbuk profila	114
5.9. Fejsbuk kao sredstvo za istražne radnje	115
6. FEJSBUK I NEUTRALNOST INTERNET MREŽE	119
6.1. Ljudska prava	119
6.2. Edvard Snouden i afera “PRIZMA”	127
6.3. Ostali aspekti mešanja država u neutralnost internet mreže	135
7. ZAKLJUČAK	139
8. LITERATURA	143

Zbog čega je ništa a ne nešto?

Svet u kome živimo se pretvara u jednu fikciju u virtuelnu realnost. To je stvarnost u kojoj više ne odlučujemo. Svet u kome živimo tone u banalitet u beznačajnost. Moglo bi se reći da je današnje doba carstvo beznačajnosti! Ako je ovaj svet u kome živimo jedno ništa, banalnost jedna beznačajnost, onda on to može biti jedino ako smo okrenuli leđa svetosti, ako smo obesvetili stvarnost, ako smo desakranizovali stvarnost, ako smo zaboravili transcendenciju. Jedino okretanjem lica svetosti mi dolazimo iz ništa u nešto! Taj prelaz iz ništa je stvar naše slobode! Sloboda izvire iz bezdna tog ništa. Kad bismo se pitali o krajnjem utemeljenju te naše slobode, ne bismo mogli da ga nademo. U tome je ta čudesna moć ljudske prirode blagodareći božanskoj ličnosti, da iz ništa pređe u nešto. Naša je dužnost da uvažimo svetost, da se pridržimo za transcendenciju i da snagom svoje ličnosti, svoje slobode, svoje odluke u svakoj životnoj situaciji iz ništa pređemo u nešto!

Prof. Bogoljub Šijaković

1. UVOD

Fejsbuk je počeo sa radom 4. februara 2004. godine, a danas ga koristi više od dve milijarde ljudi na planeti. Prema podacima iz februara 2017. godine Fejsbuk ima oko milijardu i 86 miliona aktivnih korisnika. Prihodi Fejsbuka rastu iz godine u godinu enormno i za godinu 2016 iznose nešto oko 26,89 milijarde dolara (oko 22,51 milijarde evra), dok je ostvarena neto dobit oko 10,22 milijarde dolara (oko 8,56 milijarde evra). Ideja nekoliko studenata Harvarda o onlajn zajednici prijatelja sa fotografijama i profilima koje oni sami postavljaju, odnosno ideja o stvaranju interaktivne virtuelne zajednice paralelne sa društvenim zajednicama koje postoje u stvarnom svetu danas je postala realnost.¹

Fejsbuk je danas društvena mreža, pomoću koje milioni ljudi komuniciraju širom planete. Pored toga ova platforma je postala moćno sredstvo pomoću kojeg se ogroman broj podataka, slika, filmova i drugih materijala razmenjuje, postavljajući na profile i čini javno dostupnim. Ova društvena mreža je pored komunikacije između korisnika tzv. „prijatelja“ omogućila i doprinela mnogim firmama da se reklamiraju, a zbog velikog broja korisnika postala i moćno marketinško sredstvo. Fejsbukov model poslovanja sastoji se u prikupljanju informacija o korisnicima i prodaje podataka oglašivačima.²

Fejsbuk svojim korisnicima prilikom registracije i pristupa na ovu društvenu mrežu poručuje da je korišćenje besplatno, i da će ostati besplatno. Međutim, ako se zarada ostvaruje, a korisnici ne plaćaju, logičan zaključak je da oni nisu mušterije. Oni su, naime — roba.³ Štaviše, informacije koje Fejsbuk dobija od korisnika postaju vlasništvo Fejsbuka, koji njima može da trguje i ostvaruje dobit. Kada je korisnik ulogovan, na njegovom računaru mu izlaze reklame proizvoda tzv. „baneri“ za koje je pokazao interesovanje. Time je ovakvo oglašavanje efikasnije nego u drugim medijima.

Uzimajući u obzir korisnike Fejsbuka sa prostora Evropske unije, treba imati u vidu da udeo od 23 % od ukupnog broja Fejsbuk korisnika čine korisnici iz EU.⁴

1 Ben Mezrih, *Slučajni milijarder: nastajanje Fejsbuka*, Beograd: Evro-Giunti, 2010, str. 72.

2 Randi Zackerberg direktorka odeljenja za marketing Fejsbuka, a inače sestra Mark Zackerberga, izjavila je da se rešenje za Cyber-Bullying (sajber maltretiranje) mora postići na taj način što će korisnici online morati da upotrebljavaju svoja prava imena. „Anonimnost na internetu mora da nestane“ poručuje ona. Takođe je dodala da se „ljudi kriju iza anonimnosti i onda misle, da oni mogu iza zatvorenih vrata da sve urade i kažu“. Prosto rečeno ljudi treba da zaborave na privatnost u internet svetu. Za internet više ne sme biti tajni, pošto se time štiti viši interes, navodno interes „internet sigurnosti“. Datenschutz– Facebook: „Online-Anonymität muss weg“, futurezone, futurzone.at, <http://futurezone.at/digitallife/4262-facebook-online-anonymitaet-muss-weg.php>, 7. 8. 2012.

3 D. Milojković, *Fejsbuk uzima milijarde za podatke korisnika*, Blic, <http://www.blic.rs/IT/305305/Fejsbuk-uzima-milijarde-za-podatke-korisnika>, 7. 8. 2012.

4 Internet World Stats, *Internet Stats and Facebook Usage in Europe March 2017 Statistics*, <http://www.internetworldstats.com/stats4.htm>, 10. 9. 2017.

Prema nekim procenama na nivou EU ima oko 450 miliona korisnika. Zbog svega toga i velikog broja korisnika potrebno je ukazati na aspekte pravne zaštite u EU i ukazati na saglasnost sa propisima EU.

Najviše pravnih problema na Fejsbuku vezano je za pravo privatnosti, zaštitu podataka kao i mogućnost ostvarivanja prava na pravnu zaštitu. Ova pitanja regulisana su propisima EU i to pre svega Direktivom o zaštiti podataka (Directive 95/46/EC),⁵ Direktivom o privatnosti i elektronskim komunikacijama (Directive 2002/58/EC),⁶ Direktivom kojom se menja Direktiva o privatnosti i elektronskim komunikacijama (Directive 2006/24/EC),⁷ Direktivom kojom se takođe menja Direktiva o privatnosti i elektronskim komunikacijama (Directive 2009/136/EC),⁸ i Telekom paket Direktivom (Directive 2009/140/EC).⁹ Kao što se može primetiti, jedna od najvažijih direktiva je doneta još 1995. godine. I pored toga ova direktiva je ostala kamen temeljac u razvitku daljih pravnih propisa EU u oblasti zaštite podataka i prava privatnosti, pre svega zato što je dugogodišnja sudska praksa bazirana na ovoj direktivi.¹⁰ Ostale direktive predstavljaju nadogradnju kako bi se omogućila primena ovih direktiva u oblasti elektronskih komunikacija. Direktiva iz 1995. godine poslužila je kao baza za novu Opštu uredbu o zaštiti podataka (Regulation 2016/679), koja počinje da se primenjuje 25.5.2018. godine.¹¹

- 5 *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L 281, 23/11/1995.
- 6 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, Official Journal L 201, 31/07/2002.
- 7 *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, Official Journal L 105, 13/04/2006.
- 8 *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws*, Official Journal L 337, 18/12/2009.
- 9 *Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services*, Official Journal L 337, 18/12/2009.
- 10 Nataša Tomić, Dalibor Petrović, *Društveno umrežavanje i zaštita privatnosti korisnika interneta*, Saobraćajni fakultet Univerziteta u Beogradu, XXVII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju — PosTel 2009, Beograd, 15. i 16. decembar 2009. <http://postel.sf.bg.ac.rs/downloads/simpozijumi/POSTEL2009/RADOVI%20PDF/Menadzment%20procesa%20u%20postanskom%20i%20telekomunikacionom%20saobraćaju/9.%20N.%20Tomic,%20D.%20Petrovic.pdf>, 7. 8. 2012, strana 97.
- 11 *Regulation 2016/679 of the European Parliament and of the Council of 7 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, OJ L 119, 4. 5. 2016, p. 1–88.

Kako ispravno zaključuje Džulijan Asanž najmoćnije sredstvo za kontrolu i nadgledanje pojedinaca danas je internet.¹² Kada privatna kompanija uz pomoć interneta poseduje milijarde podataka i informacija među kojima su i one o političkom ubeđenju, seksualnoj orijentaciji, kretanju u digitalnom svetu, imovinskom stanju, obrazovanju, zdravstvenim problemima, profesionalnom angažovanju pojedinaca, onda mnogi počinju da se pitaju kako da se pojedinac odbrani od nadzora i kontrole koja se vrši nad njegovom privatnošću. Ovo pitanje iz dana u dan dobija sve više na važnosti i u bitnoj meri određuje slobode pojedinca, koje su očigledno danas ugrožene. Jedan od važnih koraka u odgovoru na pitanje kako se boriti za svoje pravo privatnosti svakako je razmatranje brojnih pravnih aspekata ugrožavanja privatnosti pojedinaca koji proističu iz korišćenja jedne od najvećih društvenih mreža danas Fejsbuka.

Niz primera iz prakse i sudskih presuda nastalih kao posledica korišćenja Fejsbuka, koje smo naveli u ovoj knjizi treba da predstavljaju ozbiljno upozorenje svim korsinicima ove društvene mreže sa ciljem da budu znatno oprezniji pri korišćenju ove društvene mreže, odnosno da budu svesni kakve sve posledice mogu izazvati njihove aktivnosti na Fejsbuku.

Naša knjiga predstavlja mali, ali vrlo važan korak u sagledavanju realnosti u kojoj se trenutno nalazimo, kada su u pitanju pravo zaštite podataka, pravo privatnosti, pravo na slobodu mišljenja i izražavanja, sloboda interneta kao medija, sloboda okupljanja kao i ugroženost ovih prava od strane država, internet servis provajdera i društvenih mreža poput Fejsbuka.

Autori

12 Ben Mezrih, *Slučajni milijarder: nastajanje Fejsbuka*, Beograd: Evro-Giunti, 2010, str. 174.

2. FEJSBUK I USAGLAŠENOST SA EVROPSKIM PRAVOM

2.1. Uvod

Austrijska grupa „Europe versus Facebook“ je još 18. avgusta 2011. godine na čelu sa tada studentom prava Maksom Šremsom podnela 22 tužbe protiv Fejsbuka u Dablinu zbog kršenja prava EU.¹³ Glavne tužbe su se odnosile na sakupljanje podataka uz pomoć kolačića i lajk dugmeta. Neposredni povod za ove tužbe bio je odgovor Fejsbuka na zahtev Maksa Šremsa, kojim je on tražio podatke od Fejsbuka, koje imaju o njemu. Rezultati su bili poražavajući — 1.222 stranice A4 formata ličnih podataka za period od 3 godine korišćenja ove društvene mreže.¹⁴ U ove podatke spadaju i specifične informacije o političkom opredeljenju, seksualnoj orijentaciji, učešću na demonstracijama. Ono što je ovom prilikom bilo upadljivo je da su informacije koje je student obrisao, ostale još uvek na Fejsbuku i nisu bile obrisane. U to spadaju obeležavanja na fotografijama, obrisane poruke i obrisani prijatelji, bockanja (eng. „pokes“), i promenjena imena korisnika. Pored toga su i unosi na zidu bili samo delimično obrisani, naravno one koje je student dobio.¹⁵ Pošto Fejsbuk nije dao sve podatke, na ponovni zahtev studenta, dostavljeno je obrazloženje da ostali podaci predstavljaju „poslovnu tajnu“. Sada Fejsbuk svima koji traže podatke koje Fejsbuk čuva o njima, saopštava da se podaci mogu onlajn preuzeti.¹⁶ Glavni problem je u tome, što onlajn stoje isključivo podaci koje korisnici mogu i sami videti na ovoj platformi, nema skrivenih podataka.¹⁷ To su informacije o tzv. lajk dugmetu, veb sajtovima koje je Maks posetio, a sadrže ovu opciju. Ovde spadaju i informacije o log fajlovima (podaci o kompjuteru sa kog se korisnik ulogovao na ovu društvenu mrežu) i o geografskoj lokaciji korisnika.¹⁸ U Fejsbukovoj politici

13 Barbara Wimmer, futurzone.at, *Facebook verarscht uns alle*, <http://futurezone.at/netzpolitik/5644-facebook-verarscht-uns-alle.php>, 7. 8. 2012.

14 ZDF — heute 12 Uhr, 25. 1. 2012 — Datenschutz Facebook, http://www.youtube.com/watch?v=922_CImwPvU&feature=BFa&list=PLAA5F774719E9F911&lf=plcp, 7. 8. 2012.

15 Datenschutz: *Wiener Studenten klagen gegen Facebook*, derStandard.at, <http://derstandard.at/1313024892837/Anzeigen-Datenschutz-Wiener-Studenten-klagen-gegen-Facebook>, 7. 8. 2012.

16 Nakon Maksovog zahteva podneto je oko 40.000 identičnih zahteva Fejsbuku. Korisnici su upućivani na to da mogu preuzeti podatke o sebi, međutim do sada nisu dobili sve kategorije podataka. Dobili su upola manje podataka o sebi nego austrijski student. <http://www.europe-v-facebook.org/DE/de.html>, .europe-v-facebook.org, 7. 8. 2012.

17 Fejsbuk čuva podatke na način kao i običan kompjuter. Naime, kada se određeni sadržaj izbriše, on zapravo nije obrisano nego je kao u slučaju na kompjuteru prebačen u neku korpu „Recycle Bin“. Odatle se mogu iznova ovi sadržaji ponovo uspostaviti i videti. ORF eins — direkt — Facebook & Co, youtube, <http://www.youtube.com/watch?v=In-ig9KKHec&feature=autoplay&list=PLAA5F774719E9F911&lf=plcp&playnext=1>, 7. 8. 2012.

18 Ö1 — Digital. Leben — *Auskunftsersuchen bei Facebook*, youtube, <http://www.youtube.com/watch?v=KG48oXUUh4&feature=autoplay&list=PLAA5F774719E9F911&lf=plcp&playnext=2>, 7. 8. 2012.

o privatnosti stoji da se i informacije o lajk dugmetu snimaju.¹⁹ Osim toga stoji i to da bi Fejsbuk trebalo da ove informacije pruži korisnicima u roku od 40 dana. Ova poslednja odredba je prekršena, pošto Fejsbuk odmah upućuje korisnike da mogu onlajn pogledati svoje podatke i preuzeti ih.²⁰ Ovi podaci su podstakli Maksa da podrobnije istraži pravne probleme Fejsbuka i podnese 22 tužbe.

U ovom poglavlju biće razmatrane tužbe Maksa Šremsa i njegove organizacije „Europe versus Facebook“ protiv Fejsbuka i sam tok postupka pred sudovima u Irskoj i Austriji kao i saglasnost sa još uvek važećom Direktivom o zaštiti podataka iz 1995. godine.

2.2. Tužbe protiv Fejsbuka

2.2.1. Sakupljanje podataka uz pomoć kolačića i lajk dugme

Fejsbuk sakuplja informacije o aktivnosti njegovih korisnika, u tome se ova platforma ne razlikuje od ostalih društvenih mreža. Podaci se sakupljaju na osnovu „kolačića“ (eng. cookies).²¹ *Behavioural Advertising* označava posebnu vrstu reklamiranja na internetu, kojim se surfovanje korisnika posmatra da bi se korisnicima pokazao određeni reklamni materijal uz pomoć banera. U zavisnosti od toga na koji reklamni sadržaj se klikne, vrši se grupacija i kategorizacija korisnika u posebne grupe na osnovu njihovih interesovanja i na taj način se dobijaju reklame.

Sa stanovišta zaštite podataka je ovo problematično, pošto se prati internet surfovanje odnosno saobraćaj i na taj način pravi detaljno profilisanje internet korisnika (u ovom slučaju Fejsbuk korisnika). Za ovo praćenje ponašanja korisnika koriste se gore napomenuti „kolačići“.

Srbin koji živi u Australiji Nikola Nik Čubrilović je otkrio da Fejsbuk na ovaj način špijunira korisnike. Fejsbuk je potvrdio njegovu tvrdnju da ne briše „kolačiće“, koji sa Fejsbuka šalju podatke na računar korisnika i obrnuto, kako bi se dobile informacije o imenu korisnika, lozinki, ali i drugim podacima npr. o tome koje sajtove korisnik posećuje.²² Kad se korisnici odjave sa Fejsbuka, on i dalje prati

19 Ono što je takođe zanimljivo je da se korisnici ove društvene mreže moraju složiti sa politikom privatnosti Fejsbuka. Međutim, mali broj korisnika i pročita ove odredbe, pošto se radi o 12 strana, koji su međusobno isprepletane na taj način što ima puno upućivanja sa jedne na drugu stranu. Time ove odredbe predstavljaju veliku enigmu za najveći broj korisnika ove društvene mreže. *Datenschutz: Wiener Studenten klagen gegen Facebook*, derStandard.at, <http://derstandard.at/1313024892837/Anzeigen-Datenschutz-Wiener-Studenten-klagen-gegen-Facebook>, 7. 8. 2012.

20 Barbara Wimmer, futurzone.at, *Facebook verarscht uns alle*, <http://futurezone.at/netzpolitik/5644-facebook-verarscht-uns-alle.php>, 7. 8. 2012.

21 Kolačići „Cookies“ su mali tekstualni fajlovi (mali podaci tzv. mrvice), koje veb sajt skladišti na računaru korisnika, da bi se po potrebi brzo i pouzdano ponovo prepoznali. Time su korisnici u mogućnosti da brže i pouzdanije pristupe nekom veb sajtu. *Zertifizierbarkeit von Online-Diensten zur Einblendung verhaltensbasierter Werbung („Behavioural Advertising“)*, EuroPriSe Europäisches Datenschutz-Gütesiegel, EuroPriSe beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein <https://www.datenschutzzentrum.de/europriSe/Factsheet-Behavioural-Targeting-2010826-de.pdf>, 7. 8. 2012.

22 „Ko je Srbin koji je razbio Fejsbuk?“, izvor: Kurir, sajt Vesti online, <http://www.vesti-online.com/Vesti/Srbija/168363/Ko-je-Srbin-koji-je-razbio-Fejsbuk/print>, 7. 8. 2012.

njihovo kretanje po sajtovima koji imaju dugme za podelu podataka s Fejsbukom („šer“ ili „lajk“ dugme). Fejsbuk tvrdi da oni ni na koji način ne zloupotrebljavaju ove podatke. Kao jedino rešenje stručnjaci vide u brisanju svakog Fejsbuk kolačića u browseru²³ ili korišćenje drugog browsera samo za Fejsbuk.²⁴

Lajk dugme (eng. like button) predstavlja društveni dodatak tzv. „Social-Plugin“.²⁵ Uz pomoć njega vlasnici veb sajtova preko svojih veb stranica se povezuju sa društvenim mrežama. Ukoliko lajk dugme postoji na njihovoj stranici, Fejsbuk registrovani korisnici mogu kliknuti na odgovarajući sadržaj, koji im se sviđa. Na ovaj način se na njihovom Fejsbuk profilu automatski javlja beleška o tome da se baš tom korisniku određeni sadržaj sviđa.²⁶ Informacije iz tzv. „Social Graph“ (ko šta voli) se snimaju na Fejsbuku. Jedan „Social Graph“ pokušava da rekonstruiše realne društvene odnose između ljudi na internetu.²⁷

Fejsbuk takođe može da koristi imena, slike profila svojih korisnika na bilo kojem proizvodu koji je lajkovan, jer tako stoji u njihovoj politici privatnosti.²⁸ Na početnoj strani Fejsbuk korisnika na reklami se može pojaviti i status korisnika, ukoliko je korisnik spomenuo određenu kompaniju.²⁹

Osim toga Fejsbuk je priznao da kada su korisnici prijavljeni (ulogovani), uzimaju podatke sa profila korisnika, ime, e-mail adresu, listu prijatelja i stvari koje su lajkovane, ali i IP adresu, podatke o rezoluciji ekrana, operativnom sistemu i browseru koji je korišćen. Vreme, datum i URL svake strane koja koristi Fejsbukove društvene dodatke (eng. plug-in) takođe se nalaze na ovoj listi.

- 23 Najpoznatiji internet browseri su Internet Explorer, Google Chrome, Mozilla. Korisnici browsera Mozilla mogu u podešavanjima isključiti opciju slanja kolačića trećim licima (u ovom slučaju Fejsbuku). Opcija se nalazi kada se u podešavanjima (tools), pa na opcije (options), zatim na privatnost (privacy), pa se onda pronađe prihvatanje kolačića I tu odabere opcija da se isključi trećim licima slanje kolačića. Cookies von Drittanbietern blockieren, Firefox-Hilfe, support.mozilla.org, <http://support.mozilla.org/de/kb/Cookies%20von%20Drittanbietern%20blockieren>, 7. 8. 2012. Das Like-Problem, Was Facebooks Gefällt-Mir-Buttons verraten, Jürgen Schmidt, heise Security, <http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html>, 7. 8. 2012.
- 24 „Oglašivači dobijali podatke korisnika“, sajt B92, http://www.b92.net/tehnopolis/vesti.php?yyyy=2010&mm=05&nav_id=432984, 7. 8. 2012.
- 25 Social Plugins, facebook developers, <http://developers.facebook.com/docs/plugins/>, 7. 8. 2012.
- 26 Googles Idee eines Social Graph für das gesamte Internet — und die Umsetzung durch Facebook, Andreas Köster, Wirtschaftskommunikation-Informationen, Texte und Dokumente aus dem Studium, <http://www.wirtschaftskommunikation-studium.de/2010/11/googles-idee-eines-social-graph-fur-das-gesamte-internet-%E2%80%93-und-die-umsetzung-durch-facebook/>, 7. 8. 2012.
- 27 Facebook Social Plugins und Datenschutzrecht, Rechtsanwalt Dr. Thomas Helbing, thomashebling.com, <http://www.thomashebling.com/de/facebook-social-plugins-datenschutz-bdsg-datenschutzhinweise-privacy-policy-like-button-gefällt-mir>, 7. 8. 2012.
- 28 I ne znajući, možete završiti u reklami na Facebook-u, invest. info, <http://www.itvesti.info/2011/03/i-ne-znajući-mozete-završiti-u-reklamama.html>, 7. 8. 2012.
- 29 Ovo se može isključiti tako što na svom profilu odaberete podešavanja naloga i odete na deo ‘Facebook oglasi’. Treba pronaći mogućnost „Dopusti da treća strana u svojim oglasima da prikazuje moje informacije“ i treba odabrati „Nikome“. Na istoj stranici se nalazi „Izmeni moja podešavanja u društvenim oglasima“ i treba odabrati „Nikome“. Tako ćete svoje statuse i fotografije zaštititi od nove ideje oglašivača. Međutim da li je u stvarnosti tako, veliko je pitanje. Facebook reklame, Reklame koje prikazuju treća lica, *Reklame i prijatelji*, <http://www.facebook.com/settings?tab=ads>, 7. 8. 2012.

Kada korisnici nisu ulogovani Fejsbuk poseduje podatke o jedinstvenom broju kolačića, sa kojim povezuje sve ostale podatke — IP adresu, rezoluciju ekrana, operativni sistem i browser koji koristite korisnici, kao i URL, datum i vreme posete strane sa Fejsbuk plug-inom.³⁰

Opravdanje za ovakav način prikupljanja podataka iz Fejsbuka nalaze u tome da se na ovaj način poboljšava sigurnost korisnika, smanjuju šanse da im neko drugi preotme Fejsbuk identitet i poboljšava iskustvo korisnika.

Iz Fejsbuka objašnjavaju da prilikom snimanja podataka treba praviti jasnu razliku između članova Fejsbuka kao i onih koji to nisu. Članovi su prihvatanjem ugovora sa Fejsbukom dali saglasnost za obradu njihovih podataka. Kod korisnika koji nisu članovi Fejsbuka postoji tehnički mehanizam uz pomoć kojeg se sve IP adrese čuvaju. Ovim korisnicima se ne šalju reklame i njihovi log fajlovi se posebno čuvaju. Fejsbuk kompanija „na ovaj način postupa da bi izbegla prevare, kao npr. stvaranje lažnih profila od strane korisnika“ ističu iz Fejsbuka.³¹

Korišćenje lajk dugmeta je dozvoljeno, samo ako je u saglasnosti sa evropskim relevantnim standardima o zaštiti podataka. U ovom slučaju dolazi do odgovarajuće primene člana 5 stav 3 *Direktive o privatnosti*. Međutim ovaj propis je u decembru 2009. godine putem nove *Telekom paket direktive* promenjen. Na osnovu do sada važećeg propisa iz Direktive o privatnosti je primena tzv. „Tracking-Cookies“ bila dozvoljena, samo ako bi korisnici bili na jasan i sveobuhvatan način informisani o tome da upotrebu mogu naknadno da isključe tzv. „Opt-Out“ princip. Sa stupanjem na snagu nove direktive (države članice EU su bile u obavezi da implementiraju direktivu u svoje zakonodavstvo do kraja maja 2011.) korišćenje „Tracking-Cookies“ u cilju Behavioural Advertising-a takođe je dozvoljeno, ali ako se korisnicima prilikom prvog postavljanja kolačića, dostave sve relevantne informacije poput npr. cilja i dužine obrade korisničkih profila. Neophodno je međutim, da se pribavi njihova predhodna saglasnost tzv. „Opt-In“ princip. Za dobijanje ovakvog vida saglasnosti moguće je primera radi upotrebiti jedan prozor koji bi o tome informisao korisnike tzv. „Pop-Up Window“. Transparentnost ovog ponašanja je takođe pooštrena tako što obuhvata pored informacija koje su ponudiodci dužni da pruže korisnicima i informacije o tome koji su tačno podaci o njima snimljeni.³²

Maks Šrems je u svojoj tužbi tvrdio da je povređen član 7 (a) *Direktive o zaštiti podataka*, pošto ne postoji specifična, nedvosmislena saglasnost od strane Fejsbuk korisnika za korišćenje ove mogućnosti. Podaci se prate, bez obzira da li je korisnik pristao i bez istaknute najave. Povređen je takođe i član 6 stav 1 (a) iste direktive, pošto korisnici nemaju dovoljno informacija u politici o privatnosti Fejsbuka i njihovi podaci se primaju i obrađuju, pre nego što oni imaju priliku da nešto protiv toga učine. Cilj snimanja, prosleđivanja i sigurnosti uz pomoć URL-a ili ostalih

30 *Koje podatke prikuplja Facebook*, sajt B92, http://www.b92.net/tehnopolis/vesti.php?yyyy=2011&mm=11&nav_id=558817, 7. 8. 2012.

31 Stefan Kreml, *Datenschützer und Facebook-Manager prallen im Bundestag aufeinander*, <http://www.heise.de/newsticker/meldung/Datenschuetzer-und-Facebook-Manager-prallen-im-Bundestag-aufeinander-1365988.html>, 7. 8. 2012.

32 *Zertifizierbarkeit von Online-Diensten zur Einblendung verhaltensbasierter Werbung („Behavioural Advertising“)*, EuroPriSe Europäisches Datenschutz — Gütesiegel, EuroPriSe beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, <https://www.datenschutzzentrum.de/europrise/Factsheet-Behavioural-Targeting-2010826-de.pdf>, 7. 8. 2012.

informacija o prijateljima na Fejsbuku je u potpunosti problematičan i nesrazmeran i time suprotan članu 6 stav 1 (b). Predviđeno je sakupljanje i snimanje podataka u trajanju od minimum 90 dana, što je neadekvatno i prekomerno i suprotno članu 6 stav 1 (c).³³ Član 17 stav 2 kao i članovima 25 i 26 *Direktive o zaštiti podataka* koji su na taj način prekršeni, pošto saglasnost i zaštita podataka nisu određeni na jednom odgovarajućem zaštitnom nivou od strane trećih zemalja (u slučaju Fejsbuka od strane SAD).³⁴

Upotreba „Tracking-Cookies“ bi bila dozvoljena, ukoliko bi korisnici o tome bili informisani. Takva varijanta „Opt-In“ principa bi bila neophodna, da bi se dobila potrebna saglasnost za korišćenje ovih kolačića. Fejsbuk ima ne samo obavezu informisanja prema svojim korisnicima nego takođe i korisnici mogu tražiti od ove društvene mreže informacije o snimljenim podacima, čime im se garantuje transparentnost i zaštita podataka.

2.2.2. Korišćenje podataka bez unapred date saglasnosti „Opt-Out“

Fejsbuk često tvrdi da su korisnici pristali na upotrebu i korišćenje njihovih podataka i da se oni ponašaju u skladu sa evropskim propisima, međutim činjenice govore drugačije. Korišćenjem „Opt-Out“ principa Fejsbuk od svojih korisnika:

- Ne dobija saglasnost. Pošto prilikom ućlanjenja korisnici pristaju na generalnu politiku privatnosti Fejsbuka, dok ne postoji poseban pristanak na specijalne opcije. To znači da ne postoji specifičan pristanak na određene opcije, koje Fejsbuk nudi svojim korisnicima;
- Prikuplja podatke, pre davanja mogućnosti da se korisnici o tome izjasne. To se ogleda prilikom registracije na Fejsbuku. Od korisnika se traži da unesu svoje lične podatke (ime, prezime, datum rođenja, e-mail adresu, pol).³⁵ Pored toga može se primetiti da korisnik nema ni jednu opciju, kojom može podesiti svoje informacije koje želi da podeli sa Fejsbukom. Ono što je zabrinjavajuće je i da politika privatnosti ne predstavlja sastavni deo registracije na ovu društvenu mrežu, već postoji samo jedan link na osnovu koga se korisnici mogu upoznati, kako se Fejsbuk ophodi sa njihovim podacima;
- Nudi podešavanja opcija, koje su na veoma niskom nivou zaštite. Većinu informacija može videti svako, pošto je profil nakon registracije potpuno otvoren tako da i internet pretraživači poput Gugla mogu ove podatke ubaciti u svoju bazu podataka;
- Nudi podešavanja, koja nisu lako izmenjiva. Na taj način je onemogućeno praktično starijim i ne toliko kompjuterski veštima korisnicima, da na jednostavan način promene podešavanja. Naročito treba imati u vidu da Fejsbuk skriva mogućnosti izmene transfera podataka u vezi sa već napo-

33 Maks Šrems, *Complaint against Facebook Ireland Ltd.* — 17 „Like Button“, Vienna, 19. 9. 2011, http://www.europe-v-facebook.org/Complaint_17_Like_Button.pdf, 7. 8. 2012.

34 *Spamming, Cookies, Logfiles und Location Based Service im TKG 2003*, Österreichische Juristen Zeitung, Manz Verlag.

35 Ovo se može videti pri samom pristupanju Fejsbuku na <http://www.facebook.com/>, 7. 8. 2012.

menutim funkcijama. U tom moru isprepletenih informacija i prebacivanja sa jednog na drugo mesto putem linkova, običnim korisnicima je onemogućeno da nađu podešavanja, koja bi im omogućila da opcije isključe.

Na taj način Šrems je u tužbi navo da se krši član 7 (a) *Direktive o zaštiti podataka*, pošto ne postoji konkretan, nedvosmislen pristanak korisnika, niti informacija o tome. Štaviše, Fejsbuk obeshrabruje korisnike, da podešavanjima promene koje informacije žele da podele sa ostalima. Zbog toga se i koristi „Opt-Out“ princip.

Osim toga korisnici ne dobijaju informacije na fer način, već ih samo jedna strana upućuje, što je suprotno članu 6 stav 1 (a) *Direktive o zaštiti podataka*.

Podešavanja bi trebala biti napravljena tako da od početka informacije mogu videti samo prijatelji korisnika, a ne svi Fejsbuk korisnici. Osim toga ovo bi trebalo da bude sastavni deo registracije korisnika.³⁶

2.2.3. Prepoznavanje lica

Ova Fejsbuk opcija omogućava prepoznavanje lica sa postavljenih fotografija i sugerisanje imena onih koji se na njima nalaze.³⁷ Ona funkcioniše kada korisnik ili njegov prijatelj postave nove fotografije, tada se uz pomoć softvera za prepoznavanje lica upoređuju nove fotografije sa starijim na kojima su korisnici već bili označeni, slične fotografije se grupišu i Fejsbuk predlaže ime prijatelja koji se na njima nalazi. Na taj način Fejsbuk ovom opcijom paraktično tera prijatelje korisnika da ih obeležavaju odnosno „taguju“.³⁸

Fejsbuk je saopštio da je opciju „Tag Suggestions“ uveo kako bi olakšao obeležavanje slika korisnika. Ukoliko neko ne želi da bude obeležen, ima mogućnost da ovu opciju isključi u odeljku podešavanja privatnosti „Privacy Settings“ tako što uđe na opciju „Timeline and Tagging“ a zatim na „Who sees tag suggestions when photos that look like you are uploaded?“ i tu izabere opciju „Niko“.³⁹ Kao što se primećuje, ovo predstavlja tzv. „Opt-Out“ princip, pošto se korisnicima ostavlja ovaj dug put da ovu mogućnost isključe. Naravno većina korisnika nema uopšte svest o tome, da Fejsbuk uz pomoć ove opcije koristi njihove podatke na ovaj način.

Ova mogućnost ne bi bila problematična, kada bi se ona Fejsbuk korisnicima aktivirala, kada oni to žele. Ovime bi došlo do jedne vrste pristanka korisnika da se njihovi podaci o ličnosti mogu obuhvatiti ovom softverskom metodom, a ne kao što je do sada bio slučaj da oni koji to ne žele moraju ovu funkciju naknadno da isključe.⁴⁰

36 Maks Šrems, *Complaint against Facebook Ireland Ltd.* — 16 „Opt-Out“, Vienna, 18. August 2011, http://www.europe-v-facebook.org/Complaint_16_Opt-Out.pdf, 7. 8. 2012.

37 *FB funkcija prepoznavanja lica i kod nas*, sajt B92, http://www.b92.net/tehnopolis/vesti.php?yyyy=2011&mm=06&nav_id=517499, 7. 8. 2012.

38 M. Vukelić, *Fejsbuk sam prepoznaje lica na fotografijama i potpisuje ih*, sajt Blica, <http://www.blic.rs/IT/258949/Fejsbuk-sam-prepoznaje-lica-na-fotografijama-i-potpisuje-ih>, 7. 8. 2012.

39 *Podešavanja privatnosti, Kontrolišite privatnost dok objavljujete*, Fejsbuk, <http://www.facebook.com/settings/?tab=privacy>, 7. 8. 2012.

40 Thomas Stadler, *Ist die Gesichtserkennung von Facebook datenschutzwidrig?*, Internet-Law Onlinerecht und Bürgerrechte 2.0., <http://www.internet-law.de/2011/06/ist-die-gesichtserkennung-von-facebook-datenschutzwidrig.html>, 7. 8. 2012.

Mnoge funkcije i aplikacije sakupljaju podatke o korisnicima, ali sakupljanje biometrijskih podataka u ovakvom obimu predstavlja jednu specifičnost ove opcije.

Tako je Maks Šrems u svojoj tužbi po ovom pitanju tvrdio da ne postoji konkretan, nedvosmislen i izričit pristanak korisnika na prepoznavanje lica, kao ni informacija o tome. Funkcija se automatski aktivira i biometrijski podaci sakupljaju bez unapred date saglasnosti korisnika. Stoga obrada podataka Fejsbuk korisnika nije u saglasnosti sa članom 7 (a) *Direktive o zaštiti podataka*.

Prikupljanje biometrijskih podataka od preko milijardu korisnika predstavlja prekomerno sredstvo u odnosu na svrhu koja se postiže. Time je povećan rizik mogućnosti zloupotrebe kao i čuvanje ovolikog broja podataka, što predstavlja povredu člana 6 stav 1 (c) *Direktive o zaštiti podataka*.

Ne postoji adekvatna transparentnost u postupcima Fejsbuka i upozorenje korisnicima. Ovo predstavlja kršenje principa pravičnosti iz člana 6 stav 1 (a) *Direktive o zaštiti podataka*.

Takođe nema adekvatne informacije u politici o privatnosti Fejsbuka, o tome na koji način se ova mogućnost odvija što predstavlja kršenje člana 10 *Direktive o zaštiti podataka*.

Osim toga postoji i povreda člana 6 stav 1 (b) *Direktive o zaštiti podataka* pošto ne postoji legitimna svrha za održavanje biometrijskih podataka, nakon toga što korisnici deaktiviraju ovu funkciju. To dalje znači da je svrha svake dalje obrade biometrijskih podataka korisnika od stane Fejsbuka prekomerna i nepotreba i predstavlja povredu člana 6 stav 1 (c) *Direktive o zaštiti podataka*.⁴¹

Grupa EPIC (Electronic Privacy Information Center) podnela je žalbu zbog softvera za automatsko prepoznavanje lica, koji koristi Fejsbuk pred Federalnom trgovinskom komisijom SAD. Od ove institucije se zahteva da istraži opciju prepoznavanja lica i zahteva strože standarde za zaštitu privatnosti. Osim toga ne postoji predhodna saglasnost korisnika za korišćenje ove opcije, već „Opt-out“ princip. Opcija je uvedena bez znanja i saglasnosti korisnika o potencijalnim rizicima, koji prate ovu opciju. Takva praksa je nepravična i dovodi u zabludu korisnike, te bi stoga ovu opciju trebalo posebno ispitati, stoji u žalbi grupe EPIC.⁴²

Nadležne institucije za zaštitu podataka nemačkih pokrajina Šlesvig-Holštajn i Hamburg su zatražile od Fejsbuka da se prepoznavanje lica aktivira samo za lica koja žele da korise ovu opciju. Osim toga oni ne žele da se biometrijski podaci potrebni za prepoznavanje lica šalju u centralu Fejsbuka u SAD. Zbog prevelike količine biometrijskih podataka koji se automatski obrađuju postoji samim tim i povećana mogućnost zloupotrebe.

Slikanjem putem mobilnog telefona na ulici moguće je prepoznavanje ljudi na ulici, ukoliko su korisnici Fejsbuka. Takođe i mogućnost deaktivacije ove opcije predstavlja problem, što bi trebalo učiniti lakšim i bržim nego što je to do sada bio slučaj.

41 Maks Šrems, *Complaint against Facebook Ireland Ltd. — 09 „Face Recognition“*, Vienna, 18. August 2011, http://www.europe-v-facebook.org/Complaint_09_Face_Recognition.pdf, 7. 8. 2012.

42 *Beschwerde wegen Facebook-Gesichtserkennung*, portal futurzone.at, <http://futurezone.at/netzpolitik/3546-beschwerde-wegen-facebook-gesichtserkennung.php>, 7. 8. 2012.

Potrebno je povećati nivo svesti kod samih Fejsbuk korisnika, pošto su oni ti koji ubacuju njihove fotografije na Fejsbuk servere.⁴³

Istraživač sa univerziteta Karnegi Melon napravio je bazu podataka sa oko 25.000 fotografija od Fejsbuk profila studenata. Onda je na jedan sto postavio veb kameru i zamolio dobrovoljce da pogledaju u kameru. Tako je softver za prepoznavanje lica indentifikovao 31% studenata.⁴⁴

Potom je napravljen još jedan eksperiment na osnovu koga je upoređeno oko 280.000 Fejsbuk profila sa 6.000 profila sa drugih veb lokacija koja služe za upoznavanje. Softver je prepoznao lica u 40% slučajeva, a uspeo je i da identifikuje jednog od deset članova veb lokacija za upoznavanje i pored toga što su skoro svi koristili pseudonime.

U politici o privatnosti lokacije Fejsbuka se navodi da opcija za podešavanje privatnosti korisničkog imena i slike profila ne postoji. Sve ovo donosi ogromne rizike po privatnost Fejsbuk korisnika, pošto se uz pomoć softvera za prepoznavanje lica uz vezu sa bazom podataka koja sadrži imena, lične informacije, može izgubiti osećaj anonimnosti i privatnosti na javnom mestu.

Ono što zabrinjava u ovom slučaju je da ukoliko istraživači mogu sačiniti ova-ko veliku bazu podataka, pitanje anonimnosti i privatnosti kod policijskih službi uz pomoć fotografija za pasoše i lične karte ostavlja više mogućnosti za narušavanje ovih prava. Ogromna baza podataka sa Fejsbuk profila se može iskoristiti za identifikaciju korisnika, dok npr. šetaju ulicom.⁴⁵

2.2.4. Tagovanje

Obeležavanje (eng. tagging) predstavlja opciju koju Fejsbuk daje korisnicima, da taguju odnosno obeleže u fotografijama drugog korisnika tj. prijatelja. Time ova fotografija biva uočljivija za korisnikove prijatelje. Kada se prijatelji taguju na određenoj slici, Fejsbuk to prenosi na početnu stranu kao udarnu vest i svi prijatelji će moći to da vide. Korisnici ne mogu sprečiti prijatelje da ih taguju, osim ako nemaju prijatelja. Praktično to znači da se fotografije najpre objavljuju, a pritom da svi korisnici kojima je inače dozvoljeno da vide fotografiju mogu to učiniti, tek tada obeleženi korisnik ima mogućnost da svoju oznaku ukloni. Cilj jedne ovakve funkcije je da korisnik tek kasnije može da odreaguje. Time je ovo označavanje korisnika već postalo vidljivo za većinu korisnika, pa samim time uklanjanje oznake predstavlja besmislen radnju, pošto su ostali korisnici već imali priliku da fotografiju vide.

Tag je u potpunosti aktiviran, čak iako o tome Fejsbuk korisnici nisu obavesteni. Ne postoji funkcija koja sprečava tagovanje. Samo se naknadno može uklo-

43 *Nemačka protiv Facebooka*, izvor: Deutsche Welle, sajt B92, http://www.b92.net/tehnopolis/aktuelno.php?nav_id=552305&fs=1, 7. 8. 2012.

44 Istraživači sa ovog univerziteta su napravili i aplikaciju za iPhone koja može fotografisati nečije lice i identifikovati tu osobu uz pomoć softvera za prepoznavanje lica, navodeći ime i osnovne informacije te osobe. *Prepoznavanje lica na osnovu Facebook profila*, izvor: www.mikro.rs, itvesti.info, <http://www.itvesti.info/2011/08/prepoznavanje-lica-na-osnovu-facebook.html>, 7. 8. 2012.

45 *Prepoznavanje lica na osnovu Facebook profila*, izvor: www.mikro.rs, itvesti.info, <http://www.itvesti.info/2011/08/prepoznavanje-lica-na-osnovu-facebook.html>, 7. 8. 2012.

niti oznaka, ali čim ona već postoji, praktično je nemoguće ukloniti je. Ukoliko se ukloni tag, on nije izbrisan, nego je samo deaktiviran. Oznaka se može pronaći na profilu prijatelja, koji je tag i napravio. Pritom na profilu korisnika, koji je želeo da ukloni svoje obeležavanje stoji da je obeležavanje svoje slike obrisao. Praktično je korisnik koji je obeležen samo uklonio link ka svom profilu, ali ne i svoj identitet.

Dešava se u praksi da su korisnici označeni pijani, goli, kako varaju svog partnera, ili u bilo kojoj drugoj problematičnoj situaciji. Ovakva slika se distribuira svim prijateljima korisnika koji je tagovan. Ukoliko se koristi standardna postavka Fejsbuka, to znači da praktično svi korisnici interneta imaju mogućnost da vide ove slike. Korisnici imaju mogućnost da naknadno uklone sebe sa tagovane fotografije, ali pošto se sve već desilo („Opt-Out“ princip). Nedavno je Fejsbuk uveo dodatnu mogućnost korisnicima da budu dodatno informisani o tome da li žele da se njihovo tagovanje objavi na timeline-u. Međutim i tada se tagovanje ne može isključiti niti zabraniti. Kad je neko lice tagovano, to ostaje u Fejsbukovoj bazi podataka.

Prema Šremsovima navodima iz tužbe i ova opcija funkcioniše bez izičitog pristanka Fejsbuk korisnika. Ovim je povređen član 7 (a) *Direktive o zaštiti podataka*, pošto ne postoji izričiti pristanak korisnika podataka za pojedine oznake („Opt-In“ princip). Stoga je obrada podataka korisnika nelegalna. Osim toga prilikom tagovanja ukoliko se ne isključi ova opcija, moguće je to učiniti i kasnije ali ne u celosti. Na Fejsbuku, ukoliko je jedanput osoba obeležna, nemoguće je ukloniti tag u potpunosti, pošto se može pronaći u profilima drugih korisnika. Iako stoji „ukloniti oznaku“, u praksi je ovaj tag samo ostao nevidljiv za korisnika i time korisnici obmanuti da je njihova fotografija uklonjena. Time je povređen član 6 stav 1 (a) *Direktive o zaštiti podataka*. Takođe ne postoje tačne informacije o neophodnosti ovog procesa u politici o privatnosti Fejsbuka čime je povređen član 10 *Direktive o zaštiti podataka*. Pored toga ne postoji ni legitiman cilj odnosno svrha čuvanja ovih podataka. Stoga podaci moraju biti obrisani shodno članu 6 stav 1 (b) *Direktive o zaštiti podataka*. Dalja obrada ovih delova podataka o korisnicima, zbog nedostatka odgovarajuće svrhe, izgleda prekomerna i time predstavlja povredu člana 6 stav 1 (c) i (d) *Direktive o zaštiti podataka*. Na kraju ne postoji posebno odobrenje korisnika za upotrebu ovih podataka, nakon što su oni uklonili određenu sliku ili sadržaj. Ukoliko Fejsbuk ne ukloni ove sadržaje, nedostaje pristanak i informacija korisnicima, da će se njihovi podaci i nadalje koristiti na profilima prijatelja. Time se vrši povreda člana 7 (a) *Direktive o zaštiti podataka*.⁴⁶ S obzirom da ne postoji mogućnost za korisnike da uklone trajno i potpuno njihovo obeležavanje, već je to učinjeno nevidljivo jedino za one koji su uklonili oznake, dalja obrada ovakvih podataka od strane Fejsbuka predstavlja povredu člana 14 *Direktive o zaštiti podataka*.⁴⁷

2.2.5. Prevelika količina podataka

Fejsbuk sakuplja ogromnu količinu podataka o korisnicima, kojih trenutno ima preko dve milijarde. Time je ova društvena mreža uspeła da sakupi podataka koliko ni jedna vlada na svetu do sada nije uspeła. Pošto Fejsbuk koristi veliki broj

46 Maks Šrems, *Complaint against Facebook Ireland Ltd.* — 11 „Removal of Tags“, Vienna, 18. August 2011, http://www.europe-v-facebook.org/Complaint_11_RemovalOfTags.pdf, 7. 8. 2012.

47 *Ibidem*.

podataka i nakon njihovog brisanja, postavlja se pitanje svrhe njihovog čuvanja. Sa svim je sigurno da većina tih podataka ne predstavlja neophodnu potrebu za funkcionisanje Fejsbuka kao društvene mreže. Osim toga postavlja se i pitanje sigurnosti tolikog broja podataka Fejsbuk korisnika. Iz tih razloga je Maks Šrems u svojoj tužbi tvrdio da Fejsbuk krši *princip minimizacije podataka* iz člana 6 (c) *Direktive o zaštiti podataka*: 1) korisnik mora dobiti mogućnost da obriše podatke koji nisu više potrebni; 2) neophodno je smanjiti količinu podataka.

Pored ovoga postoji konstantna pretnja po korisnike, zbog lakog pristupa osetljivim informacijama koje se čuvaju od strane Fejsbuka, čime se narušavaju članovi 16 i 17 *Direktive o zaštiti podataka*.⁴⁸

Koliko je opasna po same korisnike Fejsbuka prevelika količina podataka pokazuju i primeri iz prakse. Nedavno su lični podaci od oko 100 miliona korisnika Fejsbuka dospeli na internet i time se pokazalo koliko prevelika količina podataka koju Fejsbuk ima, može narušiti privatnost njegovih korisnika. Na stranici The Pirate Bay je objavljena lista koja sadrži URL profil, ime, i jedinstveni ID korisnika Fejsbuka. Listu je sastavio čovek, koji je želeo da ukaže na probleme vezane za privatnost Fejsbuk korisnika. On je uspeo da uz jednostavnu šifru dođe do ovakvih podataka. Ukazao je da je Fejsbuk morao da predvidi ovaj napad i da firma sa tolikim brojem inženjera nije uspela da predvidi napad. Time je pokazano koliki problem Fejsbuk ima sa zaštitom prevelike količine podataka.

Iz Fejsbuka su se branili time da su ove informacije koje su dospele u javnost ionako već bile dostupne. Naglašeno je i da su članovi Fejsbuka vlasnici svojih podataka i informacija i da imaju pravo da podele šta, sa kim i kada žele. Objasnjeno je i da je ova lista slična belim stranama telefonskih imenika, gde se mogu videti podaci koje ljudi ostavljaju da bi neko mogao da ih pronađe. To je ustvari i jedan od razloga zašto se neko i priključuje Fejsbuku, navode iz kompanije. Osim toga istaknuto je da nijedan zaštićeni ili skriveni podataka nije objavljen.⁴⁹

U Fancuskoj i Velikoj Britaniji je virus Ranmit ukrao 45.000 šifri Fejsbuk korisnika, što je kompanija i potvrdila. Virus je inače poznat po tome što je specijalizovan za krađu bankarskih podataka. Ovaj virus su hakeri slali prijateljima korisnika na čije profile su uspeli da pristupe. Na taj način se razvio moderan način hakovanja na društvenim mrežama. S obzirom na količinu podataka koju Fejsbuk poseduje, mogućnosti i opasnosti od ovog novog vida sajber kriminala su samim time povećane. U isto vreme veliku opasnost predstavlja i neočekivanost samog napada, kao i otkrivanje, pošto korisnici neće biti ni svesni da su napadnuti, jer su im ukradene lozinke.⁵⁰ Stoga korisnici moraju biti izuzetno oprezni prilikom potvrđivanja upita i poželjno je da se koriste različite šifre prilikom aktivnosti na internetu.⁵¹

48 *Ibidem*.

49 *Procurili detalji o 1/5 korisnika Facebooka*, sajt B92, http://www.b92.net/tehnopolis/vesti.php?yyyy=2010&mm=07&nav_id=448610, 7. 8. 2012.

50 *Virus ukrao 45.000 lozinke na Fejsbuku*, sajt Blica, <http://www.blic.rs/IT/300020/Virus-ukrao-45000-lozinke-na-Fejsbuku>, 7. 8. 2012.

51 *Facebook meta novog malvera*, izvor: Digital Trends, sajt B92, http://www.b92.rs/tehnopolis/vesti.php?yyyy=2012&mm=01&nav_id=571651, 7. 8. 2012.

Koliko su podaci na Fejsbuku zaštićeni pokazao je i slučaj samog osnivača Fejsbuka Marka Zakerberga, pošto je njegov album sa slikama dospelo u javnost. Greškom u prijavnim sistemu došlo je do mogućnosti da ostali Fejsbuk korisnici mogu videti privatne slike koje su inače ranije bile zatvorene za javnost. Ovaj nedostatak u sistemu su otkrili članovi jednog foruma. Naime, ukoliko se određena slika označi kao neprikladna, Fejsbuk je prebacivao korisnike na stranicu, na kojoj se traže bliži navodi o tome. Tom prilikom je opcija „golotinja ili pornografija“ dala mogućnost da se pri sastavljanju izveštaja vide i ostale slike prijavljenih korisnika. Pritom su se pokazale slike u punoj veličini, kojima inače nije bilo moguće pristupiti. Korisnici Fejsbuka naravno o ovome nisu bili obavješteni, nisu ni znali da se napad dogodio. Iz Fejsbuka je potvrđeno da je zbog promene kodova omogućen uvid u privatne slike korisnika.⁵²

Fejsbuk je otvorio centar za skladištenje podataka u mestu Luleå u Švedskoj. Ovaj gradić se nalazi blizu polarnog kruga i zbog svoje hladnoće pogoduje rashlađivanju hale sa računarima, koja bi trebala da obuhvata površinu 11 fudbalskih igrališta.⁵³ Ovo je utoliko interesantno za korisnike, koji dolaze iz EU, pošto će snimanjem i skladištenjem podataka u Evropi doći do primene evropskih propisa.⁵⁴

Izgleda da Fejsbuk nije slučajno odabrao Švedsku, kao zemlju u kojoj će čuvati podatke svojih korisnika. Naime, radi se o tome da je na osnovu švedskog zakona moguće nadzirati komunikaciju evropskih korisnika Fejsbuka od strane švedskih tajnih službi. Na osnovu zakona omogućeno je švedskom ministru odbrane kao i tajnim službama da nadziru ceo internet, telefonski saobraćaj, bez odluke suda. Dovoljena je i distribucija ličnih podataka državnim vlastima u inostranstvu. Pored toga internet servis provajderi su u obavezi da tajnim službama dostave kopiju čitavog protoka podataka, koji se odvija kroz švedsku teritoriju. Ovom kopijom bi bili naravno obuhvaćeni i korisnici Fejsbuka. Jedini način da se ovo predupredi je da se protok podataka šifrira. Inače ovaj zakon je neposredno nakon usvajanja stavljen na proveru pred Evropskim sudom za ljudska prava. Problem je što će se sud o tome odlučiti tek za 5 godina, a dotle će ovaj zakon biti na snazi.

Upravo držanje Fejsbuka i insistiranje na gradnji ovakvog centra za skladištenje podataka baš u Švedskoj, jasno pokazuje namere firme. Gugl je, primera radi, imao sličnu nameru da napravi centar u gradu Lund, ali je od toga odustao, pošto su se upoznali sa kontroverznim zakonom. Umesto toga odlučili su se za pravljenje centra za skladištenje podataka u Finskoj.

Treba imati uvek u vidu da od prikupljanja podataka, u mnogome zavisi udeo zastupljenosti na tržištu.⁵⁵ Pošto ljudi vole direktnu onlajn komunikaciju sa prija-

52 *Fehler gab private Facebook-Fotos frei, futurzone*, futurzone. at, <http://futurezone.at/digitallife/6255-fehler-gab-private-facebook-fotos-frei.php>, 7. 8. 2012.

53 Cindy Michel, *So sieht es zu Hause bei Facebook in Schweden aus*, <https://www.wired.de/collection/tech/so-sieht-es-zu-hause-bei-facebook-schweden-aus>, 15. 10. 2017.

54 *Facebook will Datenzentrum in Schweden bauen*, futurzone.at, <http://futurezone.at/b2b/5641-facebook-will-datenzentrum-in-schweden-bauen.php>, 7. 8. 2012.

55 Na osnovu istraživanja kompanije Symantec pokazano je da organizacije širom sveta drže oko 2,2 zetabajta (deset na dvadeset prvi) podataka i troše 1.100 milijardi dolara da ih obezbede i omoguće im pristup. Veće kompanije godišnje prosečno troše 38 miliona dolara, a male i

teljima, kontrola sadržaja komunikacije pomaže kompanijama da bi korisnicima omogućile kvalitetniji sadržaj. To se čini na osnovu komunikacije između osoba sa kojima su korisnici najčešće u kontaktu. Na taj način će kompanije koje imaju veću kontrolu podataka korisnika, imati i veću zaradu. Veliki rat u ovom pogledu se vodi između Gugla i Fejsbuka. Koja firma sakupi više informacija, imaće bolji položaj na tržištu i veću dobit.⁵⁶

2.2.6. Slike korisnika

Svaki korisnik Fejsbuka koji poznaje URL adresu određene slike, može joj pristupiti i nakon njenog brisanja.⁵⁷ To je moguće učiniti i nakon 16 meseci od brisanja slike unošenjem URL adrese. Neki korisnici su ovakvim postupkom došli i do fotografija, koje su zvanično bile obrisane pre tri godine.⁵⁸ Iz Fejsbuka su obećali da će sve obrisane slike biti zaista obrisane u roku od 2 meseca.⁵⁹

Šrems je smatrao da je na ovaj način je povređen član 6 stav 1 (a) *Direktive o zaštiti podataka*, pošto ne postoji transparentan način da se podaci i dalje mogu zadržavati. Za razliku od toga, korisnicima je saopšteno da se ti podaci brišu. Osim toga ne postoje ni tačne informacije o ovome u politici o privatnosti Fejsbuka čime se krši član 10 *Direktive o zaštiti podataka*.

Ne postoji legitimna svrha čuvanja ovih slika, te bi stoga trebale biti obrisane shodno članu 6 stav 1 (b) *Direktive o zaštiti podataka*. Pošto dalja obrada tih podataka nije neophodna, dolazi do povrede člana 6 stav 1 (c) *Direktive o zaštiti podataka*.

Pored toga obrada podataka traje duže nego što je potrebno da bi se ispunio cilj, što predstavlja povredu člana 6 stav 1 (d) *Direktive o zaštiti podataka*.

Štaviše, čini se da nikad nije postajao pristanak od strane korisnika za korišćenje ovih podataka. Tako da ukoliko Fejsbuk prilikom klika na taster brisanje, podatke ne ukloni, samim time ne dobija pristanak ni da te podatke zadrži, što predstavlja kršenje člana 7 (a) *Direktive o zaštiti podataka*.⁶⁰

srednje oko 332.000 dolara kako bi smestile i obezbedile svoje poslovne podatke. *Čuvanje podataka košta nas 1.100 mlrd \$*, izvor: Mikro, sajt B92, http://www.b92.net/tehnopolis/vesti.php?yyyy=2012&mm=06&nav_id=621914, 2. 8. 2012.

56 *Apple, FB, Google: Rat oko poruka*, Izvor: Techcrunch, sajt B92, http://www.b92.net/tehnopolis/vesti.php?yyyy=2012&mm=07&nav_id=623771, 1. 8. 2012.

57 URL (akronim za engl. Uniform Resource Locator) je veb adresa određenog resursa na internetu. Resurs na koji pokazuje URL adresa može biti HTML dokument (bilo koja veb stranica), slika, ili bilo koja datoteka koja nalazi na određenom veb serveru. URL, *Wikipedija slobodna enciklopedija*, <http://hr.wikipedia.org/wiki/URL>, 7. 8. 2012.

58 *FB čuva obrisane fotografije*, sajt B92, http://www.b92.net/tehnopolis/vesti.php?nav_id=465257&fs=1, 7. 8. 2012.

59 *Facebook: Gelöschte Fotos bleiben abrufbar*, futurzone.at, <http://futurezone.at/digitallife/7279-facebook-geloeschte-fotos-bleiben-abrufbar.php>, 7.8.2012.

60 Maks Šrems, *Complaint against Facebook Ireland Ltd. — 20 „Deleted Pictures“*, Vienna, 19. September 2011, http://www.europe-v-facebook.org/Complaint_20_deleted_pictures.pdf, 7. 8. 2012.

2.2.7. Friend Finder opcija

Ova opcija je izazvala mnogo burnih reakcija pre svega u Nemačkoj. Radi se o opciji kojom se omogućava Fejsbuk korisnicima da potraže svog prijatelja na ovoj društvenoj mreži. Tom prilikom Fejsbuk zna tačno koga bi određena osoba mogla da poznaje, a i da sama nije korisnik Fejsbuka.⁶¹ Ovom opcijom Fejsbuk je želeo da korisnicima omogući da lakše stupe u kontakt sa svojim prijateljima.

Fejsbuk šalje pozive u ime korisnika, pošto obradi njihove podatke. Opravdanje za ovakvo postupanje je dobrovoljni pristanak korisnika na ovu opciju, pošto se korisnici sa ovim moraju prethodno saglasiti.⁶² Problematično je prilikom korišćenja ove opcije i to što su njome pogođeni i korisnici koji uopšte i ne koriste Fejsbuk. Prilikom sakupljanja podataka o licima koja nisu korisnici ove društvene mreže, snimaju se njihovi lični podaci, bez njihovog pristanka. Ovo se obavlja na taj način što se npr. podaci uzimaju od e-mail provajdera, sinhronizacijom preko mobilnih telefona, preuzimanjem podataka iz sms poruka, ili čuvanjem upita pretrage kada korisnik pretražuje svoje prijatelje. Ovom prilikom je moguće utvrditi odnose između ljudi, bez da su oni uopšte i prijavljeni na ovoj društvenoj platformi.⁶³ Snimljene e-mail adrese se onda putem reklamnih mejlova koriste, tako da se pozivaju prijatelji da pristupe Fejsbuku. Tom prilikom se u mejl unose fotografije mogućih poznanika, koji su već članovi Fejsbuka i šalju se potencijalnim članovima. Na taj način se stvaraju tzv. „profili iz senke“.⁶⁴

Još 2009. godine je kritikovana ova opcija od strane Evropske komisije, naročito u pogledu prikupljanja i korišćenja e-mail adresa i podataka od korisnika koji nisu na Fejsbuku. Ovo svakako predstavlja prekršaj osnovnih principa zaštite podataka, ukoliko se snimaju podaci korisnika koji ne koriste ovu društvenu mrežu, pošto nedostaje pravni osnov za prikupljanje ovih podataka.⁶⁵

Osim ovih kritika, primetno je da nedostaje obaveštenje o tome da se uopšte prave ovi profili iz senke i na koji način se ovakvi podaci koriste i sakupljaju. Prema Šremsovoj tužbi to ponašanje predstavlja kršenje člana 6 stav 1 (a) *Direktive o zaštiti podataka*. Fejsbuk u svojoj politici o privatnosti ne napominje ovu mogućnost, čime se krši član 10 *Direktive o zaštiti podataka*. Izostaje i svrha korišćenja daljih podataka prilikom upotrebe ove opcije shodno članu 6 stav 1 (b). Stoga je i dalja obrada podataka suvišna na osnovu člana 6 stav 1 (c).

U politici o privatnosti postoje samo opšte odredbe ali ne i informacije o tome koji se podaci sakupljaju putem ove opcije, tako da ne postoji specifičan pristanak

61 *Facebook entschärft „Friend Finder“ (aber nur ein bißchen)*, freidaten.org, <http://www.freidaten.org/facebook-andert-friend-finder-aber-nur-ein-bisichen/>, Presseerklärung von Prof. Dr. Caspar vom 24. 1. 2011, 7. 8. 2012.

62 Dr. Günther Leissler, *Social Networks*, Ecolex 2010/837.

63 *Facebooks unsichtbare Listen*, Datenschutz, Zeit online, <http://www.zeit.de/2010/35/Facebook>, 7. 8. 2012.

64 Maks Šrems, *Complaint against Facebook Ireland Ltd. — 02 „Shadow Profiles“*, Vienna, 18. August 2011, http://www.europe-v-facebook.org/Compalint_02_Shadow_Profiles.pdf, 7. 8. 2012.

65 Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking*, Adopted on 12 June 2009.

korisnika, koji je neophodan da bi se postupalo u skladu sa članom 7 (a) *Direktive o zaštiti podataka*.⁶⁶

Hamburški poverenik za zaštitu podataka je zbog koršćenja ove opcije od strane Fejsbuka žestoko kritikovao društvenu mrežu Fejsbuk. Kritika je urodila plodom pa je popisan i sporazum sa Fejsbukom u vezi sa opcijom Friend Finder. Uбудuće bi ova opcija trebalo da bude transparentna i u skaldu sa standardima zaštite podataka.⁶⁷ Trebalo bi korisnike upozoriti jasno na to šta se dešava sa njihovim adresarom, kada se u njega ubacuju podaci.⁶⁸ Korisnik bi trebalo da ima mogućnost da sam odredi koji kontakti iz njegovog adresara mogu da se nađu na ovakvoj pozivnici od strane Fejsbuka.⁶⁹

Glavni deo sporazuma se odnosi na ophođenje sa podacima korisnika, koji nisu registrovani na Fejsbuku. Ovi podaci se smeju koristiti samo za cilj pretrage prijatelja.⁷⁰ Osim toga korisnici koji nisu na Fejsbuku a koji dobiju pozivnicu, moraju dobiti naznaku o tome, zbog čega su dobili pozivnicu i na koji način mogu sprečiti dalji prijem pozivnica. Putem „Opt-Out“ principa, korisnicima se daje naknadna mogućnost da ovakve mejlove spreče.⁷¹ Ipak može se primetiti da nije postignuto jedno sveobuhvatno rešenje, kojim bi se sprečilo prikupljanje podataka od trećih lica, koja nisu uopšte na Fejsbuku.⁷²

Organizacija za zaštitu prava potrošača podnela je zbog ove opcije tužbu protiv Fejsbuka. Fejsbuku je prigovoreno da korisnici o ovoj opciji nisu bili adekvatno informisani, da se njihovi kontakti iz adresara koriste za slanje pozivnica za priključenje Fejsbuku. Nemački regionalni sud je doneo odluku da Fejsbuk mora da informiše korisnike Friend Finder opcije o tome šta radi sa njihovim kontaktima iz adresara.⁷³ Pored toga Fejsbuk ne bi smeo nadalje u opštim uslovima da dobije besplatno pravo korišćenja sadržaja korisnika, koji oni postavljaju na svoje profile. Korisnici bi trebalo da ostanu vlasnici njihovih sadržaja.⁷⁴

66 *Complaint against Facebook Ireland Ltd. — 02 „Shadow Profiles“*, Vienna, 18. August 2011, http://www.europe-v-facebook.org/Compalint_02_Shadow_Profiles.pdf, 7. 8. 2012.

67 *Facebook: Friend Finder wird transparenter*, Focus online, http://www.focus.de/digital/internet/facebook/facebook-friend-finder-wird-transparenter_aid_593133.html, 7. 8. 2012.

68 *Facebook entschärft „Friend Finder“ (aber nur ein bisschen)*, freidaten.org, <http://www.freidaten.org/facebook-andert-friend-finder-aber-nur-ein-bischen/>, Presseerklärung von Prof. Dr. Caspar vom 24. 1. 2011, 7. 8. 2012.

69 *Sieg für Datenschützer: Facebook will „Friend Finder“ ändern*, netzwelt.de, <http://www.netzwelt.de/news/85390-sieg-datenschuetzer-facebook-will-friend-finder-aendern.html>, 7. 8. 2012.

70 *Facebook entschärft „Friend Finder“ (aber nur ein bisschen)*, freidaten.org, <http://www.freidaten.org/facebook-andert-friend-finder-aber-nur-ein-bischen/>, Presseerklärung von Prof. Dr. Caspar vom 24. 1. 2011, 7. 8. 2012.

71 *Sieg für Datenschützer: Facebook will „Friend Finder“ ändern*, netzwelt.de <http://www.netzwelt.de/news/85390-sieg-datenschuetzer-facebook-will-friend-finder-aendern.html>, 7. 8. 2012.

72 *Facebook entschärft „Friend Finder“ (aber nur ein bisschen)*, freidaten.org, <http://www.freidaten.org/facebook-andert-friend-finder-aber-nur-ein-bischen/>, Presseerklärung von Prof. Dr. Caspar vom 24. 1. 2011, 7. 8. 2012.

73 *Nemačka: Sudska odluka protiv Facebooka*, sajt B92, http://www.b92.rs/tehnopolis/vesti.php?yyyy=2012&mm=03&nav_id=588644, 7. 8. 2012.

74 *Gerichtsurteil: Facebook-Freundfinder illegal*, futurzone.at, <http://futurezone.at/digitallife/7836-gerichtsurteil-facebook-freundfinder-illegal.php>, 7. 8. 2012.

2.2.8. Politika privatnosti Fejsbuka

Mnogi korisnici Fejsbuka bi želeli da imaju stari izgled svog profila i da ne budu na novom Timeline-u. Sa tim u vezi se pojavio veliki broj prevaranata, koji nude mogućnost prebacivanja na stari profil uz pomoć tzv. Scam — linkova.

Činjenica je da korisnici nikako ne mogu povratiti stari izgled profila, iako je ova opcija uvedena polovinom decembra 2011. Ukoliko se korisnik jedanput prebaci na timeline, povratak na stari izgled profila više nije moguć.

Uprkos tome mnogi korisnici veruju da je moguće da se povrati stari izgled njihovih profila, pa prevaranti takvima i nude pomoć, kako da „povrate“ izgled svojih ranijih profila. Tako se korisnicima nudi da uz više klikova na lajk dugme, ili više pregleda Jutjub video klipova ponovo vrata stari izgled profila.

Ukupno je do sada pronađeno 16 sajtova, koji su se bavili ovom vrstom prevare. Prikupili su za kratko vreme oko 70.000 lajkova korisnika, koji su verovali da je moguće uspostaviti ranije profile. Pored postojanja ove vrste prevare, na Fejsbuku ne postoji nikakvo upozorenje o tome. Fejsbuk kompanija daje samo mogućnost korisnicima da prijave ovakvo ponašanje prevaranata.⁷⁵

Fejsbuk je ponovo promenio politiku privatnosti, što je već uobičajeno. I pored kritika, prava korisnika se još više ograničavaju. Fejsbuk kompanija je zadržala pravo da promeni svoje uslove korišćenja bez informacija o tome. Stručnjaci za zaštitu podataka ističu da mali broj korisnika ima predstavu o promeni politike privatnosti i uopšte korišćenja Fejsbuka. To se događa iz razloga, što se korisnici automatski ne informišu, kada se planira ova vrsta promene. Da bi korisnik uopšte bio upućen o planovima Fejsbuka, potrebno da postane član „Fan“ stranice „Facebook Site Governance“.⁷⁶

Sa stanovišta zaštite podataka politika Fejsbuka nije u skladu sa propisima evropskog prava. I dalje ne postoji pristanak korisnika i objašnjenje o načinu obrade njihovih podataka. Osim toga ne postoji ni mogućnost izbora za korisnike, koji žele da spreče upotrebu njihovih podataka u reklamne svrhe. Ograničena mogućnost izbora je propisana u odeljku 14.6. Nove politike Fejsbuka, u kojoj se kaže da: „tvoje dalje korišćenje Fejsbuka nakon promena naših uslova znači ujedno i tvoj pristanak na naše promenjene uslove“.⁷⁷ Neophodan bi bio izričit pristanak i informacija od strane Fejsbuka o tome. Bez informacija o tome pre stupanja na snagu ovih pravila od strane Fejsbuka, ne može se smatrati da je korisnik pristao na dalje korišćenje Fejsbuka pod ovakvim uslovima. Za korisnike Fejsbuka iz Nemačke postoji posebno pravilo, da promene uslova korišćenja stupaju na snagu 30 dana nakon usvajanja, što takođe ne predstavlja jasan i nedvosmislen pristanak korisnika.

Pored toga problematična je odredba iz odeljka 2.3. „Kada ti ili ostali korisnici, koji tvoje sadržaje i informacije mogu videti, koristite jednu aplikaciju, prenose se

75 *Facebook-Timeline im Visier von Betrügern*, futurzone, portal futurzone. at, <http://futurezone.at/digitallife/6671-facebook-timeline-im-visier-von-betruergern.php>, 7. 8. 2012.

76 Stranici se može pristupiti pomoću adrese <http://www.facebook.com/fbsitegovernance>, Fejsbuk, 7. 8. 2012.

77 Celokupni spisak odredbi može se videti na https://www.facebook.com/note.php?note_id=10151419988630301, *Aktualisierung der Erklärung der Rechte und Pflichten*, Facebook Site Governance, Fejsbuk, dostupno na nemačkom jeziku., 7. 8. 2012.

tvorji sadržaji i informacije aplikaciji“.⁷⁸ Veliki problem predstavljaju u ovoj odredbi „ostali korisnici“, pošto se pored njihovih podataka šalju i podaci korisnika, koji su njihovi prijatelji, na tu aplikaciju.

Još jedna problematična odredba se nalazi u odeljku 10.3. „Ti razumeš da mi plaćene usluge i komunikacije ne obeležavamo uvek kao takve“. Što takođe govori o transparentnosti na Fejsbuku.⁷⁹

Koliko je politika privatnosti jasna i razumljiva govori još jedan njen segment „Mi obrađujemo vaše podatke, da bi vam ponudili sigurno, efikasno i prijatno iskustvo“.⁸⁰

Fejsbuk je takođe 7. septembra 2011. godine promenio svoju politiku privatnosti, koja je trajala nešto više od 8 meseci. Ovaj postupak je objavljen isto tako jednostrano i bez istaknutih informacija o tome i saglasnosti korisnika, iako su se obavezali na to u svojoj politici, ali se u praksi dešava suprotno.

Po Šremsovim navodima u tužbi može se zaključiti da Fejsbuk krši član 7 (a) *Direktive o zaštiti podataka*, pošto se upotreba i obrada podataka može odnositi samo na nedvosmisleni, izričit pristanak korisnika, koji je predhodno bio informisan o ovim radnjama. Nema sumnje da saglasnost korisnika izostaje potpuno u ovom slučaju.⁸¹ Fejsbuk bi se mogao braniti time da su korisnici samim prijavljivanjem na Fejsbuk prihvatili njihove standarde. I pored toga izgleda da je pristanak posebno pod znakom pitanja, pošto bi trebalo uvesti „Opt-In“ princip, kojim bi korisnik bio u mogućnosti da sam kontroliše svoj nalog, a ne da konstantno vrši proveru privatnosti. Takođe bi trebalo usvojiti sistem, kojim bi korisniku bilo omogućeno da se izjasni o novoj politici Fejsbuka. Korisnici koji ne bi želeli da daju saglasnosti, trebali bi da dobiju mogućnost brisanja naloga.

Fejsbuk često menja svoje politike privatnosti. U jednoj od promena svog načina ophođenja sa privatnosti, bio je promenjen pristup. Podstaknuti tužbama Maksa Šremsa čelnici Fejsbuka su dozvolili da, pre usvajanja promene politike, korisnici imaju mogućnost da glasaju o tome. Upravo se ovo i svelo samo na mogućnost. Treba imati u vidu da Fejsbuk smatra da su korisnici dovoljno svesni promena, ukoliko se one objave u medijima ili na njihovom sajtu.⁸² Pored toga su ove odredbe izuzetno komplikovane, tako da ih korisnici ne razumeju.⁸³ Fejsbuk je propisao da bi ova nova politika o privatnosti bila obavezujuća za sve korisnike u slučaju

78 Odredba se može videti na https://www.facebook.com/note.php?note_id=10151419988630301, *Aktualisierung der Erklärung der Rechte und Pflichten*, Facebook Site Governance, Fejsbuk, dostupno na nemačkom jeziku., 7. 8. 2012.

79 *Weniger Rechte, mehr Pflichten — Facebook ändert Nutzungsbedingungen*, ULD | Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Pressemitteilung, <https://www.datenschutzzentrum.de/presse/20120321-facebook-nutzungsbedingungen.htm>, 7. 8. 2012.

80 Pressekonferenz vom 20120207 — Max Schrems, *Europe vs. Facebook*, <http://www.youtube.com/watch?v=YJ4Ey-h9wYo>, 7. 8. 2012.

81 Max Schrems, *Complaint against Facebook Ireland Ltd. — 08 „Consent and Privacy Policy“*, Vienna, 18. August 2011, http://www.europe-v-facebook.org/Complaint_08_ConsentPrivacyPolicy.pdf, 7. 8. 2012.

82 Barbara Wimmer, *Datenschutz— Facebook vs. Schrems: Das Gesprächsprotokoll*, futurzone.at, <http://futurezone.at/netzpolitik/7555-facebook-vs-schrems-das-gespraechsprotokoll.php>, 3. 8. 2012.

83 *Diskussion— „User-Daten sind das neue Öl“*, futurzone, futurzone.at, <http://futurezone.at/netzpolitik/10349-user-daten-sind-das-neue-oel.php>, 3. 8. 2012.

da se sa njom saglasi 30% registrovanih korisnika ove društvene mreže. U tom periodu je to predstavljalo oko 270 miliona korisnika.⁸⁴ Rezultat je pokazao da je skoro 87% glasača za to da se zadrže stara pravila privatnosti a ne nova. Iako je na glasanju učestvovalo samo 0,038% članova ili jedan na svakih 2.600, Fejsbuk je promenio politiku privatnosti.⁸⁵ Pored toga što su prekršili svoja pravila, pokazalo se i koliko su korisnici svesni i upućeni u promene koje se dešavaju potpuno bez njihovog znanja i saglasnosti.

Najveću novinu u ovoj promeni politike privatnosti predstavljala odredba kojom Fejsbuk može zadržati podatke korisnika, kako bi se korisnicima omogućile i ostale usluge. Ova odredba se odnosi na sve podatke, pa i na one koje Fejsbuk dobije od oglašivača.⁸⁶

Maks Šrems je tu odredbu po kojoj se Fejsbuk ovlašćuje za kontrolora svih podataka njegovih korisnika nazvao „*potpunom eksproprijacijom ličnih podataka korisnika*“. Na taj način korisnici nisu više imaoi tj. vlasnici svojih podataka, već je to Fejsbuk, što je u potpunosti u suprotnosti sa svim standardima i propisima o zaštiti podataka.⁸⁷ Iako je ovu svoju odredbu Fejsbuk negirao, u politici o privatnosti je ona propisana.⁸⁸

Fejsbuk je početkom 2012. godine uveo timeline. Korisnici su imali mogućnost da sami pokrenu ovaj novi sistem i da ga isprobaju. Potom je on postao obavezan za sve korisnike. Ovaj sistem predviđa svojevrsnu digitalnu biografiju korisnika. On je utoliko problematičan, jer korisnici koji nisu primetili ovu promenu, mogli su sve svoje podatke, slike kao i komentare videti onlajn. Tek naknadno su bili u mogućnosti da svoje profile podese na način na koji oni žele. Propisivanje roka za upoznavanje kao i prinudna promena Fejsbuk profila korisnika je svakako nedopustiva bez saglasnosti korisnika.⁸⁹

2.2.9. Aplikacije

Na Fejsbuku postoji veliki broj aplikacija, koje svakodnevno koriste korisnici ove društvene mreže. Ove aplikacije nude na Fejsbuku tzv. „treće strane“, koje ih prave, i upravljaju njima sa bilo koje lokacije na svetu. Fejsbuk omogućava trećim stranama da dođu do podataka korisnika aplikacija. Prema nekim izvorima dnevno se na Fejsbuk instalira oko 20 miliona aplikacija. Ovako veliki broj aplikacija uzrokuje i velike probleme na polju privatnosti, zbog povećanog transfera podataka

84 *Befragung — Facebook lässt über Datenschutz abstimmen*, futurezone/apa, futurzone.at, <http://futurezone.at/netzpolitik/9400-facebook-laesst-ueber-datenschutz-abstimmen.php>, 2. 8. 2012.

85 *Prvo glasanje na FB prošlo neslavno*, sajt B92, http://www.b92.net/tehnopolis/vesti.php?yyyy=2012&mm=06&nav_id=617494, 2. 8. 2012.

86 *Facebook will Daten länger speichern*, futurezone.at, apa/dpa, <http://futurezone.at/digitallife/9052-facebook-will-daten-laenger-speichern.php>, 2. 8. 2012.

87 *Kritik— Facebook-Änderungen: „Enteignung der Nutzer“*, futurzone.at, <http://futurezone.at/netzpolitik/9056-facebook-aenderungen-enteignung-der-nutzer.php>, 2. 8. 2012.

88 Carsten Meyer, *Facebook: Frage nach Daten-Eigentum geklärt?*, heise.de, <http://www.heise.de/newsticker/meldung/Facebook-Frage-nach-Daten-Eigentum-geklaert-1578497.html>, 2. 8. 2012.

89 *Neuer Daten-Skandal um Facebook, Neues System legt alle Privat-Daten offen*, Wiener plant Anzeige, dnevne novine Österreich, 27 Januar 2012, strana 8.

od Fejsbuka ka trećim licima. Mnoge aplikacije ni nemaju sopstvenu politiku privatnosti, iako to Fejsbuk zahteva. Kada korisnik doda aplikaciju, na kojoj nema politike privatnosti, ne postoji čak ni upozorenje korisnicima da ne postoji politika privatnosti. Fejsbuk je čak u nekim slučajevima sakrio link koji bi trebalo da dovede do politike privatnosti.

Većina korisnika nije uopšte svesna, da ako njihov prijatelj na Fejsbuku instalira neku aplikaciju, aplikacija može automatski dovesti do transfera podataka i pristupa profilu, slikama, imenima i ostalnim podacima prijatelja. Informacija o ovome se naravno nalazi u njihovoj politici o privatnosti, koja je većini korisnika u potpunosti nepoznata. S obzirom da prosečan Fejsbuk korisnik ima oko 130 prijatelja na listi, postoji velika verovatnoća da je neko od prijatelja prihvatio ovakve aplikacije. Ipak, postoje i aplikacije koje ne zahtevaju prístup podacima prijatelja npr. igrice, kvizovi, međutim Fejsbuk i u ovakvim slučajevima nudi ograničen pristup svim osnovnim podacima o prijateljima.

Izmenom „Opt-Out“ principa moguće je postići zadovoljavajući nivo zaštite Fejsbuk korisnika. Ne postoji mogućnost korišćenja aplikacija, a da korisnici mogu da ograniče pristup podacima, koji se odnose na njihove prijatelje. Stoga bi trebalo primeniti „Opt-In“ princip, da bi se pribavila izričita saglasnost korisnika u ovom slučaju. I pored toga veoma je teško ustanoviti na koji način bi se ovi podaci korisnika, od strane trećih lica obrađivali.

Šrems je u tužbi tvrdio da, pošto korisnici nisu informisani o korišćenju njihovih podataka, time se postupa suprotno članu 7 (a) *Direktive o zaštiti podataka*. Osim toga postoje samo ograničene informacije o ovome i tačne informacije su korisnicima sakrivene što nije u skladu sa članom 10 *Direktive o zaštiti podataka*.

Svrha korišćenja podataka od strane Fejsbuka je prekršena, pošto su korisnici pristali da Fejsbuk koristi njihove podatke a ne i treća lica, time se krši član 6 stav 1 (a) *Direktive o zaštiti podataka*. Fejsbuk sa svoje strane ne nudi odgovarajući nivo zaštite privatnosti, da će treća lica ispuniti kriterijume u skladu sa članom 25 *Direktive o zaštiti podataka*, pošto ne postoji saglasnost korisnika za transfer njihovih podataka. Naime, mnoge aplikacije i ne sadrže politiku privatnosti, koje bi ovaj transfer objasnile, tako da korisnici nisu ni pitani, da li svoje podatke žele da prebace trećim licima.⁹⁰

Kompanija Symantec, koja se inače bavi bezbednošću na internetu je otkrila da je veliki broj aplikacija prosleđivao lične podatke korisnika Fejsbuka oglašivačima. U pitanju su podaci sa profila korisnika, njihove fotografije i istorijat četovanja. Navodno lica koja upravljaju aplikacijama nisu bila uopšte svesna da primaju ove podatke od korisnika Fejsbuka, iako je utvrđeno da je u pitanju stotine hiljada aplikacija, koje su primale ovakve podatke.⁹¹ Do toga je došlo tako što je Fejsbuk omogućio čitanje ovih informacija, dostavivši im greškom bezbednosni ključ.⁹²

90 Maks Šrems, *Complaint against Facebook Ireland Ltd. — 13 „Applications“*, Vienna, 18. August 2011, http://www.europe-v-facebook.org/Complaint_13_Applications.pdf, 7. 8. 2012.

91 *Lični podaci sa FB-a u rukama oglašivača*, sajt B92, http://www.b92.net/tehnopolis/vesti.php?yyyy=2011&mm=05&nav_id=511393, 7. 8. 2012.

92 *Greškom otkriveni profili korisnika „fejsbuka“*, izvor: Tanjug, sajt Blica, <http://www.blic.rs/IT/253148/Greskom-otkriveni-profil-korisnika-fejsbuka>, 7. 8. 2012.

Sa početkom korišćenja novog timeline-a korisnici su u mogućnosti da lakše i brže dolaze do informacija o aktivnostima, koje njihovi prijatelji preduzimaju. Na osnovu tzv. „Open Graph“ mogu se videti sve aktivnosti korisnika Fejsbuk aplikacije. Ove aktivnosti mogu se videti na tzv. „ticker-u“. Razlika između lajk dugmeta i Open Grapha je u tome što je sa lajkovanjem postojala samo jedna mogućnost povezivanja objekta i korisnika, dok je sa Open Graphom omogućeno pored ovoga i izbor glagola npr. čita knjigu. Suština je da korisnici ubuduće ne moraju da kliknu na određeni sadržaj, kao kod lajk dugmeta, nego je to implicirano aktivnošću korisnika automatski. Dakle, ova inovacija bi trebala u potpunosti da zameni lajk dugme. Trenutno ove aplikacije nude britanski Gardijan, američki Washington Post, video portal MyVideo, kao i Yahoo aplikacije. Korisnici dodavanjem ovih aplikacija na Fejsbuk pristupaju automatski Open Graph funkcijama. Washington Post uvek objavljuje šta korisnik trenutno čita. Ipak bi trebalo dati mogućnost korisnicima da sami odrede koje aktivnosti žele da se objavljuju svima i u kom periodu npr. do kraja nedelje, meseca.

Uvođenje ove funkcije na Fejsbuku omogućilo je pre svega firmama koje se oglašavaju veću mogućnost protoka informacija, pristupa aplikacijama, a samim tim i zarade.

Sa stanovišta zaštite podataka korisnika je ova funkcija utoliko problematična pošto se odvija bez znanja korisnika o tome, da se njihove aktivnosti objavljuju njihovim prijateljima, a oni na to nisu pristali. Osim toga nije moguće ograničiti koji prijatelji mogu da vide ove aktivnosti. Iz Fejsbuka poručuju da se objavljuju samo aktivnosti vezane za aplikacije kojima korisnici svakodnevno pristupaju i da su korisnici u mogućnosti da se saglase sa ovom opcijom.⁹³

2.3. Postupak u Irskoj protiv Fejsbuka

Ispitivanje tužbenih navoda Maksa Šremsa izvršeno je u Irskoj. Ceo postupak je trajao tri meseca. Fejsbuk je obavezan od strane irske Komisije za zaštitu podataka da mora da više vodi računa o jednostavnijim objašnjenjima u svojoj politici o privatnosti.⁹⁴ Ipak ova Komisija je zatražila u njihovom izveštaju od Fejsbuka izvesna poboljšanja, dok teže povrede iz navedenih tužbi nije ustanovila. Ova poboljšanja je trebalo da budu sprovedena do kraja marta 2012. godine, dok se dalja provera stanja od strane irske Komisije za zaštitu podataka nastavila u junu 2012. godine.

Podnosilac tužbenih zahteva smatra da su oni delimično obuhvaćeni, kao i da nije urađena potpuna pravna analiza tužbenih zahteva.⁹⁵ Naročito se prigovara da je u izveštaju potpuno isključeno ophođenje prema tzv. „profilima iz senke“ i njihovom pravljenju od strane Fejsbuka, na osnovu praćenja komunikacije među

93 Facebook: Automatische Nutzererfassung läuft an, Jakob Steinschaden, futurzone.at, <http://futurezone.at/produkte/5683-facebook-automatische-nutzererfassung-laeuftan.php>, 7. 8. 2012.

94 „Fejsbuk“ prošao test bezbednosti privatnih podataka, sajt Blica, <http://www.blic.rs/IT/297483/Fejsbuk-prosao-test-bezbednosti-privatnih-podataka>, 7. 8. 2012.

95 Barbara Wimmer, Max Schrems: „Facebook muss noch viel lernen“, futurzone.at, <http://futurezone.at/netzpolitik/7314-max-schrems-facebook-muss-noch-viel-lernen.php>, 7. 8. 2012.

korisnicima. Za to ne postoji adekvatna analiza u izveštaju koja pokazuje da je to tačno, tvrde iz Fejsbuka.⁹⁶

Osim toga kod tehnike prepoznavanja lica, konstatovano je da nije obezbeđen jasan i nedvosmislen pristanak korisnika na ovu opciju.

Fejsbuk je obavezan da:

1. Dostavi kopiju kategorija podataka, koju ima o preko 40.000 korisnika, koji su to zahtevali. Ovi podaci treba da uključe i podatke o prepoznavanju lica, kao i sve podatke koje Fejsbuk ima u svojoj bazi podataka;
2. Podatke korisnika može upotrebljavati ograničeno za reklamiranje;
3. Koristi lajk dugme od sada u ograničenom obimu;
4. Ne sme da prati korisnike na osnovu lajk dugmeta;
5. Slike korisnika ne sme koristiti za reklame, osim ukoliko se korisnik izričito sa time saglasio;
6. Korisniku mora dati mogućnost da obriše svoje slike, pošto su do sada izbrisane slike bile zadržavane od strane Fejsbuka;
7. Korisnici se ne smeju dodavati u grupe bez njihove saglasnosti;
8. Neaktivne ili deaktivirane profile mora obirsati, ako se duže vremena ne upotrebljavaju;
9. Mora da obriše poslednji broj kod IP-adresa, koje se na osnovu Social-Plugin-a sakupljaju;
10. Unose vezane za pretraživanja obriše nakon 6 meseci od unosa;
11. Pri upotrebi aplikacija podatke trećih korisnika tj. prijatelja može samo ograničeno prosljeđivati;
12. Celokupno brisanje podataka korisnika mora sprovesti u roku od 40 dana;
13. Mora proveriti uslove za zaštitu podataka od strane vlasnika aplikacija;
14. Mora dobiti ponovni pristanak korisnika, pošto je opcija prepoznavanja lica ilegalno aktivirana.⁹⁷

Ukoliko se Fejsbuk ne bude pridržavao navedenih mera, pretili mu kazna do 100.000 evra, što za ovu kompaniju predstavlja simboličnu sumu.⁹⁸ Zatim je na sastanku između predstavnika Fejsbuka i podnosioca zahteva pokušano sporazumno i vansudsko rešenje postupka, kako je predviđeno irskim pravom.⁹⁹ Pošto je ovaj pokušaj propao, dalji korak podnosioca tužbi je zahtev za formalnim rešenjem spora.¹⁰⁰ Upravo je i Fejsbuk zainteresovan za ovakvo rešenje, pošto će prema njihovim navodima tada tačno znati šta je legalno a šta nije.

96 Barbara Wimmer, *Datenschützer zweifeln an Facebook-Prüfung*, futurezone.at, <http://futurezone.at/netzpolitik/6534-datenschuetzer-zweifeln-an-facebook-pruefung.php>, 7. 8. 2012.

97 *Europe versus Facebook*, Neuigkeiten, <http://www.europe-v-facebook.org/DE/de.html>, 7. 8. 2012.

98 Jakob Steinschaden, *Wiener Studenten zwingen Facebook in die Knie*, futurezone.at, <http://futurezone.at/netzpolitik/6505-wiener-studenten-zwingen-facebook-in-die-knie.php>, 7. 8. 2012.

99 *Jus Student gegen Facebook keine Einigung*, futurzone, futurzone.at <http://futurezone.at/netzpolitik/7303-jus-student-gegen-facebook-keine-einigung.php>, 7. 8. 2012.

100 Pressekonferenz vom 20120207 — Max Schrems, *Europe vs. Facebook*, <http://www.youtube.com/watch?v=YJ4Ey-h9wYo>, 7. 8. 2012.

Ukoliko ni tom odlukom ne budu bili zadovoljni, u planu je pokretanje postupka protiv države Irske, zbog povrede ugovora EU. Potrebno bi bilo podneti zahtev za pokretanje ovog postupka pred Evropskom komisijom.¹⁰¹ Ipak su navedene mere već donele izvesne rezultate, pošto je Fejsbuk najavio da će ukinuti spornu opciju prepoznavanja lica. Međutim ostaje i dalje sumnjivo u kojoj meri i da li će svi biometrijski podaci korisnika biti obrisani kao i da li će i dalje softver za prepoznavanje lica ostati u funkciji, ali sa drugačijom svrhom. Sumnje potiču upravo s obzirom na dosadašnju praksu u obradi podataka korisnika.¹⁰²

Ceo postupak u Irskoj je mogao da traje pet i više godina, što bi predstavljao jedan dug proces, pogotovo imajući u vidu da se radi o zaštiti osnovnih ljudskih prava korisnika Fejsbuka.

U međuvremenu Maks Šrems je povukao sve svoje tužbene zahteve pred irskim sudom osim one pred Evropskim sudom. Razlog su bili troškovi postupka, koji su enormno visoki.¹⁰³

2.4. Postupak u Austriji protiv Fejsbuka

Odustajanje od tužbi protiv Fejsbuka u Irskoj, nije značilo da je Šrems odustao od njegove borbe protiv Fejsbuka. Naprotiv, on je početkom avgusta 2014. godine pozvao na zajedničku masovnu tužbu Fejsbuk korisnika protiv Fejsbuka (po uzoru na eng. class action, predviđena u pravu USA Federal Rules of Civil Procedure, Title 28 United States Code Appendix Rule 23).¹⁰⁴

Masovna/grupna ili zajednička tužba predstavlja građansku tužbu, koja u slučaju povoljnog ishoda po tužioca, donosi koristi ne samo za onoga ko je direktno tužio nego i celoj grupi — u ovom slučaju Fejsbuk korisnicima koji su se priključili tužbenom zahtevu. Dok ova tužba nije poznata u nemačkom i švajcarskom pravu, Vrhovni sud Austrije je proglasio dozvoljenom.¹⁰⁵

Tako je Maks Šrems odlučio da u Austriji podigne ovu tužbu pred Osnovnim sudom za građanske sporove u Beču. Smatrao je da su odredbe o koršćenju podataka Fejsbuka nevažeće po pravu EU. Pored toga se puno toga dešava „iza leđa“, tako da korisnici nemaju uvid u stvarno koršćenje njihovih podataka. Ovom prilikom Šrems je nudio 500 evra kao odštetu svakom Fejsbuk korisniku, koji se priključio tužbenom zahtevu. Uslov je naravno pozitivan ishod tužbenog zahteva. Po Šremsu

101 Barbara Wimmer, *Facebook verarscht uns alle*, futurezone.at, <http://futurezone.at/netzpolitik/5644-facebook-verarscht-uns-alle.php>, 7. 8. 2012.

102 *Fejsbuk isključuje sistem za prepoznavanje lica*, sajt Blica, <http://www.blic.rs/IT/344293/Fejsbuk-isklucuje-sistem-za-prepoznavanje-lica>, 24. 10. 2012.

103 Barbara Wimmer, *Datenschützer gegen Facebook: Prozess in Wien startet*, <https://futurezone.at/netzpolitik/datenschuetzer-gegen-facebook-prozess-in-wien-startet/123.636.762>, 20. 9. 2017.

104 Građanska procesna pravila SAD doneta 1937 sa mnoštvom amandmana. The original Rules of Civil Procedure for the District Courts were adopted by order of the Supreme Court on Dec. 20, 1937, transmitted to Congress by the Attorney General on Jan. 3, 1938, and became effective on Sept. 16, 1938., https://www.law.cornell.edu/rules/frcp/rule_23, 20. 9. 2017.

105 Presuda iz 2005. godine (12. 7. 2005, 4 Ob 116/05w) Vrhovni sud Austrije (OGH). http://www.verbraucherrecht.at/cms/index.php?id=51&no_cache=1&tx_ttnews%5Btt_news%5D=1109, 20. 9. 2017.

je ova suma niska, kada se uzme u obzir dosadašnja sudska praksa. Tako je u Austriji do sada minimalna odštetna suma iznosila 750 evra po osobi. Ova presuda bi po nekim proračunima mogla Fejsbuk da košta više od 10 miliona evra.

Za samog tužioca ova tužba je bila besplatna, pošto je troškove spora snosila firma Roland ProzessFinanz AG.¹⁰⁶ Međutim ova firma je zadržala pravo da se procentualno naplati iz sume od dobijenog spora.

Da bi se priključili ovoj inicijativi Šremsa, napravljen je bio poseban portal na stranici „Europe versus Facebook“ (stranica je još uvek onlajn <https://www.fbclaim.com/ui/register?lang=en>), na koji se pristupalo sa Fejsbuk profila. Argumentacija je bila da se sudu mora pokazati da svaki učesnik u tužbi ima profil na Fejsbuku. Dalji uslovi za učešće u tužbi bili su da se radi o odraslom Fejsbuk korisniku, koji ne živi u USA i Kanadi.¹⁰⁷

Pošto se tužbenom zahtevu priključilo 25.000 korisnika Fejsbuka, Maks Šrems je podneo tužbu. Tužbeni zahtev se odnosi na manjkave odredbe o zaštiti podataka koje nisu u saglasnosti sa EU pravom. Pored toga zahtev se odnosio i na postupanje prilikom obrade podataka od strane Fejsbuka. Prema Šremsu to uključuje i program nadzora PRIZMA, funkciju Graph, Fejsbukove aplikacije, lajk dugme, preveliku količinu podataka.

Osim toga značaj ovog tužbenog zahteva je ogroman, jer je ovo prva masovna tužba vezana za zaštitu podataka na evropskom kontinentu.

Na prvom zasjedanju pred Osnovnim sudom za građanske sporove u Beču bilo je rasprave o tome, da li je ovaj sud uopšte nadležan.¹⁰⁸

U odgovoru na tužbeni zahtev je Fejsbuk naveo da 25.000 učesnika u ovom tužbenom zahtevu nisu poslovno sposobni i da stoga nisu u mogućnosti da tuže. Fejsbuk je istakao da Šrems nije dostavio nikakav dokaz da su u vreme pristajanja na opšte uslove poslovanja Fejsbuka učesnici u tužbenom zahtevu bili poslovno sposobni. Na taj način je Fejsbuk po tvrdnji Šremsa korisnike Fejsbuka, koji su se priključili tužbenom zahtevu označio kao „mentalno bolesne“.

Osim toga Fejsbuk je osporavao nadležnost Osnovnog suda za građanske sporove u Beču kao mesno nadležnog za sporove protiv firmi iz SAD.

Pritom odbrana Fejsbuka je nazvala ovu vrstu masovne tužbe kao pseudo masovnu tužbu, koja nije „US-Style Class Action“. U odgovoru na to je Šremsov advokat istakao da „korisnici ne moraju da putuju u zemlju, gde ne žive da bi podneli tužbu i da Fejsbuk ne želi da bude tužen. Sama ideja ovog spora je da korisnici (potrošači) mogu da tuže tamo gde imaju boravište“.

Fejsbuk je prebacio Šremsu da on uopšte nije korisnik (potrošač u smislu konzumenta), „pošto nema ni jedne konferencije o zaštiti podataka, gde Šrems nije na podijumu“.¹⁰⁹

106 ROLAND ProzessFinanz AG Fact Sheet http://www.europe-v-facebook.org/sk/rl_fs_de.pdf, 20. 9. 2017.

107 Schon 12.000 Teilnehmer an Sammelklage gegen Facebook, portal futurezone.at, <https://futurezone.at/netzpolitik/schon-12-000-teilnehmer-an-sammelklage-gegen-facebook/78.479.420>, 20. 9. 2017.

108 Barbara Wimmer, *Datenschützer gegen Facebook: Prozess in Wien startet*, <https://futurezone.at/netzpolitik/datenschuetzer-gegen-facebook-prozess-in-wien-startet/123.636.762>, 20. 9. 2017.

109 Barbara Wimmer, *Facebook wirft Schrems „Pseudo-Sammelklage“ vor*, <https://futurezone.at/netzpolitik/facebook-wirft-schrems-pseudo-sammelklage-vor/123.988.333>, 20. 9. 2017.

Taj argument Fejsbuka je Šremsov advokat pobijao troškovima kirije, minimalcem koji Šrems zarađuje, dokazima sa bankovnog računa kao i fejsbuk aktivnostima Maksa Šremsa.

Osnovni sud za građanske sporove u Beču oglosio se da nije mesno nadležan za ovaj spor i odbacio tužbu Maksa Šremsa. Po stanovištu suda mesno nadležan je sud u Irskoj, gde Fejsbuk ima svoje predstavništvo. Pošto se radilo o formalnom procesnom nedostatku, sud u ovom postupku nije uopšte razmatrao pitanja vezana za zaštitu podataka.

Ključna tačka za ovu odluku suda je bila klasifikacija tužioca kao korisnika (potrošača), da bi postojala mogućnost Šremsa da uopšte tuži pred sudom u Beču. Sud je utvrdio da je Šrems privatno koristio Fejsbuk, ali ga nije klasifikovao kao korisnika (potrošača). „Tužilac koristi ogromnu pažnju medija u njegovom postupanju protiv tuženog, takođe i poslovno za prodaju njegovih knjiga i karijeru uopšte“. Pošto Šrems svoj nalog na Fejsbuku koristi i u komercijalne svrhe, ne može važiti kao potrošač. Takođe nije uredno izneto da je mesto nastupanja štete Beč.

Šrems je u reagovanju na presudu rekao da kada neko deluje kao aktivista, onda se on smatra kao firma. Ali isto tako kada nije dokazana nedvosmislena poslovna aktivnost, taj neko se može smatrati potrošačem.¹¹⁰

Na ovu odluku Šrems je uložio žalbu Višem sudu za građanske sporove u Beču. Ovaj sud je dao za pravo Maksu Šremsu većinu njegovih zahteva i odbio prigovore Fejsbuka. Ono što je važno, to je da je sud u drugoj instanci ustanovio da je tuženi može da podnese tužbu pred sudom u Beču, pošto je on potrošač i sme da tuži u svojoj matičnoj državi. U ovoj odluci suda ipak nije bilo reči o tome i ostalo je sporno, da li je učešće ostalih Fejsbuk korisnika u masovnoj tužbi zakonito. Zbog toga su obe strane uložile žalbu i na ovu presudu.¹¹¹

Tako je tužba stigla do Vrhovnog suda Austrije. Vrhovni sud je odlučio da se obrati Evropskom sudu sa sedištem u Luksembugu. Pitanje na koje Evropski sud treba da da odgovor je „Da li jedan potrošač može da tuži u svojoj domovini po prenetom ovlašćenju ostalih potrošača?“. Zavisno od presude mogla bi da bude moguća masovna tužba širom Evrope ili pak samo u određenim zemljama. Kao alternativa stoji mnogo pojedinačnih postupaka u Austriji i drugim zemljama.¹¹²

Evropski sud se ovim pitanjem počeo baviti krajem jula 2017. godine. Do sada još uvek nema sudske presude, ali ni mišljenja glavnog evropskog advokata o ovoj stvari. Činjenica je da se već godinama raspravlja samo o tome, ko je za Fejsbuk mesno nadležan. O stvarnim i suštinskim pitanjima još uvek nije bilo govora. Ova presuda je pored zaštite podataka od izuzetnog značaja za prava zaštite potrošača. U zavisnosti od odgovora na ovo pitanje potrošači će dobiti mogućnost da u svojoj zemlji tuže kompanije.¹¹³

110 Michael Leitner, *Sammelklage gegen Facebook in Wien abgewiesen*, <https://futurezone.at/netzpolitik/sammelklage-gegen-facebook-in-wien-abgewiesen/139.216.192>, 20. 9. 2017.

111 Klage von Max Schrems gegen Facebook in Wien zulässig, portal futurezone.at, <https://futurezone.at/netzpolitik/klage-von-max-schrems-gegen-facebook-in-wien-zulaessig/159.718.863>, 20. 9. 2017.

112 OGH gibt Facebook-Sammelklage an EuGH weiter, portal futurezone.at, <https://futurezone.at/netzpolitik/ogh-gibt-facebook-sammelklage-an-eugh-weiter/220.821.267>, 20. 9. 2017.

113 Facebook-„Datenschutz-Sammelklage“ vor dem EuGH, portal futurezone.at, <https://futurezone.at/netzpolitik/facebook-datenschutz-sammelklage-vor-dem-eugh/275.932.118>, 20. 9. 2017.

3. FEJSBUK I ZAŠTITA PODATAKA

3.1. Uvod

Da bi se adekvatno razumela pravna problematika vezana za Fejsbuk, potrebno je ukazati na razvoj zaštite podataka iz prava privatnosti. Osim toga za sam Fejsbuk je od značaja i tendencija razvoja zakonodavnog okvira EU, pre svega u svetlu primene nove Opšte uredbe o zaštiti podataka.

3.2. Zaštita privatnosti

Zaštita privatnosti predstavlja jedno od najvažnijih osnovnih ljudskih prava. U svetu modernih internet tehnologija može se reći da je ovo pravo u pravom smislu reči ugroženo, iako je proklamovano u ustavima od strane država i garantovano međunarodnim konvencijama kao neprikosnoveno pravo svim građanima. Treba ukazati da u svetu modernih internet tehnologija jedan od najistaknutijih boraca za internet slobodu i osnivač Fondacije za slobodni softver (Free Software Foundation) Ričard Stolmen Fejsbuk naziva „*mašinom za digitalni nadzor ljudi*“.¹¹⁴ Pored već navedenog slučaja Maksa Šremsa, Stolmen navodi i slučaj jednog Irca koji je dobio 2000 stranica sa podacima, koje Fejsbuk ima o njemu. O ovakvoj količini podataka i ugroženosti prava svakog pojedinca na privatnost je i „Staljin mogao samo da sanja“. Ovakvu tvrdnju Stolman je izneo i u pogledu mobilnih telefona nazivajući ih „Staljinov san“.¹¹⁵ Mobilne telefone smatra oruđem „velikog brata“, koji beleže gde ljudi idu i prati ih u svakom momentu. Spas se shodno ovom stručnjaku nalazi u slobodi softvera, koji bi bio besplatan za sve korisnike. Ljudi jednostavno nisu svesni svoje neslobode, pored toga i plaćaju velike sume novca, kako bi dobili bolji softver i bolje performanse.

Kada govorimo o pravu privatnosti uopšte, ono je utemeljeno članom 8 *Evropske konvencije o zaštiti ljudskih prava i osnovnih sloboda* (u daljem tekstu: EKLJP),

114 Richard Stallman, *Facebook je mašina za digitalni nadzor*, sajt B92, http://www.b92.net/tehnopolis/aktuelno.php?yyyy=2012&xmm=06&nav_id=615411, 19. 7. 2012.

115 Stolmen dalje dodaje „Mi danas živimo u svetu u kojem vlade suzbijaju narodne pobune i rade u korist bankara. U Evropi je Mađarska u tome za sada otišla najdalje. Digitalna tehnologija omogućava vlastima povećanje kontrole nad ljudima i nalazimo se na putu koji nije demokratski. Fejsbuk će američkoj vladi dati sve podatke koje ima o nekoj osobi, zahvaljujući licemerno nazvanom zakonu Patriot Act. Zato se moramo odupreti i vladinom i korporativnom nadzoru. Ukratko, Fejsbuk nije vaš prijatelj“, rekao je Stolmen. O grupi Anonymus ovaj stručnjak kaže „Oni se zapravo bave virtuelnim ekvivalentnom uličnih protesta, što ljudima može biti iritantno, isto kao i kada štrajkuju vozači autobusa pa je gradski prevoz zaustavljen. No, tada se uvek treba zapitati — zbog čega vozači štrajkuju? Kod Anonymosa mi se ne sviđa što su nekoliko puta objavili nečiju privatnu komunikaciju“. Richard Stallman, *Mobilni telefoni su Staljinov san*, sajt B92, http://www.b92.net/tehnopolis/vesti.php?yyyy=2011&xmm=03&nav_id=499267, 19. 7. 2012.

koja je usvojena 4. 11. 1950. od strane Saveta Evrope.¹¹⁶ Evropski sud za ljudska prava sa sedištem u Strazburu je utvrdio da se zaštita na osnovu ovog člana odnosi i na komunikaciju putem interneta, e-mail komunikaciju, onlajn praćenje internet komunikacije. Pored ovih oblika zaštite, koje je sud utvrdio, svakako najvažnija je zaštita podataka o ličnosti koja je takođe obuhvaćena ovim članom konvencije.¹¹⁷ Ova zaštita se odnosi na podatke o celokupanom psihičkom i fizičkom integritetu čoveka¹¹⁸ (od zdravstvenog stanja, imena, porekla, seksualne orijentacije do posrednih podataka tzv. potencijalno osetljivih podataka kao što su IP-adrese¹¹⁹ internet korisnika).

Povrede ovog člana predstavljaju mere nadziranja, praćenja internet saobraćaja, kao i čuvanje podataka izvan njihove svrhe prikupljanja.

Na osnovu teksta EKLJP zaštitu zagaranovanih prava dužna je da omogućiti država potpisnica EKLJP.¹²⁰

Mešanje države, odnosno povreda ovog prava, koji inače u državama potpisnicama konvencije ima rang ustavne odredbe i direktno se primenjuje, može se opravdati jedino u slučajevima navedenim u članu 8 stavu 2 EKLJP. To su pre svega interesi nacionalne bezbednosti, zaštite zdravlja. Međutim, treba imati u vidu da ovo pravo državi da se meša u osnovna prava pojedinaca ima i svoje granice. To se pre svega misli na principe i uslove koje je Evropski sud za ljudska prava utvrdio. Da bi se intervencija države u sferi ljudskih prava mogla opravdati, neophodno je slediti sledeće principe:

Princip proporcionalnosti odnosno srazmernosti — Neophodno je postaviti na jednu stranu interese pojedinaca (u ovom slučaju Fejsbuk korisnika) a na drugu stranu javne interese.

Ukoliko je javni interes utvrđen i definisan, dalje treba ispitati

- 1) Da li je *podesno sredstvo* upotrebljeno za zaštitu javnog interesa. Ukoliko vlast izabere sredstvo koje nije pogodno da bi služilo javnom interesu, to ne opravdava mešanje tj. intervenciju države. Samim tim predstavlja povredu člana 8. Ukoliko je i ovaj uslov ispunjen treba ispitati;
- 2) Da li je ovo sredstvo bilo neophodno. *Princip neophodnosti* podrazumeva da li je u slučaju mešanja bilo moguće postići isti cilj odnosno svrhu blažim sredstvom (sredstvom koje bi najmanje moguće ograničilo ovo ljudsko pravo);

116 Član 8 Pravo na poštovanje privatnog i porodičnog života: Svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske; Javne vlasti neće se mešati u vršenje ovog prava sem ako to nije u skladu sa zakonom i neophodno u demokratskom društvu u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala, ili radi zaštite prava i sloboda drugih. *Evropska konvencija o zaštiti ljudskih prava i osnovnih sloboda*, Rim, 4. novembra 1950. http://www.tuzilastvorz.org.rs/html_trz/PROPISI/evr_konvencija_ljudska%20prava_lat.pdf, 26. 6. 2012.

117 *Verfassungsrecht, Recht auf Achtung des Privat- und Familienlebens*, Öhlinger, 8. Auflage, facultas. wuv, 2009. Wien, strane 364 i 365.

118 *Grundzüge des Öffentlichen Rechts, Der Schutz des Privat- und Familienlebens*, Stelzer, LexisNexis ARD Orac, 2005. Wien, strane 152 i 153.

119 Na osnovu IP-adresa se posredno može doći do podataka o internet korisnicima, ukoliko se utvrdi ko stoji iza navedene adrese. Ove adrese predstavljaju pandan broju telefona u telefonskom saobraćaju, koje su dodeljene svakom internet korisniku.

120 Republika Srbija je potpisnica konvencije, kao i mnoge druge države koje nisu članice EU.

- 3) Da li je *sredstvo uporedivo*. Treba isključiti situaciju u kojoj relativno nizak stepen javnog interesa može da dovede do masovnih povreda ljudskih prava.¹²¹

Uvek prilikom procene da li je došlo do povrede osnovnih ljudskih prava treba poći od gore navedenog principa srazmernosti i njegovih uslova.

3.3. Razvoj zaštite podataka

Shodno evropskom shvatanju, zaštita podataka predstavlja osnovno ljudsko pravo, koje zagarantovano ustavom. Ovo pravo je subjektivno pravo, koje svoje osnove ima u ustavu. To znači da se svaki pojedinac može na ovo pravo pozivati i država je u obavezi aktivno da ovo pravo pojedincu omogući.¹²²

Na primeru nemačke sudske prakse može se ukazati na razvoj prava zaštite podataka. *Osnovno ljudsko pravo na zaštitu podataka se razvilo upravo iz prava privatnosti.*

Pravo privatnosti se može podeliti na sledeće oblasti:

1. Zaštita podataka o ličnosti (zaštita podataka);
2. Nepovredivost pošte i telekomunikacija (obuhvata bezbednost sredstava komunikacije kao što su pošta, telefon, e-mejil);¹²³
3. Nepovredivost stana (pretres stana sme se narediti samo na osnovu odluke suda).¹²⁴

Sama zaštita privatnosti se u nemačkom Osnovnom zakonu izvodi iz prava ličnosti.¹²⁵ Od same zaštite prava ličnosti i na osnovu presude Saveznog ustavnog suda Nemačke razvilo se *pravo na informaciono samoodređenje*, koje je temelj modernog prava zaštite podataka.¹²⁶

Obim prava zaštite podataka o ličnosti se značajno razlikuje u odnosu na obim zaštite prava ličnosti tj. konkretno od zaštite privatnosti. Moderne norme o zaštiti podataka nalaze svoju primenu u svakoj automatskoj i neautomatskoj obradi informacija, koja se odnosi na ličnost, čiji je identitet utvrđen ili se može utvrditi.

121 *Grundzüge des Öffentlichen Rechts, Verfassungsrechtliche Rechtfertigung*, Stelzer, LexisNexis ARD Orac, 2005. Wien, strane 148, 149 i 150.

122 Theo Öhlinger, *Verfassungsrecht 8.Auflage*, facultas.wuv, 2009 Wien, Strana 298 red 677.

123 U Nemačkoj je ovo pravo regulisano u Osnovnom zakonu Nemačke čl. 10, http://www.gesetze-im-internet.de/gg/art_10.html i čl. 88 Zakona o telekomunikacijama, http://www.gesetze-im-internet.de/tkg_2004/_88.html i čl. 206 Krivičnog zakona, http://www.gesetze-im-internet.de/stgb/_206.html, 15. 9. 2017.

124 U Nemačkoj je ovo pravo regulisano u Osnovnom zakonu Nemačke čl. 13 http://www.gesetze-im-internet.de/gg/art_13.html, 15. 9. 2017.

125 Pravo ličnosti reguliše nemački Osnovni zakon čl. 2, http://www.gesetze-im-internet.de/gg/art_2.html u vezi sa čl. 1 http://www.gesetze-im-internet.de/gg/art_1.html, Das Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. S. 1), zuletzt geändert durch Artikel 1 des Gesetzes vom 23. 12. 2014 (BGBl. I S. 2438).

126 Presuda iz 1983. godine (Urteil vom 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83), Savezni ustavni sud Nemačke (BVerfG), <https://openjur.de/u/268440.html>, 15. 9. 2017.

Pritom da bi došlo do primene prava zaštite podataka nije neophodna veza sa privatnom sferom pojedinca. Za primenu prava zaštite podataka mora se pokazati veza sa određeni fizičkim licem tj. pojedincem.¹²⁷

Pravo ličnosti štiti samu ličnost pojedinca u njegovim različitim manifestacijama. Nemački Savezni ustavni sud je iz prava ličnosti izvukao:

1. Osnovno pravo na zaštitu tajnosti i integriteta informaciono-tehničkih sistema;¹²⁸
2. Zaštita privatne, tajne i intimne sfere;¹²⁹
3. Pravo na sopstvenu fotografiju;¹³⁰
4. Pravo na izgovorenu reč;¹³¹
5. Pravo na napisanu reč;¹³²
6. Zaštita od uvreda i podmetanja misli i izražavanja;¹³³
7. Pravo lične časti;
8. Pravo na rehabilitaciju;
9. Pravo na dalje zaposlenje u radnim odnosima;
10. Pravo na znanje o svom poreklu.

Upravo razvojem osnovnog ljudskog prava na zaštitu podataka i uvidom u njegovu kompleksnost može se lako uočiti, da ovo pravo sadrži i mnoge elemente drugih osnovnih ljudskih prava. Stoga dolazi često u sukob pre svega sa autorskim pravom, i pravom slobode mišljenja i izražavanja.

3.4. Zaštita podataka i pravo EU

Na nivou Evropske unije, je stupanjem na snagu Ugovora iz Lisabona 1.12.2009. puni zakonski efekat dobila *Povelja Evropske unije o osnovnim pravima* usvojena 18.12.2000. Do usvajanja Lisabonskog ugovora, ovaj pravni dokument je predstavljao običnu političku proklamaciju. Nakon stupanja na snagu Ugovora iz Lisabona, Povelja Evropske unije o osnovnim pravima postaje sastavni deo evropskog prava i samim tim obavezujuća prema svim organima EU (ona ima rang primarnog izvora prava EU). Osim toga to znači takođe i da se svaki građanin EU može direktno pozvati na tekst ove Povelje pred Evropskim sudom sa sedištem u Luksemburgu, kao i pred nacionalnim sudovima država članica.¹³⁴

127 Jan-Hinrik Schmidt/Thilo Weichert, *Datenschutz—Grundlagen, Entwicklungen und Kontroversen*, Bundeszentrale für politische Bildung, Bonn 2012, strane 325 i 326.

128 Presuda iz 2008. godine (Urteil vom 27. Februar 2008 · Az. 1 BvR 595/07, 1 BvR 370/07), Savezni ustavni sud Nemačke (BVerfG), <https://openjur.de/u/59199.html>, 17. 9. 2017.

129 Presuda iz 1980. godine (NJW 1980, 2070 f.), Savezni ustavni sud Nemačke (BVerfG).

130 Presuda 1980. godine (NJW 1980, 34, 238, 246.), Savezni ustavni sud Nemačke (BVerfG).

131 *Ibidem*.

132 *Ibidem*.

133 Presuda 1980. godine (NJW 1980, 34, 269, 282.), Savezni ustavni sud Nemačke (BVerfG).

134 *Vertrag von Lissabon*, <http://www.bmask.gv.at/cms/site/dokument.html?channel=CH0124&doc=CMS1218184665925>, Bundesministerium für Arbeit, Soziales und Konsumentenschutz, 26. 6. 2012.

Za Fejsbuk korisnike je od značaja član 8 Povelje Evropske unije o osnovnim pravima, kojim se reguliše pravo na zaštitu podataka o ličnosti.¹³⁵ Posebno treba istaći stav 2 ovog člana, kojim je *za obradu podataka neophodna predhodna saglasnost* imaoca podataka. To praktično znači da Fejsbuk ne sme ni jednu radnju preduzeti bez predhodne saglasnosti korisnika, koja menja svrhu i cilj na osnovu prvobitno date saglasnosti o obradi podataka.

3.5. Opšta uredba EU o zaštiti podataka

U poglavlju II je bilo govora o *Direktivi o zaštiti podataka Evropske unije* (Direktiva 95/46/EU). Doneta davne 1995. godine, uspeła je do današnjih dana da ostane kamen temeljac zaštite privatnosti internet korisnika. Današnji svet modernih tehnologija je u mnogome promenjen u odnosu na 1995. Danas ne postoji samo jedan centar za zaštitu podataka, već svako od nas poseduje jedan mobilni centar za zaštitu podatka. Na taj način mi možemo kreirati profile na Fejsbuku, razmenjivati bilo koje vrste informacija i podataka putem interneta. Pored toga snimanje podataka se ne odvija samo u jednom centru za zaštitu podataka, već i u institucijama, firmama, na serverima širom sveta kao i sve češće u tzv. ¹³⁶ „oblacima“. ¹³⁷ Da bi ova materija sveobuhvatno bila regulisana doneta je Opšta uredba o zaštiti podataka, kojom je ova materija postala obavezna za sve članice EU i to neposredno.¹³⁸ To znači da sve države članice EU moraju direktno da primenjuju ovaj propis. Za razliku od direktiva, kojom su dati pravni okviri pa su države članice dužne da implementiraju ove propise u skladu sa svojim zakonodavstvom, uredbe na nivou EU se primenjuju kao bilo koji drugi zakoni i predstavljaju zakone EU.

Opšta uredba o zaštiti podataka (Regulation 2016/679) predstavlja ograničenje suvereniteta država članica EU u pogledu zaštite podataka.¹³⁹ Države članice EU

135 Član 8 Zaštita ličnih podataka: 1. Svaka osoba ima pravo na zaštitu ličnih podataka, koji se na nju odnose; 2. Lični podaci moraju se obrađivati pošteno i mogu se koristiti u za to utvrđene svrhe i to na osnovu pristanka osobe koje se tiču ili na nekoj drugoj zakonskoj osnovi. Svako ima pravo na pristup prikupljenim podacima o njemu i pravo na njihovo ispravljanje; 3. Nadzor nad poštovanjem ovih pravila vrši nezavisni organ. *Charta der Grundrechte der Europäischen Union (2000/C 364/01), Povelja Evropske Unije o osnovnim pravima*, Službeni glasnik Evropske Zajednice, http://www.europarl.europa.eu/charter/pdf/text_de.pdf, 26. 6. 2012.

136 Viviane Reding, *Herausforderungen an den Datenschutz bis 2020: Eine europäische Perspektive*, ZD Zeitschrift für Datenschutz, beck.de Zeitschriften, <http://rsw.beck.de/cms/main?docid=321429>, 20. 7. 2012.

137 Računarstvo u oblaku (Cloud Computing) je tehnologija koja je zasnovana na pružanju usluga korisnicima nezavisno od lokacije na kojoj se oni nalaze. Korisnici se pomoću ove usluge mogu priključiti i isključiti sa mreže u bilo kom trenutku i sa bilo kog mesta na svetu. Mogućnosti ove tehnologije idu toliko daleko da korisnici i njihovi podaci upotrebom ove tehnologije dolaze u jurisdikciju različitih zemalja. Ovo predstavlja i rizike po pitanju zaštite podataka i primene prava u ovoj oblasti, pošto se podaci nalaze u tzv. oblaku. *Računarstvo u oblaku*, Iz Vikipedije, slobodne enciklopedije, http://sr.wikipedia.org/wiki/Ra%C4%8Dunarstvo_u_oblaku, 22. 7. 2012.

138 *Reding stellt EU-Datenschutzreform vor*, Falk Lücke, heise online, <http://www.heise.de/newsticker/meldung/Reding-stellt-EU-Datenschutzreform-vor-1421418.html>, 20. 7. 2012.

139 Andreas Wilkens, *Debatte über europäisches Datenschutzrecht geht weiter*, heise online, <http://www.heise.de/newsticker/meldung/Debatte-ueber-europaeisches-Datenschutzrecht-geht-weiter-1621939.html>, 20. 7. 2012.

više nemaju kao u slučaju direktiva okvire koje će slediti, već direktno primenjuju odredbe ove uredbe. Na ovaj način se postigla veća pravna sigurnost ali i bolja zaštita osnovnih ljudskih prava.¹⁴⁰ Iako je uredba usvojena i stupila na snagu, njena primena je odložena za 25.05.2018. godine (čl. 94 st. 1 Uredbe o zaštiti podataka; Regulation 2016/679).

Jedan od osnovnih ciljeva donošenja Opšte uredbe o zaštiti podataka bila je usaglašenost ove pravne materije na nivu EU kao i zalaganje za primenu već postojećih propisa u ovoj pravnoj materiji (tačka 3 uvodnog razmatranja Uredbe o zaštiti podataka; Regulation 2016/679). Osim toga postavljanje novih pravnih mehanizama i standarda na osnovu člana 16 B Ugovora iz Lisabona¹⁴¹ kao i već pomenutog člana 8 Povelje Evropske Unije o osnovnim pravima. Naglašena je i dobra pravna osnova već utvrđena Direktivom iz 1995 godine.¹⁴² Posebno se naglašava da međunarodni sporazumi koje EU potpiše sa trećim zemljama¹⁴³ moraju imati standarde vezane za zaštitu podatka koje sadrži Opšta uredba.¹⁴⁴

Treba istaći da uredba sadrži čak 69 tzv. „otvorenih klauzula“. To znači da je ostavljen prostor državama članicama EU da u sopstvenim zakonodavstvima određene teme detaljnije urede. Na taj način se ne može govoriti o potpunom usaglašavanju ove pravne materije na nivou EU. U literaturi se ova uredba naziva „tromom“ zbog velikih manevarskih mogućnosti država članica EU.¹⁴⁵

140 *Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*, Europäische Kommission, Brüssel, den 25. 1. 2012, 3.1.Rechtsgrundlage, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 22. 7. 2012.

141 Član 16 B: 1. Svako ima pravo na zaštitu svojih ličnih podataka; 2. Evropski parlament i Veće, odlučujući u skladu sa redovnim zakonodavnim postupkom, utvrđuju pravila o zaštiti pojedinaca s obzirom na obradu ličnih podataka u institucijama, telima i agencijama Unije kao i u državama članicama kad obavljaju svoje aktivnosti u području primene prava Unije i pravila o slobodnom kretanju takvih podataka. Poštovanje tih pravila podleže nadzoru nezavisnih tela. Pravila usvojena na osnovu ovog člana ne dovode u pitanje posebna pravila utvrđena u članu 25.A Ugovora o Evropskoj uniji. Član 25.A U skladu sa članom 16.B Ugovora o funkcioniranju Evropske unije i odstupajući od njegovog stava 2., Veće usvaja odluku u kojoj se utvrđuju pravila o zaštiti pojedinaca s obzirom na obradu ličnih podataka od strane država članica pri obavljanju aktivnosti u području primene ovog poglavlja i pravila o slobodnom kretanju takvih podataka. Poštovanje tih pravila podleže nadzoru nezavisnih tela. Ugovor iz Lisabona o izmeni ugovora o Evropskoj Uniji i Ugovora o osnivanju Evropske Zajednice, (2007/C 306/01), http://www.mvpep.hr/custompages/static/hrv/files/EUugovori/12007L_Ugovor_iz_Lisabona_hrv.pdf, 22. 7. 2012.

142 *Entschließung des Europäischen Parlaments vom 6. Juli 2011 zum Gesamtkonzept für den Datenschutz in der Europäischen Union*, (2011/2025(INI)), Europäisches Parlament, 1–10 <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&format=XML&language=DE>, 22. 7. 2012.

143 *Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*, Europäische Kommission, Brüssel, den 25. 1. 2012, Artikel 40 Allgemeine Grundsätze der Datenübermittlung, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 24. 7. 2012.

144 *Entschließung des Europäischen Parlaments vom 6. Juli 2011 zum Gesamtkonzept für den Datenschutz in der Europäischen Union*, (2011/2025(INI)), Europäisches Parlament, 45, <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&format=XML&language=DE>, 22. 7. 2012.

145 Lukas Feiler, *Öffnungsklauseln in der Datenschutz-Grundverordnung — Regelungsspielraum des österreichischen Gesetzgebers*, *jusIT* 2016/93, str. 210.

Sa druge strane sam naziv uredbe „Opšta uredba o zaštiti podataka“ je i imao kao jedan od ciljeva da omogući i tzv. sektorske zakone.¹⁴⁶

3.5.1. Nove kategorije podataka

Uredba reguliše i jednu novu kategoriju podataka, koja nije postojala do sada, a to su *biometrijski podaci* (čl. 4 tč. 14 Uredbe o zaštiti podataka; Regulation 2016/679).¹⁴⁷ To su podaci koji omogućavaju psihička, psihološka obeležja kao i elemente ponašanja ljudi, na osnovu kojih se može izvršiti identifikacija. Najvažniji primer u slučaju Fejsbuka je svakako skeniranje lica.¹⁴⁸

Naročiti značaj se daje *posebnim kategorijama podataka* koji se odnose na rasu, etničko poreklo, politička i religiozna uverenja, pripadnost sindikatima, genetske podatke, podatke o zdravlju, seksualnom životu i podatke o osuđenim licima (čl. 9 Opšte uredbe o zaštiti podataka; Regulation 2016/679). Prikupljanje ovih podataka je generalno zabranjeno, osim ukoliko se lice sa ovime izričito saglasi.¹⁴⁹

Pored toga uvodi se i nova zaštita korisnika koja se odnosi pre svega na internet korisnike. Korisnici društvenih mreža, a pre svega Fejsbuka su ovim direktno pogođeni. Naime radi se o tzv. *profilisanju ili pravljenju profila korisnika* na osnovu procena određenih obeležja lica ili analiza korisnika uz pomoć prognoza njihovog poslovnog uspeha, njihove sposobnosti, njihovog boravka, finansijske situacije, zdravstvenog stanja, preferencija, kao i njihovog ponašanja. Naravno i ove podatke je moguće prikupiti uz saglasnost korisnika (čl. 22 Opšte uredbe o zaštiti podataka; Regulation 2016/679).¹⁵⁰

3.5.2. Prava pojedinaca

Novom uredbom insistira se na jačanju prava pojedinaca. Tu su pre svega „*prava na digitalni zaborav*“ odnosno „prava na brisanje podataka“ npr. brisanje

146 Bereit für die EU-Datenschutz-Grundverordnung?, portal new business, <http://www.newbusiness.at/magazin/new-business/nr-4--mai-2017/bereit-fuer-die-eu-datenschutz-grundverordnung>, 20. 10. 2017.

147 Entschließung des Europäischen Parlaments vom 6. Juli 2011 zum Gesamtkonzept für den Datenschutz in der Europäischen Union, (2011/2025(INI)), Europäisches Parlament, 11–23 <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&format=XML&language=DE>, 22. 7. 2012.

148 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Europäische Kommission, Brüssel, den 25. 1. 2012, Artikel 4 Begriffsbestimmungen (11) „biometrische Daten“, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 24. 7. 2012.

149 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Europäische Kommission, Brüssel, den 25. 1. 2012, Vertragsbedingungen Artikel 9, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 24. 7. 2012.

150 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Europäische Kommission, Brüssel, den 25. 1. 2012, Artikel 20 Auf Profiling basierende Maßnahmen, Absätze 1,2,3, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 24. 7. 2012.

Fejsbuk profila na zahtev korisnika (čl. 17 Uredbe o zaštiti podataka; Regulation 2016/679).¹⁵¹ Pojedinci do sada nisu imali uvek osećaj i kontrolu, šta se sa njihovim podacima dešava.¹⁵² Osim toga centralna uloga u zaštiti internet korisnika data je i tzv. Opt-In principu, kojim bi korisnici za njihovu obradu podataka morali da daju izričitu i predhodnu saglasnost kao i da budu obavešteni o svrsi sakupljanja njihovih podataka i to kroz jedan ciklus kojim bi se od početka štitila privatnost korisnika Fejsbuka tzv. princip „*Privacy by design* odnosno *Privacy by default*“ (čl. 25 Opšte uredbe o zaštiti podataka; Regulation 2016/679).¹⁵³ Naglašena komponenta je pristanak pojedinca, koji bi trebalo da bude saglasan sa propisima, samo ukoliko je dat: nedvosmisleno (neophodno je da korisnik bude upoznat sa svim relevantnim činjenicama), slobodan (za konkretan slučaj) kao i da je pristanak učinjen na način da ga korisnik u svakom trenutku može opozvati (čl. 7 Opšte uredbe o zaštiti podataka; Regulation 2016/679). Prećutno odobrenje ne predstavlja saglasnost u ovom pogledu, pa se ne može tako ni posmatrati.¹⁵⁴ Pristanak odnosno odobrenje treba da se odnosi na sve svrhe odnosno ciljeve, koji se preduzimaju u toku postupka obrade podataka.

Važna odredba se pritom odnosi i na *izmenu opštih uslova (politike privatnosti) poslovanja*. U tom slučaju neophodno je dobiti ponovnu saglasnost korisnika (čl. 6 st. 4 Opšte uredbe o zaštiti podataka; Regulation 2016/679). U slučaju Fejsbuka bi to značilo da pri svakoj pomeni politike privatnosti na ovoj društvenoj mreži mora stajati jasno uočljivo i razumljivo obaveštenje o tome, kao i mogućnost da korisnici odustanu od daljeg korišćenja Fejsbuka.¹⁵⁵

Poseban značaj tom prilikom se daje i onlajn reklamiranju u ovom pogledu. Naime, ističe se neophodnost da korisnik pristane na gore naveden način. Isto tako se zahteva pristanak i u pogledu „kolačića“ u svrhu reklamiranja.¹⁵⁶

Jačanjem transparentnosti i ukazivanjem korisnicima na njihova prava, jačaju se prava pojedinaca u pogledu kontrole njihovih podataka. Informacije treba da budu jasne, lako razumljive običnim korisnicima, kao i pristupačne (čl. 12 Opšte uredbe o zaštiti podataka; Regulation 2016/679). Upravo jačanjem svesti putem pristupa podacima, mogućnosti njihovog brisanja, ispravljanja, blokiranja, postiže se gore navedeni princip „prava na digitalni zaborav“. Korisnici takođe imaju mogućnost da ovo garantovano pravo dobiju bez ikakve naknade. Uz ovo svakako je veoma bitno da se korisnici informišu i da znaju u svakom trenutku kod koga, kako i za koju svrhu se obrađuju i snimaju njihovi podaci i na koji period se vrši obrada i snimanje podataka.

151 *EU-Datenschutzverordnung geleakt*, futurezone, futurezone.at, <http://futurezone.at/netzpolitik/6273-eu-datenschutzverordnung-geleakt.php>, 20. 7. 2012.

152 *Datenschutzverordnung soll EU-Bürgern mehr Kontrolle geben*, Zeit Online, Datenschutz, <http://www.zeit.de/digital/datenschutz/2012-01/eu-datenschutzverordnung-reading>, 20. 7. 2012.

153 *EU-Kommissarin gegen Facebook & Co.*, futurezone, futurezone.at, <http://futurezone.at/netzpolitik/2289-eu-kommissarin-gegen-facebook-amp-co.php>, 22. 7. 2012.

154 *Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*, Europäische Kommission, Brüssel, den 25. 1. 2012, 25, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 22. 7. 2012.

155 *Ibidem*.

156 Više o ovome u poglavlju II kao i u nastavku ovog poglavlja.

Uredbom je regulisano da korisnici dobijaju informacije o tome ko je odgovoran za obradu podataka, kao i kontakt podatke odgovornih lica i svrhu prikupljanja njihovih podataka uključujući i opšte uslove poslovanja odnosno politiku privatnosti, na koji period se snimaju podaci korisnika, postojanje prava korisnika na brisanje, ispravku odnosno informisanje uopšte, kontakt podatke nadležne nadzorne institucije za sprovođenje zaštite podataka, podatke o tome da li se podaci korisnika šalju u tzv. treće zemlje (čl. 13 i 14 Opšte uredbe o zaštiti podataka; Regulation 2016/679).¹⁵⁷ Ovo predstavlja minimalni standard, koji mora da ispuni svaka firma ili institucija koja se bavi obradom podataka.

Ukoliko korisnici podnesu zahtev za dobijanje informacija o njihovim podacima, firme odnosno državne institucije su dužne da najkasnije *u roku od mesec dana od dana podnošenja zahteva, saopšte tražene informacije korisnicima* (čl. 12 st. 3 Opšte uredbe o zaštiti podataka; Regulation 2016/679). Ovaj rok se maksimalno može produžiti na još mesec dana, ukoliko bi to bilo neophodno da se izbegnu ne-srazmerni troškovi odgovornih lica za obradu podataka. Informacije o korisnicima se dostavljaju u pismenoj ili elektronskoj formi.¹⁵⁸

Bitan element u jačanju prava pojedinaca je i „*pravo na prenosivost podataka*“ (čl. 20 Opšte uredbe o zaštiti podataka; Regulation 2016/679). Ovim pravom bi se omogućilo korisnicima da slično upotrebi mobilnih telefona, prenesu svoje podatke drugom ponudocu usluga. U slučaju Fejsbuka bi to bilo npr. ako bi korisnik želeo da svoje podatke sa Fejsbuka prenese na Gugl + ili bilo koju drugu društvenu mrežu.¹⁵⁹ Da bi se ovo pravo bolje ostvarivalo predviđeno je i da korisnici mogu zahtevati da im se njihovi podaci dostave strukturisani u elektronskom formatu.¹⁶⁰ Treba imati u vidu da svi navedeni principi treba da budu u skladu sa već spomenutim principom srazmernosti.¹⁶¹

Korisnici moraju biti informisani o svakoj *zloupotrebi njihovih podataka kao i svakoj pretnji po sigurnost podataka* (čl. 34 Opšte uredbe o zaštiti podataka; Regulation 2016/679).

157 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Europäische Kommission, Brüssel, den 25. 1. 2012, Artikel 14 Information der betroffenen Person, Absatz 1. und 2., http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 24. 7. 2012.

158 *Ibidem*.

159 Evropa: Veća zaštita ličnih podataka na vebu, Izvor: Tanjug, sajt Večernje Novosti online, <http://www.novosti.rs/vesti/naslovna/aktuelno.236.html:363817-Evropa-Veca-zastita-licnih-podatakana-vebu>, 20. 7. 2012.

160 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Europäische Kommission, Brüssel, den 25. 1. 2012, 3.4.3.3. Abschnitt 3—Berichtigung und Löschung, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 22. 7. 2012.

161 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Europäische Kommission, Brüssel, den 25. 1. 2012, 30, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 22. 7. 2012.

Prava pojedinca	
Opšta uredba o zaštiti podataka	Obaveze Fejsbuka
Član 6 stav 4	Obavezna saglasnost pri izmeni opštih uslova poslovanja odnosno politike privatnosti Fejsbuka
Član 12 stav 3	Ostvarivanje prava pojedinaca u predviđenim rokovima
Članovi 12, 13 i 14	Transparentnost informisanja korisnika Fejsbuka
Član 15	Dobijanje informacija o obradi podataka na zahtev korisnika
Član 16	Ispravljanje podataka na zahtev korisnika
Član 17	Brisanje podataka i digitalni zaborav (npr. brisanje Fejsbuk profila) na zahtev korisnika
Član 20	Prenosivost podataka sa Fejsbuka na drugu društvenu mrežu npr. na Gugl + na zahtev korisnika
Član 21	Prigovor na dalju obradu podataka Fejsbuka (po osnovu marketinga)
Član 22	Prigovor na dalju obradu podataka u svrhu pravljanja profila od strane Fejsbuka
Član 34	Informisanje korisnika o zloupotrebi Fejsbuk profila (npr. hakovanje, krađa identiteta, upad na profil itd.)

3.5.3. Odgovornost firmi

U načelu odgovornost za Fejsbuk i ostale firme koje posluju u EU regulisana je članom 5 Opšte uredbe o zaštiti podataka (Regulation 2016/679). Radi se o tzv. *društvenoj odgovornosti* „eng. *accountability*“, koja se ogleda u pridržavanju Opšte uredbe o zaštiti podataka, koje firme moraju da dokažu (čl. 5 st. 2 Opšte uredbe o zaštiti podataka; Regulation 2016/679). Firme moraju biti u stanju da dokažu poštovanje opštih principa iz uredbe.

Opšti principi zaštite podataka shodno uredbi su (čl. 5 st. 1 Opšte uredbe o zaštiti podataka; Regulation 2016/679):

- 1) *Zakovitost* obrade podataka, *fer obrada* podataka, *transparentnost* u obradi podataka;
- 2) *Ograničenje svrhe obrade podataka* na konkrentu obradu;
- 3) *Minimizacija podataka* (smanjenje količine podataka na neophodno potrebnu);
- 4) *Tačnost podataka* (podaci koji se obrađuju moraju biti tačni, u suprotnom ih treba ispraviti ili obrisati);

- 5) *Ograničenje čuvanja podataka* (podaci se smeju čuvati radi identifikacije pojedinaca onoliko dugo, koliko to zahteva svrha njihove obrade);
- 6) *Integritet i poverljivost podataka* (odnosi se na upotrebu tehničkih i organizacionih mera u cilju sprečavanja kompromitacije podataka).

Jačanje sprovođenja i primene prava u oblasti zaštite podataka omogućava se uvođenjem *poverenika za zaštitu podataka u okviru firme*. Ovu funkciju moraće da uvedu firme čija je osnovna delatnost bazirana shodno vrsti, obimu i svrsi na redovnom i sistematskom praćenju lica. Osim toga takođe će poverenika za zaštitu podataka morati da imenuju i one firme, koje obrađuju tzv. posebne kategorije podataka i podatke o krivičnim delima (čl. 37 Opšte uredbe o zaštiti podataka; Regulation 2016/679). Posebne kategorije podataka predstavljaju podaci o koji se odnose na rasu, etničko poreklo, politička i religiozna uverenja, pripadnost sindikatima, genetske podatke, podatke o zdravlju, seksualnom životu i podatke o osuđenim licima (čl. 9 Opšte uredbe o zaštiti podataka; Regulation 2016/679). Stoga se može zaključiti lako da Fejsbuk ove podatke obrađuje, pa je stoga u obavezi da imenuje poverenika za zaštitu podataka.

Državne institucije će morati da angažuju poverenika za zaštitu podataka (čl. 37 st. 1 a) Opšte uredbe o zaštiti podataka; Regulation 2016/679). Ovo se ne odnosi na sudsku vlast, koja nije u obavezi da ima ovu funkciju. Poverenik za zaštitu podataka se stara na nivu firme o sprovođenju propisa iz oblasti zaštite podataka.¹⁶² Naglašava se uloga ove funkcije u podizanju svesti pre svega rukovodećih struktura preduzeća u pogledu zaštite podataka i insistira se na njihovoj samostalnosti u delovanju.¹⁶³ Sprovođenjem i primenom prava postiže se veće poverenje korisnika.¹⁶⁴ Da bi se poverenje postiglo neophodno je uspostaviti funkcionalno zakonodavstvo, nezavisne institucije u primeni prava, kao i odgovornu politiku preduzeća prema korisnicima.

Obaveza vođenja dokumentacije o obradi podataka korisnika, obaveštenje nadležnih organa o bezbednosti podataka korisnika, konsultacije sa nadzornim institucijama i određivanje poverenika za zaštitu podataka na nivou firme doprinosi

162 Viviane Reding, Herausforderungen an den Datenschutz bis 2020: Eine europäische Perspektive, ZD Zeitschrift für Datenschutz, beck online Zeitschriften, <http://rsw.beck.de/cms/main?docid=321429>, 25. 7. 2012.

163 *Opinion of the European Data Protection Supervisor on the data protection reform package*, The European Data Protection Supervisor Peter Hustinx, Done in Brussels, 7 March 2012, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf, 1. 8. 2012.

164 U Nemačkoj već postoji ova institucija. Tamo su međutim u obavezi sve firme da imenuju poverenika za zaštitu podataka. Kao glavni zadatak poverenika se navodi kontrola zaštite podataka kao i rizika u zaštiti prava zaposlenih (član 4d VI 1 Saveznog zakona o zaštiti podataka). Insistira se i na nezavisnosti poverenika, čije odluke mogu biti u suprotnosti sa stavovima rukovodećih struktura preduzeća (član 4f III 2 Saveznog zakona o zaštiti podataka). Da bi se ostvarila maksimalna zaštita i nezavisnost poverenika, uvedena je i apsolutna zaštita od otkaza. Poverenik se može razrešiti dužnosti, samo iz važnih razloga (izričito navedenih u zakonu). Betrieblicher Datenschutzbeauftragter — Welche Rechte und Pflichten hat er?, Datenschutzbeauftragter INFO Informationen zum Datenschutz, zvanični sajt nemačkog poverenika za zaštitu informacija i podataka, <http://www.datenschutzbeauftragter-info.de/betrieblicher-datenschutzbeauftragter-welche-rechte-und-pflichten-hat-er/>, 3. 8. 2012.

svakako u punoj meri zaštititi podataka korisnika.¹⁶⁵ *Obaveza vođenja dokumentacije o obradi podataka* važi za firme koje imaju više od 250 zaposlenih (čl. 30 Opšte uredbe o zaštiti podataka; Regulation 2016/679). To bi praktično značilo da firme sa manjim brojem zaposlenih ne treba da vode toliko računa o zaštiti podataka kao velike firme, što takođe nije tačno. Obaveza vođenja dokumentacije postoji i za one firme ukoliko postoji visok rizik za pojedince pri obradi podataka. Takođe ova obaveza se odnosi i na firme koje konstantno obrađuju podatke pojedinaca. Dokumentaciju o obradi podataka su u obavezi da vode i firme koje obrađuju tzv. posebne kategorije podataka (čl. 9 Opšte uredbe o zaštiti podataka; Regulation 2016/679) ili podatke o krivičnim delima (čl. 10 Opšte uredbe o zaštiti podataka; Regulation 2016/679). Jasno je da Fejsbuk mora da ispuni i ovu obavezu.

Fejsbuk mora konstantno da procenjuje rizik po privatnost korisnika, a naročito pri upotrebi novih tehnologija (čl. 35 Opšte uredbe o zaštiti podataka; Regulation 2016/679). Izuzetno je značajna obaveza za Fejsbuk u vezi sa zaštitom prava pojedinaca. Ova obaveza se odnosi na *procenu uticaja na zaštitu podataka Fejsbuk korisnika* npr. pri inicijalnoj obradi naročito osetljivih podataka — slika, podataka o verskoj, seksualnoj pripadnosti itd., ali i pri pravljenju profila Fejsbuk korisnika.

Obaveza za Fejsbuk je i da pruži neophodna obavještenja u slučaju pristupa podacima korisnika od strane neovlašćenih lica „*data breach notification*“. Bez odlaganja od trenutka saznanja Fejsbuk je dužan da *obavesti korisnike o povredi prava zaštite podataka* (čl. 34 st. 1 Opšte uredbe o zaštiti podataka; Regulation 2016/679).¹⁶⁶ Na ovaj način korisnici imaju mogućnost da efektivno spreče gubitak njihovih podataka u najbržem mogućem roku.¹⁶⁷

Osim obavještenja korisnika predviđen je i rok za *obavještenje nadzornih institucija* prilikom zloupotrebe podataka. Taj rok iznosi 72 časa od događaja (čl. 33 st. 1 Opšta uredbe o zaštiti podataka; Regulation 2016/679).

Od izuzetnog značaja za korisnike Fejsbuka je i obaveza ukazivanja o nivou zaštite, u tzv. trećim zemljama (zemljama van EU). Time je Fejsbuk obavezan da dostavlja informacije korisnicima, na kom nivou zaštite podataka se nalaze npr. SAD, ukoliko bi se podaci slali u SAD. Svaka firma koja ima predstavništvo u EU, mora da se pridržava i posluje u skladu sa ovim propisom. Ovo je i do sada bilo regulisano, međutim novina je da će se ova uredba odnositi i na firme koje nemaju predstavništvo u EU, ako se radi o licima koja su u EU. Neophodno je da ove firme

165 *Opinion of the European Data Protection Supervisor on the data protection reform package*, The European Data Protection Supervisor Peter Hustinx, Done in Brussels, 7 March 2012, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf, 1. 8. 2012.

166 *Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*, Europäische Kommission, Brüssel, den 25. 1. 2012, Artikel 31 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 24. 7. 2012.

167 Carsten Ulbricht, *Datenleck bei SchülerVZ und die datenschutzrechtliche Meldepflicht Web 2.0, Social Media & Recht, Datenleck bei SchülerVZ und die datenschutzrechtliche Meldepflicht*, <http://www.rechtzweinull.de/index.php?/archives/143-Datenleck-bei-SchuelerVZ-und-die-datenschutzrechtliche-Meldepflicht.html#extended>, 3. 8. 2012.

nude usluge ili robu unutar granica EU (čl. 3 st. 2 Opšte uredbe o zaštiti podataka; Regulation 2016/679).¹⁶⁸ Firme čije se sedište nalazi van EU dužne su da imenuju zastupnika za zaštitu podataka (čl. 4 tč. 17 Opšte uredbe o zaštiti podataka; Regulation 2016/679). Ovo ne važi za firme koje neobrađuju tzv. posebne kategorije podataka i podatke o krivičnim delima, koje imaju povećani rizik pri obradi podataka, kao i na institucije drugih zemalja (čl. 27 st. 2 Opšte uredbe o zaštiti podataka; Regulation 2016/679).¹⁶⁹

Neophodno je da firme van EU imaju odgovarajući stepen zaštite podataka, koji utvrđuje Evropska komisija. Tom prilikom Komisija uzima u obzir:

- 1) Vladavinu prava u određenoj zemlji, a u tom pogledu stanje sigurnosti javnog poredka, odbrane, nacionalne bezbednosti kao i postojanje odnosno sprovođenje administrativnih i žalbenih postupaka prema građanima EU;
- 2) Postojanje nezavisnih nadzornih tela za zaštitu podataka i pridržavanja standarda zaštite podataka, kao i njihova saradnja sa EU.

Pošto ove činjenice utvrdi, Komisija objavljuje listu tj. spisak zemalja, koje ispunjavaju „odgovarajući stepen zaštite podataka“.¹⁷⁰ Za Fejsbuk je u ovom slučaju merodavan sporazum Privacy Shield.

Obaveze Fejsbuka	
Opšta uredba o zaštiti podataka	Odgovornost Fejsbuka
Član 5	Poštovanje osnovnih principa zaštite podataka od Fejsbuka: <ul style="list-style-type: none"> — Zakonitost obrade podataka, fer obrada podataka, transparentnost u obradi podataka; — Ograničenje svrhe obrade podataka na konkretnu obradu; — Minimizacija podataka (smanjenje količine podataka na neophodno potrebnu); — Tačnost podataka (podaci koji se obrađuju moraju biti tačni, u suprotnom ih treba ispraviti ili obrisati);

168 *Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*, Europäische Kommission, Brüssel, den 25. 1. 2012, Artikel 3, Räumlicher Anwendungsbereich, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 24. 7. 2012.

169 *Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*, Europäische Kommission, Brüssel, den 25. 1. 2012, Artikel 25 Vertreter von nicht in der Union niedergelassenen für die Verarbeitung Verantwortlichen, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 24. 7. 2012.

170 *Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)*, Europäische Kommission, Brüssel, den 25. 1. 2012, Artikel 41 Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 24. 7. 2012.

Obaveze Fejsbuka	
Član 5	— Ograničenje čuvanja podataka (podaci se smeju čuvati radi identifikacije pojedinaca onoliko dugo, koliko to zahteva svrha njihove obrade); — Integritet i poverljivost podataka (odnosi se na upotrebu tehničkih i organizacionih mera u cilju sprečavanja kompromitacije podataka).
Član 30	Vođenje dokumentacije o obradi podataka Fejsbuk korisnika
Član 32	Obavezno preduzimanje tehničkih i organizacionih mera da bi se zaštitili podaci Fejsbuk korisnika
Članovi 33 i 34	Informisanje nadležnih institucija i Fejsbuk korisnika o zloupotrebi profila (npr. hakovanje, krađa identiteta, upad na profil itd.)
Član 35	Procena uticaja na zaštitu podataka Fejsbuk korisnika (npr. pri obradi naročito osetljivih podataka)
Član 37	Obavezno angažovanje Poverenika za zaštitu podataka, koji će se starati o zahtevima Fejsbuk korisnika

3.5.4. Kazne

Uredbom su predviđene *kazne samo za firme*, pošto jedna od tzv. „otvorenih klauzula“ predviđa mogućnost da države članice EU predvide kažnjavanje državnih institucija, ali ne i obavezu (čl. 83 st. 7 Opšte uredbe o zaštiti podataka; Regulation 2016/679).

Fejsbuk može biti kažnjen na sledeće načine:

- 1) Kazna u iznosu od *4% godišnjeg prometa firme ili do maksimalno 20 miliona evra*, ukoliko ne dostavlja korisnicima informacije, ukoliko to ne učini u odgovarajućem formatu kao i ukoliko zahteva naknadu za pružanje ovih informacija (čl. 12 u vezi sa čl. 83 st. 5 b Opšte uredbe o zaštiti podataka; Regulation 2016/679).
- 2) Propisana je takođe kazna u iznosu od *4% godišnjeg prometa firme ili do maksimalno 20 miliona evra*, ukoliko ne da informacije na transparentan, razumljiv i pristupačan način, ne pouči korisnike o pravnim mogućnostima za ostvarenje njihovih prava na zaštitu podataka i ne odgovori na zahtev korisnika podataka, čiji se podaci obrađuju.
- 3) Kazna od *4% godišnjeg prometa firme ili do maksimalno 20 miliona evra* odnosi se i na uskraćivanje podataka o svrsi njihovog prikupljanja, trajanju snimanja podataka, kategoriji podataka, pravu na ispravljanje, brisanje, mogućnostima ulaganja žalbe itd. Identičan procenat je predviđen i za postupanje suprotno „pravu na digitalni zaborav“.

- 4) Identična kazna primeniće se ukoliko se ne poštuju propisi u pogledu saglasnosti korisnika na obradu podataka kao i u pogledu zaštite posebnih kategorija podataka i u pogledu uskraćivanja prava korisnika da svoj pristanak na obradu podataka opozovu.¹⁷¹ Identična kazna je predviđena i za pravljenje profila korisnika, koji je u suprotnosti sa uredbom.¹⁷²
- 5) Identična kazna primeniće se za ne pridržavanje odredbi koje se odnose na slanje podataka u treće zemlje.¹⁷³ Ovo važi svakako i za sve ostale firme van EU koje žele da obrađuju podatke EU građana.¹⁷⁴ Na taj način se izbegava dosadašnji pravni vakum i jasno stavlja do znanja firmama koje posluju van EU, a obrađuju podatke građana EU da će morati da se pridržavaju propisa EU.¹⁷⁵

Fejsbuk može blaže biti kažnjen u iznosu od *2% godišnjeg prometa firme ili do maksimalno 10 miliona evra*, ukoliko ne imenuje zastupnika u EU, ne poštuje propise o sigurnosti i tehničkoj podršci zaštite podataka, ne imenuje poverenika za zaštitu podataka na nivou firme (čl. 83 st. 4 Opšte uredbe o zaštiti podataka; Regulation 2016/679).

Uzimajući u obzir **visine kazne za Fejsbuk mogu se izreći dve vrste:**

1. 4% godišnjeg prometa firme ili do maksimalno 20 miliona evra
 Obračun:
Fejsbuk godišnji promet u 2016.godini: oko 22, 51 milijarde evra
4% od 22, 51 milijarde evra = 900,400,000 evra
Zaključak: Fejsbuk se može kazniti maksimalno do 900,400,000 evra
2. 2% godišnjeg prometa firme ili do maksimalno 10 miliona evra
 Obračun:
Fejsbuk godišnji promet u 2016.godini: oko 22, 51 milijarde evra
2% od 22, 51 milijarde evra = 450,200,000 evra
Zaključak: Fejsbuk se može kazniti maksimalno do 450,200,000 evra

Tabela pokazuje u kojim slučajevima se Fejsbuk može kazniti i po kom osnovu

171 Videti u nastavku. To su podaci koji se odnose na rasu, etničko poreklo, politička i religiozna uverenja, pripadnost sindikatima, genetski podaci, podacima o zdravlju, seksualnom životu i podaci o osuđenim licima.

172 Videti u nastavku. Profilisanje se vrši na osnovu procena određenih obeležja lica ili analiza lica uz pomoć prognoza njihovog poslovnog uspeha, njihove sposobnosti, njihovog boravka, finansijske situacije, zdravstvenog stanja, preferencija, kao i njihovog ponašanja.

173 Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), Europäische Kommission, Brüssel, den 25. 1. 2012, Artikel 79 Verwaltungsrechtliche Sanktionen, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf, 24. 7. 2012.

174 EU-Kommissarin gegen Facebook & Co., futurezone, futurezone.at, <http://futurezone.at/netzpolitik/2289-eu-kommissarin-gegen-facebook-amp-co.php#userkommentare>, 20. 7. 2012.

175 EU will „Recht auf Vergessen“ im Internet, APA, futurezone.at, <http://futurezone.at/netzpolitik/5823-eu-will-recht-auf-vergessen-im-internet.php>, 20. 7. 2012.

Moguće kazne za Fejsbuk	
Ne pridržavanje Uredbe o zaštiti podataka	Član 83 stavovi 4 i 5 Opšte uredbe o zaštiti podataka
Član 5 Obavezna poštovanja opštih principa zaštite podataka	Max. 900,400,000 €
Član 6 stav 4 Obavezna saglasnost pri izmeni opštih uslova poslovanja	Max. 900,400,000 €
Članovi 12, 13 i 14 Transparentnost informisanja korisnika Fejsbuka	Max. 900,400,000 €
Član 12 stav 3 Ostvarivanje prava pojedinaca u predviđenim rokovima	Max. 900,400,000 €
Član 15 Dobijanje informacija o obradi podataka na zahtev korisnika	Max. 900,400,000 €
Član 16 Ispravljanje podataka na zahtev korisnika	Max. 900,400,000 €
Član 17 Brisanje podataka i digitalni zaborav na zahtev korisnika	Max. 900,400,000 €
Član 20 Prenosivost podataka sa Fejsbuka na drugu društvenu mrežu na zahtev korisnika	Max. 900,400,000 €
Član 21 Prigovor na dalju obradu podataka	Max. 900,400,000 €
Član 22 Prigovor na dalju obradu podataka u svrhu profilisanja	Max. 900,400,000 €
Član 30 Vođenje dokumentacije o obradi podataka Fejsbuk korisnika	Max. 450,200,000 €
Član 32 Obavezno preduzimanje tehničkih i organizacionih mera	Max. 450,200,000 €
Članovi 33 i 34 Informisanje nadležnih institucija i Fejsbuk korisnika o zloupotrebi profila	Max. 450,200,000 €
Član 35 Procena uticaja na zaštitu podataka Fejsbuk korisnika	Max. 450,200,000 €

Moguće kazne za Fejsbuk	
Član 37 Obavezno angažovanje Poverenika za zaštitu podataka	Max. 450,200,000 €

3.5.5. Budućnost i ocene Opšte uredbe o zaštiti podataka

Prilikom reagovanja na uredbu pokazalo se da su internet giganti poput Gugla i Fejsbuka i Tvitera veliki protivnici predloženog prava na digitalni zaborav. Oni su istakli da ova odredba predstavlja kršenje prava na slobodu izražavanja, kao i prava na informaciju.¹⁷⁶ Osim toga stručnjaci ukazuju na veoma naivan pristup ovom pravu na tzv. onlajn gumicu,¹⁷⁷ pošto ono ne može tehnički da se sprovede u praksi.¹⁷⁸

Ono što je uočljivo je da je Evropskoj komisiji data odlučujuća uloga u primeni ovog zakona. Tako pored utvrđivanja stepena zaštite podataka van EU, Komisija je dobila mogućnost da reguliše princip *Privacy by Design*.¹⁷⁹

Svakako da uredba predstavlja veliki korak u zaštiti podataka u EU. Ova pravna pravila će ojačati prava pojedinaca i odgovornih lica za zaštitu podataka. Ojačana je i uloga nacionalnih nadzornih organa. Opšti utisak o uredbi je generalno pozitivan. Tako je u svom mišljenju Evropski nadzornik za zaštitu podataka Peter Hustinx istakao prednosti i nedostatke ove uredbe.¹⁸⁰ Naročito je pozitivno ocenjen opšti princip važenja ove uredbe, kojom se teži da ona bude primenljiva za sve članice EU.¹⁸¹ Samim tim što predstavlja pravni akt najveće pravne snage tzv. sekundarnog zakonodavstva EU, neposredno će uredba važiti u svim državama članicama i na taj način obrazovati jedinstvenu obavezu za sve države članice EU.¹⁸²

Uredbu obeležavaju definicije i pojmovi koji su u mnogobrojnim slučajevima neodređeni i neprecizni, što može dovesti do teškoća u primeni.¹⁸³ Velike pohva-

176 Facebook, Google i Twitter protiv „prava na zaborav“, Izvor: Tanjug, sajt Večernje Novosti online, <http://www.novosti.rs/vesti/naslovna/aktuelno.236.html:376012-Facebook-Google-i-Twitter-protiv-quotprava-na-zaboravquot>, 25. 7. 2012.

177 Jyn Schultze-Melling, Ein Datenschutzrecht für Europa — eine schöne Utopie oder irgendwann ein gelungenes europäisches Experiment?, ZD Zeitschrift für Datenschutz, beck online Zeitschriften, <http://rsw.beck.de/cms/main?docid=321429>, 25. 7. 2012.

178 Jo Bager, EU-Kommissarin Reding bekräftigt einheitlichen EU-Datenschutz, heise online, <http://www.heise.de/newsticker/meldung/EU-Kommissarin-Reding-bekraeftigt-einheitlichen-EU-Datenschutz-1432964.html>, 25. 7. 2012.

179 EU-Datenschutzreform: Der Teufel steckt im Detail, Falk Lücke, heise online, <http://www.heise.de/newsticker/meldung/EU-Datenschutzreform-Der-Teufel-steckt-im-Detail-1422742.html>, 25. 7. 2012.

180 *Opinion of the European Data Protection Supervisor on the data protection reform package*, The European Data Protection Supervisor Peter Hustinx, Done in Brussels, 7 March 2012, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf, 1. 8. 2012.

181 *Ibidem*.

182 *Ibidem*.

183 *Ibidem*.

le su namenjene jačanju prava pojedinaca na njihovu zaštitu podataka putem veće transparentnosti, prava na prigovor, prava na zaborav, prava na prenosivost podataka, jačanja uloge nacionalnih nadzornih tela, kao i obaveza odgovornih lica za zaštitu podataka na usklađenost sa ovom uredbom i jačanju mehanizama za sprovođenje ovih propisa.¹⁸⁴ Istaknuta je sprovodljivost prava na digitalni zaborav od strane odgovornih lica za zaštitu podataka (Fejsbuk je pravi primer odgovornog lica). Na osnovu Uredbe brisanje podataka na zahtev korisnika ne sastoji se samo u preduzimanju radnji koje vode ka tome, već se očekuje i rezultat tj. stvarno brisanje podataka. Uloga odgovornih lica je dobila na značaju i kroz čitav niz mehanizama ostvarivanja prava na zaštitu podataka.

Evropskoj komisiji je data prevelika uloga u pogledu odobrenja za prenos podataka van EU. Pored toga uloga Komisije je data u formulisanju pojedinih standarda kao npr. u pogledu definicija.¹⁸⁵

Što se tiče sankcija koje su zaprećene odgovornim licima za obradu podataka postoje izvesne nejasnoće. Naime postavlja se pitanje, šta će se desiti ukoliko npr. Fejsbuk delimično obriše podatke, da li će takva radnja predstavljati osnov za kažnjavanje? Na ovakva pitanja predložena uredba ne daje jasne i nedvosmislene odgovore.¹⁸⁶

Za Fejsbuk će biti od značaja i donošenje *Uredbe E-Privacy*, koja će zameniti postojeću Direktivu o privatnosti i elektronskim komunikacijama (Directive 2002/58/EC).¹⁸⁷ Na taj način će biti uređena pre svega oblast kolačića, obrade tzv. meta podataka (videti poglavlje 4.4.3. Maks Šrems i tužbe zbog afere „PRIZMA“), aplikacija, što će imati uticaja na Fejsbuk. Očekuje se da Uredba E-Privacy stupi na snagu zajedno sa Opštom uredbom o zaštiti podataka.¹⁸⁸ Treba imati u vidu da će time biti regulisana oblast elektronskih komunikacija kao sektorska uredba u odnosu na Opštu uredbu o zaštiti podataka. Buduća Uredba E-Privacy mora biti u skladu sa Opštom uredbom o zaštiti podataka i predstavlja nadogranju u specifičnoj oblasti elektronskih komunikacija.

184 *Ibidem*.

185 Tako je propisan koncept „Privacy by Design“, ali je sadržina ovog principa ostavljena Komisiji da je definiše. *EU-Datenschutzreform: Der Teufel steckt im Detail*, Falk Lücke, heise online, <http://www.heise.de/newsticker/meldung/EU-Datenschutzreform-Der-Teufel-steckt-im-Detail-1422742.html>, 2. 8. 2012.

186 *Opinion of the European Data Protection Supervisor on the data protection reform package*, The European Data Protection Supervisor Peter Hustinx, 242. I 276, Done in Brussels, 7 March 2012, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf, 1. 8. 2012.

187 Predlog Uredbe E-Privacy, Evropska Komisija, <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0010&rid=1>, 15. 10. 2017.

188 Michael Neuber, *ePrivacy-Verordnung*, Bundesverband Digitale Wirtschaft (BVDW), https://www.iab-austria.at/wp-content/uploads/2017/04/Neuber_ePrivacy-Verordnung-Vortrag-IAB-Austria.pdf, 15. 10. 2017.

3.6. Problemi zaštite podataka na Fejsbuku

3.6.1. Prikupljanje podataka prilikom registracije

Iako većina društvenih mreža zahteva veliku količinu podataka prilikom registracije novih korisnika, pitanje je koliko je to opravdano. Ovako prikupljeni podaci se mogu koristiti ukoliko su neophodni za korišćenje usluga koje pružaju. Kao minimalni standard se prikupljaju šifre i ime korisnika. Međutim, prema mišljenju određenih eksperata u slučaju Fejsbuka ne postoji ugovorni odnos na osnovu koga bi se ovakvi podaci mogli koristiti, pošto se radi o uslugama koje se pružaju bez nadoknade.¹⁸⁹

Pošto Fejsbuk prikuplja i ostale podatke kao što su e-mail adresa, pol, datum rođenja korisnika, za ove podatke neophodno bi bilo da postoji ugovorni odnos korisnika i Fejsbuka. Čini se da bi korišćenje e-mail adresa bilo opravdano, ukoliko bi postojala generalno neophodnost njihovog prikupljanja. To bi bilo u slučaju npr. kada bi Fejsbuk obavestavao korisnike putem e-mejla o tome da njihovi prijatelji žele da podele određene informacije sa njima. Pored toga bili bi opravdani i slučajevi kada dolazi do promena na Fejsbuku, kao sredstvo ukoliko se zaboravi šifra da bi se identifikovao korisnik. Dok za e-mail postoji opravdanje, u slučaju prikupljanja informacija o datumu rođenja, odnosno polu korisnika, deluje da je to potpuno nepotrebno.

Podatke o datumu rođenja Fejsbuk pravda „autentičnosti strana kao i pristupom starim sadržajima“. Svakako da ova formulacija ne predstavlja neophodnost prikupljanja ove vrste ličnih podataka.¹⁹⁰

3.6.2. Saglasnost korisnika da se njihovi podaci obrađuju

I do donošenja Opšte uredbe o zaštiti podataka u većini evropskih zakonodavstava zahtevano je da je za obradu podataka o ličnosti neophodna saglasnost imaoa podataka. Tako i korisnici Fejsbuka treba da daju saglasnost za njihovu obradu i korišćenje, da bi Fejsbuk mogao da ih koristi. Da bi saglasnost bila punovažna, mora biti predhodna i u pismenoj formi po pravilu. U slučaju društvenih mreža čini se kao opravdana i elektronska forma. Međutim ovom formom trebalo bi osigurati da je korisnik dao svoj pristanak na obradu podataka na nedvosmislen i svestan način. Svakako da svest o obradi podataka predstavlja najveći problem prilikom prikupljanja ovih podataka. Nije redak slučaj da korisnici automatski po navici kliknu i na taj način potvrde obradu podataka o njima, a da toga uopšte nisu svesni. Osim toga ovakve izjave o prihvatanju obrade podataka korisnika, da bi opravdale elektronsku formu, moraju imati i jednu vrstu elektronskog zapisa na koji bi korisnici svakog trenutka mogli da pristupe, ali i da svoj pristanak opozovu.

189 Ulrich Wackerbarth, *Datenschutz in sozialen Netzwerken, Seminararbeit, Rechtliche Fallstricke im Internet*, Hubert Mayer, Fernuniversität in Hagen Fachbereich Rechtswissenschaft, strana 5, http://hubert-mayer.de/dateien/Seminararbeit_Datenschutz.pdf, 15. 10. 2017.

190 Početna stranica Fejsbuka <https://www.facebook.com/>.

Veliki problem predstavlja i sam način registracije, pošto se ne može govoriti o svesnosti i nedvosmislenosti pristanka korisnika o obradi njihovih podataka, ukoliko se izjava o saglasnosti ne nalazi u samom tekstu registracije. Tekstu izjave o saglasnosti za obradu podataka kao i uslovima korišćenja Fejsbuka je moguće pristupiti samo ako se klikne na link. Osim toga prilikom registracije u završnoj fazi stoji malim slovima da prilikom pristupanja Fejsbuku korisnici prihvataju politiku o privatnosti kao i uslove korišćenja.¹⁹¹ Sa tim u vezi potrebno bi bilo još jedanput sažeto prikazati na ekranu korisnicima izjavu o korišćenju njihovih podataka, u kojem bi oni nedvosmisleno potvrdili svoju saglasnost. Stoga se može zaključiti da na Fejsbuku svesnost korisnika po ovom pitanju nedostaje.

Kada govorimo o formi i dostupnosti informacija o opštim uslovima korišćenja i informacijama o politici privatnosti, oni su dostupni i registrovanim i ne registrovanim korisnicima na uvid. Međutim treba ukazati da u ovim informacijama ne postoji obaveštenje o izjavi o saglasnosti korisnika kao i mogućnosti njenog opoziva. Ove saglasnosti nema ni u samoj prijavi niti u politici o privatnosti Fejsbuka.¹⁹²

3.6.3. Predlozi prijatelja

Po završetku registracije korisnicima se „pomaže“ u pronalasku prijatelja uz pomoć spomenute Friend Finder opcije.¹⁹³ Na osnovu ove opcije se od kontakta koje Fejsbuku daju Skajp, GMX i ostali, predlažu prijatelji novim korisnicima Fejsbuka. Podaci novog korisnika se upoređuju sa njegovim potencijalnim prijateljima i na taj način predlažu. Taj proces obuhvata i treća lica, koja uopšte nisu ni registrovana na Fejsbuku. Prilikom upoređivanja ukoliko postoji poklapanje sa određenim korisnicima, oni se predlažu novom korisniku. Pored toga budućim korisnicima se šalju pozivnice za priključenje ovoj društvenoj mreži.

Ovi podaci se nikada ne brišu iz baze podataka Fejsbuka, a koriste se u dve svrhe. Prva je da bi se budućim novim članovima na isti način „pomoglo“ u pronalasku prijatelja. Druga je da bi se ovi podaci upoređivali sa ostalim podacima i na taj način u potpunosti omogućila ova opcija.

Prikupljanju podataka na ovakav način takođe se, kao i u predhodnim slučajevima, može prigovoriti da ne postoji predhodni pristanak korisnika na ovu opciju kao ni dovoljno informacija o tome na adekvatan način. Poseban problem ovom prilikom su treća lica koja dobijaju nepoželjnu poštu (eng. spam) u vidu pozivnica za pristup, koju mogu naknadno isključiti. Postavlja se pitanje, kako neko ko ni ne zna, niti želi da pristupi Fejsbuku može uopšte biti obuhvaćen obradom podataka?!¹⁹⁴

191 *Ibidem*.

192 Ulrich Wackerbarth, *Datenschutz in sozialen Netzwerken, Seminararbeit, Rechtliche Fallstricke im Internet*, Hubert Mayer, Fernuniversität in Hagen Fachbereich Rechtswissenschaft, strana 8, http://hubert-mayer.de/dateien/Seminararbeit_Datenschutz.pdf, 15. 10. 2017.

193 Videti poglavlje II.

194 Ulrich Wackerbarth, *Datenschutz in sozialen Netzwerken, Seminararbeit, Rechtliche Fallstricke im Internet*, Hubert Mayer, Fernuniversität in Hagen Fachbereich Rechtswissenschaft, strana 10, http://hubert-mayer.de/dateien/Seminararbeit_Datenschutz.pdf, 15. 10. 2017.

3.6.4. Vidljivost podataka

Ukoliko bilo ko na svetu ukuca na pretraživaču Guglu — Petar Petrović Fejsbuk, dobiće rezultate sa slikom pomenutog lica ali i sa listom njegovih prijatelja. Istim principom je moguće pronaći lica na ovoj društvenoj mreži, koja nisu ni svesna da su dostupna na ovakav način svakom internet korisniku. Ova mogućnost je dostupna dakle i licima koja uopšte nisu korisnici Fejsbuka. Ova lica se pozivaju da pristupe Fejsbuku i postanu prijatelji sa traženom osobom. Naročito su osetljivi podaci ukoliko se na ovaj način dobiju o određenoj osobi koja je npr. pripadnik određene političke partije, sindikata, udruženja, određene veroispovesti. Ukoliko se radi o prijavi za određeni posao, a poslodavac ovo prekontoliše (što nije redak slučaj, već moglo bi se reći pravilo), postoji velika šansa da se iz ovih razloga ostane bez traženog posla, ili da poslodavac odustane od kandidata nezavisno od kvalifikacija kandidata.

Obrada podataka korisnika na ovakav način ne opravdava svrhu njihovog prikupljanja i teško je uopšte kvalifikovati ovakvu vrstu podataka. Informacija o ovakvom načinu obrade podataka kao i pristanka korisnika takođe nema pri registraciji na adekvatan način.¹⁹⁵ Fejsbuk generalno nema obavezu da filtrira protivpravni sadržaj, ako se korisnik saglasio sa upotrebom podataka na ovakav način.¹⁹⁶ To znači da korisnik može računati da će ostali internet korisnici biti u mogućnosti da pristupe njegovim najintimnijim podacima.

Osetljive informacije koje su na ovaj način vidljive kao što su informacije o političkoj i verskoj pripadnosti korisnika shodno važećim evropskim propisima predstavljaju posebno osetljive podatke. Stoga zahtevaju posebnu vrstu saglasnosti za njihovu obradu. Tako da se posebna izjava o korišćenju ove vrste podataka mora pribaviti pre njihove obrade. To svakako nedostaje na ovoj društvenoj mreži.

Poseban problem ovom prilikom predstavlja vidljivost podataka neposredno posle registracije. Naime, svi podaci tek registrovanih korisnika mogu se videti, tako da bilo koji internet korisnik može njima pristupiti. Pravilan pristup bi bio da samo korisnik može da vidi svoje podatke i da on sam odluči sa kim želi da ih подели. Svakako pristup po kojem svi mogu da imaju uvid u podatke korisnika, ne opravdava svrhu i saglasnost većine korisnika. Stoga većina korisnika naknadno zaključava svoje profile i određuje sa kime želi da deli svoje lične podatke.¹⁹⁷ Može se reći da su Fejsbuk korisnici sami administratori svojih profila i organizacionom i u tehničkom smislu, bez svesti i tehničke sposobnosti da održavaju svoje profile.

3.6.5. Korišćenje podataka u reklamne svrhe

Na Fejsbuku se podaci korisnika mogu prikupljati za ciljno reklamiranje, na osnovu njihovih interesovanja. Svakako da i ovaj način obrade podataka mora za-

195 *Ibidem*, str. 12.

196 Thomas Hoeren, *Facebook und Co: Es ist nicht alles Gold, was glänzt, Risiken für Unternehmen und Privatnutzer*, Wissen+Karriere časopis, broj Ausgabe 06/2011 September/Okttober, strana 31.

197 Ulrich Wackerbarth, *Datenschutz in sozialen Netzwerken, Seminararbeit, Rechtliche Fallstricke im Internet*, Hubert Mayer, Fernuniversität in Hagen Fachbereich Rechtswissenschaft, strana 13., http://hubert-mayer.de/dateien/Seminararbeit_Datenschutz.pdf, 13. 12. 2013.

htevati izričitu saglasnost korisnika, kao i mogućnost opozivanja iste. S obzirom da Fejsbuk ne nudi mogućnosti korisnicima da uopšte saznaju, otkazu mogućnost korišćenja njihovih podataka na ovakav način, može se zaključiti da Fejsbuk i po ovom pitanju deluje suprotno osnovnim propisima o zaštiti podataka.¹⁹⁸

Naročito je sporno prikupljanje podataka na osnovu „kolačića“.¹⁹⁹ Pošto se ovaj način prikupljanja podataka korisnika odnosi na tzv. oglašavanje na osnovu ponašanja korisnika (behavioural advertising), kolačići omogućavaju pristup i snimanje podataka korisnika sa njihovih računara i na taj način ciljno reklamiranje. Nije neka novina ako se kaže da je internet danas postao sredstvo pomoću koga ljudi komuniciraju, dele informacije, kupuju, obavljaju administrativne poslove. Mogućnosti praćenja internet saobraćaja i ponašanja korisnika od strane vlasnika veb sajtova se u poslednjih godina drastično povećao.

Federalna trgovinska komisija SAD (Federal Trade Commission) ustanovila je da Fejsbuk oglašivačima dopušta pristup privatnim podacima korisnika. Osim toga Fejsbuk koristi podatke korisnika i nakon brisanja njihovih profila, iako je to uporno negirao. Komisija je takođe istakla „nepravdom i varljivom“ praksu Fejsbuka, pošto je ova firma od 2009. godine privatne podatke korisnika upotrebljavala u javne svrhe bez njihovog znanja i pristanka. Iz Fejsbuka su odlučili da se nagode sa Komisijom i da priznaju povredu prava korisnika. Na osnovu nagodbe Fejsbuk je prihvatio da ne sme pogrešno da predstavi privatnost ili bezbednost podataka na svojoj mreži, te da mora da traži eksplicitno odobravanje korisnika za bilo koju izmenu koju uvedu u vezi privatnosti korisnika. Pored toga dužan je da spreči pristup informacijama korisnika čiji nalog je ugašen u roku od 30 dana, uspostavi i održava sveobuhvatan program privatnosti u roku od 180 dana, kao i da svake dve godine u narednih 20 godina obezbedi nezavisnu kontrolu svog programa privatnosti kako bi se utvrdilo da li poštuje sve ove obaveze Federalne trgovinske komisije SAD. Ukoliko ovu nagodbu ne ispoštuje, Fejsbuk će za svaki prekršaj plaćati 16.000 dolara po danu.²⁰⁰ U praksi na osnovu ove odluke bi Fejsbuk trebalo da svaki put predhodno dobije saglasnost korisnika, ukoliko želi da preda korisničke podatke nekim oglašivačima.²⁰¹

Ove činjenice su naterale i čelnike EU da promene E-Privacy direktivu i na taj način regulišu ovo osetljivo pitanje, koje se ne tiče samo Fejsbuka već i svih internet korisnika.²⁰² Mnogobrojna istraživanja su pokazala da kao i u većini navedenih problema vezanih za zaštitu privatnosti na Fejsbuku, korisnici uopšte nisu svesni niti informisani o ugroženosti njihove privatnosti.²⁰³

198 *Ibidem*, str. 14 i 15.

199 Više o tome u poglavlju II.

200 *FB će morati da poštuje privatnost*, sajt B92, http://www.b92.net/tehnopolis/aktuelno.php?yyyy=2011&mm=11&nav_id=561874, 7. 8. 2012.

201 *Odluka američke Federalne trgovinske komisije, Fejsbuk će morati bolje da štiti privatnost korisnika*, sajt Blica, <http://www.blic.rs/IT/292814/Fejsbuk-ce-morati-bolje-da-stiti-privatnost-korisnika>, 7. 8. 2012.

202 E-Privacy direktiva zamenjena je novom Direktivom 2009/136/EK.

203 *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, 02005/11/EN WP 188, Article 29 Data Protection Working Party, Jacob Kohnstamm, 08 Decembar 2011, strana 3.

Da bi se ovakve informacije prikupile pristanak je takođe obavezan.²⁰⁴ Pored toga što je neophodno da bude jasan i nedvosmislen, mora biti i dat u odgovarajućoj formi. Nije dovoljno da se nalazi negde na veb sajtu, već ova forma mora biti dostupna korisnicima na jednostavan način.²⁰⁵ Pored toga treba jasno korisnicima ukazati da se njihov saobraćaj prati i koji se podaci korisnika snimaju kao i da oni mogu biti upotrebljeni u svrhu ciljnog reklamiranja, na osnovu njihovog ponašanja.²⁰⁶ Korisnici moraju imati mogućnost da izraze svoju predhodnu saglasnost na obradu ove vrste podataka kao i da obradu ovih informacija opozovu.

3.6.6. Prikupljanje podataka na osnovu Social Plugin

Opcijom Social Plugin tj. društvenih dodataka je omogućeno na većini sajtova lajkovanje, deljenje određenog sadržaja koji se korisniku dopada.²⁰⁷ Na taj način oglašivači povezuju korisnike sa društvenom mrežom koja se koristi (Fejsbuk, Gugl +, Tviter) i omogućuju korisnicima da podele određeni interesantan sadržaj sa svojim prijateljima. Pritom se informacije tj. podaci o korisnicima šalju ponudiocima ovih usluga.²⁰⁸ Glavni problem svakako predstavlja nedostatak informacija o ovome i mogućnost korisnika da opozovu odnosno zabrane korišćenje svojih ličnih podataka. Tako primera radi u Nemačkoj, ponudilac ove vrste usluge snosi odgovornost za korišćenje podataka korisnika. Neohodna je izjava o saglasnosti korisnika o obradi njihovih ličnih podataka koja je punovažna, ako su date pouzdane informacije od strane ponudioca usluge kao i svrha prikupljanja podataka na ovaj način.²⁰⁹ Iz ovoga proizlazi da su u ovom slučaju odgovorni ne samo ponudilac ove usluge već i Fejsbuk. Stoga bi mogli solidarno odgovarati za uskraćivanje prava korisnicima na pristanak o obradi njihovih podataka kao i transparentnost u ovom pogledu. Može

204 *Ibidem*, str. 4.

205 Kako se zaštititi od ove vrste praćenja, odlični saveti u vezi sa ovom vrstom prikupljanja podataka mogu se naći na veb sajtu <http://www.youronlinechoices.com/>. Ove informacije mogu biti od koristi ne samo običnim internet korisnicima, već i kompanijama u cilju sprečavanja praćenja njihovog internet saobraćaja. Međutim treba istaći da one nisu takođe dovoljne i u saglasnosti u potpunosti sa direktivom EU. Pošto se nudi mogućnost korisnicima samo da isključe opcije za praćenje tzv. Opt-out. Ne postoji predhodna saglasnost u skladu sa članom 5 stav 3 Direktive 2009/136/EK. <http://www.youronlinechoices.com/>, 5. 8. 2012.

206 Kolačići koji ne bi trebalo da budu obuhvaćeni pristankom korisnika su npr. kolačići koji se odnose na bezbedonosnu prijavu, pri identifikaciji korisnika (ukoliko se Fejsbuk korisnik loguje na svoj profil). Ovo važi i za npr. onlajn kupovinu i kolačiće koji se tom prilikom snimaju o korisnicima, koji omogućavaju čuvanje podataka o tome koje su korisnici dodali u svoju korpu. Svakako da bi bilo poželjno da korisnici dobiju informacije o ovome prilikom registrovanja. Time bi u potpunosti bile ispoštovane direktive EU. Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising, 02005/11/EN WP 188, Article 29 Data Protection Working Party, Jacob Kohnstamm, 8. 12. 2011, strana 9.

207 Videti više o tome u poglavlju II.

208 Npr. Ukoliko na sajtu Blica postoji određeni članak koji nam se dopada, pritiskom na lajk dugme naši podaci se prenose sajtu Blica i Fejsbuku. Problematično je to, što će se podaci i građana koji ne koriste Fejsbuk preneti ovoj društvenoj mreži a ne samo samom veb sajtu koji se posećuje, ukoliko dotični veb sajt nije blokirao transfer podataka prema Fejsbuku a poseduje ikonicu sa povezivanjem na Fejsbuk tzv. Social Plug-In.

209 Datenschutz in sozialen Netzwerken, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Düsseldorf Kreis am 08. Dezember 2011, strana 2.

se zaključiti da je dosadašnje korišćenje Social Plugin opcija od većine veb sajtova bilo protivpravno.

Koliko je korišćenje lajk dugmeta problematično pokazalo se u praksi. Tako je na veb sajtu grada Hamburga (www.hamburg.de) bilo postavljeno lajk dugme. Administrator veb sajta je saznao tehničke mogućnosti lajk dugmeta, odnosno na koji način Fajsbuk prikuplja podatke. Činjenica da se podaci prikupljaju i prilikom ne pritiskanja lajk dugmeta, dakle jednostavnom posetom veb sajta, izazvala je sumnju u funkcionisanje ove Fejsbuk opcije. Stoga je grad Hamburg zahtevao mišljenje Fejsbuka u vezi sa ovom funkcijom. Fejsbuk je ukazao na to da se obrada podataka vrši, kao i da se sakupljeni podaci brišu nakon 3 meseca od njihovog skupljanja. Pošto grad Hamburg nije bio zadovoljan odgovorom od Fejsbuka, administratori ovog veb sajta su 17.06.2010. godine uklonili lajk dugme sa svoje veb stranice.²¹⁰

Pored ovoga su vlasti nemačke pokrajine Šlezvig-Holštajn odlučile da ukinu lajk dugme i fan strane na društvenoj mreži Fejsbuk.²¹¹ Postavljanje opcije za lajkovanje od strane vlasnika sajtova se od oktobra 2011. godine kažnjava novčanom kaznom u iznosu do 50.000 evra.²¹² Glavni razlog za ovu odluku po njima je što Fejsbuk krši evropske i nemačke zakone o zaštiti podataka. To se čini prosleđivanjem podataka sa mreže na servere u Americi. Komesar za zaštitu privatnosti je zapretio tužbom ako Fejsbuk ne prestane da prosleđuje korisničke podatke ka Fejsbuk serverima u Americi. Iz Fejsbuka su tim povodom poručili da je tačno da se informacije o korisniku poput njegove IP adrese mogu videti kada se klikne na dugme lajk, ali da se ti podaci brišu posle 90 dana i da je „to u skladu sa uobičajenim standardima u industriji“.²¹³

Problem vezan za lajk i šer dugme moguće je rešiti sa dva klika „duplim klikom“ kao i u skladu sa principom „Privacy by Default“.

Sa rešenjem dva klika može se dobiti saglasnost od korisnika za slanje podataka Fejsbuku u SAD kao i njihovo korišćenje prilikom pravljenja profila, koji se koriste u marketinške svrhe. Za to je Fejsbuku neophodna predhodna saglasnost korisnika u formi predhodne informacije o obimu, odgovornosti i svrsi obrade podataka.²¹⁴

U praksi bi primena ovog duplog klika trebalo da izgleda ovako: Ukoliko se poseti bilo koji sajt koji nudi mogućnost lajkovanja, a pritom je korisnik ulogovan na Fejsbuk, podaci se ne smeju prenositi samim time što su korisnici ulogovani na Fejsbuk. Kada se klikne na izvestan sadržaj, neophodno bi bilo sadržaj još jednim

210 Georg Konjovic, *Wieso wir den Facebook „Like-Button“ wieder entfernten*, <http://intern.hamburg.de/2010/06/22/wieso-wir-den-facebook-like-button-wieder-entfernten/>, 7. 8. 2012.

211 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Facebook, <https://www.datenschutzzentrum.de/facebook/>, 7. 8. 2012.

212 *Datenschützer will Like-Button verbieten, futurezone/dpa*, sajt futurezone.at <http://futurezone.at/netzpolitik/4555-datenschuetzer-will-like-button-verbieten.php>, 7. 8. 2012.

213 *Nemačka pokrajina ukida lajk dugme i fan strane na Fejsbuku*, Beta, sajt Blica, <http://www.blic.rs/IT/272360/Nemacka-pokrajina-ukida-lajk-dugme-i-fan-strane-na-Fejsbuku>, 7. 8. 2012.

214 ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, *Stellungnahme zum Öffentlichen Expertengespräch zum Thema „Datensicherheit bei Facebook und anderen sozialen Netzwerken in Anbetracht einer Entschließung der Datenschutzbeauftragten der Länder und des Bundes“* am 24. 10. 2011, PLH E.800 Ihre Einladung vom 13. 10. 2011, Gz. PA 22/1.

klikom potvrditi. Time bi korisnici bili u potpunosti sigurni da bez njihove saglasnosti njihovi podaci neće na ovaj način biti preuzeti.²¹⁵

Dupli klik je već etablirano rešenje u praksi i može se naći na veb sajtu <http://heise.de/-1333879>. Na ovom veb sajtu je moguće preuzeti besplatnu skriptu i ovaj dodatak (eng. Plugin) ugraditi na svoju veb stranicu.²¹⁶ Na taj način se može reći da je ovo rešenje u skladu sa konceptom „*Privacy by Default*“.

Princip „*Privacy by Default*“ odnosno koncept podrazumevane privatnosti se realizuje tako što se vrše podešavanja tako da se obrada ličnih podataka, može preduzeti jedino uz svesne radnje korisnika. Ovo podrazumeva najveću moguću transparentnost o načinu obrade podataka korisnika pre odgovarajućeg aktiviranja, kao i informacije o rizicima i odgovornosti. Osim toga podrazumeva se i mogućnost prigovora korisnika kao i upotreba tehnike uz pomoć koje je moguće postići veću zaštitu podataka korisnika, tako da oni mogu sami upravljati svojim podacima. Ovaj princip je regulisan na nivu EU u Opštoj uredbi o zaštiti podataka u članu 25 (Regulation 2016/679).

Sve ovo pokazuje da lajk dugme sa sobom nosi jedan niz pravnih problema, pre svega u pogledu zaštite podataka. Trebalo bi prihvatiti to da se lajk dugme upotrebljava, ako je ono neophodno za funkcionisanje veb sajta. Svakako se politika privatnosti mora prilagoditi potrebama korisnika i tom prilikom dobiti u punom obimu odgovarajući pristanak korisnika. Štaviše, sakupljanje podataka od vlasnika veb sajtova i pravljenje profila na osnovu tih podataka od strane Fejsbuka, bilo bi u potpunosti neprihvatljivo, ukoliko se lajk dugme uopšte ne klikne ili se radi o korisnicima koji nisu članovi Fejsbuka, a koji takođe nisu kliknuli na lajk dugme.

3.6.7. *Brisanje profila*

Fejsbuk na svaki mogući način pokušava da zadrži svoje korisnike, da ih osujeti od namere da obrišu, deaktiviraju svoje profile. Tako se prilikom procesa deaktiviranja korisnici pitaju „Da li ste sigurni da želite da deaktivirate svoj nalog?“. Uz sve to se postavljaju i slike od 5 prijatelja kojima ćete nedostajati, razlozi deaktivacije, kao i primanje daljih e-mejllova od Fejsbuka. Pored toga što je opcija za deaktivaciju sakrivena, brisanje profila omogućeno je tek ukoliko se korisnik saglasi sa deaktivacijom. Deaktivacija znači privremeno ukidanje profila, ali ne i trajno. Naime ukoliko korisnik deaktivira svoj nalog, Fejsbuk će i dalje držati njegove podatke, za slučaj da se vrati. Upravo ovakav način zadržavanja podataka je suprotan modernim propisima o zaštiti podataka. Ukoliko korisnik ne želi više da koristi Fejsbuk, makar i privremeno, njegovi podaci bi trebalo da budu obrisani.²¹⁷ Poseban problem predstavlja brisanje profila, koje nije lako naći, a pravo je pitanje, da li se Fejsbuk

215 Gerald Reischl, *Zwei Klicks für mehr Privatsphäre*, sajt futurzone.at, <http://futurezone.at/digitallife/5022-futurezone-zwei-klicks-fuer-mehr-privatsphaere.php>, 7. 8. 2012.

216 Rešenje sa sa skriptama se može pronaći na sajtu <https://www.heise.de/ct/ausgabe/2014-26-Social-Media-Buttons-datenschutzkonform-nutzen-2463330.html>.

217 Ulrich Wackerbarth, *Datenschutz in sozialen Netzwerken, Seminararbeit, Rechtliche Fallstricke im Internet*, Hubert Mayer, Fernuniversität in Hagen Fachbereich Rechtswissenschaft, str. 16 i 17, http://hubert-mayer.de/dateien/Seminararbeit_Datenschutz.pdf, 13. 12. 2013.

profil zaista može i obrisati, s obizom na sve dosadašnje navedene činjenice u vezi sa načinom korišćenja podataka korisnika.

Samo *brisanje naloga* predstavlja dug proces. Ukoliko neko želi da obriše trajno nalog, potrebno je poslati zahtev na <http://on.fb.me/n5OemK> centru za pomoć i kliknuti da se nalog obriše. Potom se mora sačekati odobrenje od Fejsbuka. Ukoliko se u međuvremenu uloguje korisnik, a nalog za brisanje je poslat, taj zahtev se onda prekida i automatski se aktivira članstvo na ovoj društvenoj mreži. Iz Fejsbuka se nadaju da će se korisnici predomisлити i zbog toga odlažu proces brisanja naloga, koji traje najduže 2 nedelje.²¹⁸ Ako se profil jedanput izbriše, nema mogućnosti ponovne aktivacije.²¹⁹

U slučaju smrti korisnika, Fejsbuk takođe ne daje dovoljno podataka o tome. Postoji formular, na osnovu koga je moguće informisati Fejsbuk da je korisnik preminuo. Međutim, njega nije lako pronaći kao i mnoge informacije koje su u interesu korisnika.²²⁰ Na ovaj način moguće je bar za javnost izbrisati podatke preminulih. Veliki problem je što se zaštita podataka po važećim propisima odnosi samo na žive korisnike. Stoga bi takođe bilo interesantno uspostavljanje opcije jedne vrste digitalnog testamenta, čime bi korisnici bili u mogućnosti da odrede šta će se desiti sa njihovim profilima, posle njihove smrti.²²¹

3.6.8. Mogućnost preuzimanja podataka

Generalno je moguće preuzeti svaki podatak sa bilo kog profila, ukoliko su podaci vidljivi. Ovo se odnosi na slike, video klipove i ostale vidljive podatke.

Ovde bi se moglo postaviti pitanje: Da li drugi korisnici imaju pravo da snimaju tuđe podatke na svojim računarima? Da li je potrebna saglasnost korisnika, čiji se podaci snimaju?

Većina zakona ne reguliše ovakvu obavezu za ostale korisnike, već samo za, u ovom slučaju, Fejsbuk. Stoga se može zaključiti da je upotreba podataka na ovakav način dozvoljena. Trebalo bi razmotriti regulisanje ovog pitanja imajući u vidu koliko su korisnici uopšte svesni ovog pitanja.²²²

3.6.9. Skeniranje lica, korišćenje opasnih aplikacija

Upotreba fotografija u cilju skeniranja lica kao i snimanje i korišćenje biometrijskih podataka uz pomoć ove tehnologije je protivpravna, ukoliko ne postoji izri-

218 *Kako trajno obrisati FB nalog*, sajt B92, http://www.b92.rs/tehnopolis/vesti.php?yyyy=2011&mm=10&nav_id=547478, 7. 8. 2012.

219 *Da li ste sigurni da znate kako se trajno briše profil na Facebook-u?*, itvesti.info, <http://www.itvesti.info/2011/10/da-li-ste-sigurni-da-znate-kako-se.html>, 7. 8. 2012.

220 Formular se može videti na stranici <http://www.facebook.com/help/contact/?id=305593649477238>, 5. 8. 2012.

221 Ulrich Wackerbarth, *Datenschutz in sozialen Netzwerken, Seminararbeit, Rechtliche Fallstricke im Internet*, Hubert Mayer, Fernuniversität in Hagen Fachbereich Rechtswissenschaft, str. 18, http://hubert-mayer.de/dateien/Seminararbeit_Datenschutz.pdf, 13. 12. 2013.

222 Ibidem, str. 21.

čit pristanak i obaveštenja korisnika u ovom pogledu.²²³ Identično važi i za korisnije opasnih aplikacija i prikupljanje podataka korisnika na ovaj način.

Svaki dan dajemo lične podatke, iako najčešće i nismo ni svesni toga. Svesnost odnosno bolje rečeno nesvesnost internet korisnika pa i korisnika Fejsbuka (npr. svako pretraživanje mreže) o tome predstavlja jedan od najvećih problema u korišćenju društvenih mreža, ali i interneta uopšte. Najčešće su ljudi nesvesni svojih postupaka, koje obavljaju putem društvenih mreža, ali i putem računara u obavljanju bankarskih poslova, ili dok se voze automobilima putem navigacionih sistema, da tim svojim postupcima šalju podatke o sebi, svojoj lokaciji. Svaki put se ostavljaju digitalni tragovi!

Velika dostupnost podataka na Fejsbuku o svakom korisniku najbolje je pokazana na slučajevima masovnih ubica — Norvežanina Andresa Brejvika i Amerikanca Džejmisa Holmsa, koji je počinio masakr na premijeri filma „Betmen“. Odmah posle počinjenih zločina mediji su preko Fejsbuk profila saznali bukvalno sve o ovim masovnim ubicama, njihove želje i motive, kao i najave njihovih zločina.

Preveliku dostupnost podataka koriste i poslodavci koji putem društvenih mreža prate i kontrolišu zaposlene, ali i proveravaju kandidate za zaposlenje. Pošto korisnici često nesvesno ostavljaju podatke o sebi, smatraju da otkrivanje informacija na društvenoj mreži deluje manje lično od izgovoreni reči u društvu. Pri tom to rade zbog želje za samopromocijom, zbog koje često postavljaju nove fotografije, pišu statuse i tako celom svetu stavljaju na raspolaganje svoje aktivnosti i razmišljanja i najintimnije sfere života.²²⁴

Osnovno ljudsko pravo na zaštitu podataka postoji i propisano je nezvano za to da li smo na meži ili ne (eng. online ili offline), kao i za to u kojoj zemlji se nalazimo, ono je za sve jednako. Ovo pravo važi kako u javnom tako i u privatnom sektoru.²²⁵ Obrada i način korišćenja podataka korisnika predstavlja najveću nedoumicu. I dalje nije poznato šta zapravo Fejsbuk radi sa podacima korisnika.²²⁶ Ukoliko korisnik nije zadovoljan kako se Fejsbuk ophodi prema njegovim podacima, ne postoji drugi izbor osim, ili da prihvati ovakvo stanje, ili da prestane sa korišćenjem u potpunosti. Na taj način korisnici Fejsbuka postaju „robovi“ ove društvene mreže.²²⁷ Upravo usvajanjem Opšte uredbe o zaštiti podataka na nivu EU stvorili su se važni uslovi za pravedniju tržišnu utakmicu u domenu društvenih mreža.

223 Datenschutz in sozialen Netzwerken, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Düsseldorf Kreis am 08. Dezember 2011, strana 1.

224 Aleksandar Palić, *Internet: Svi smo u Velikom Bratu*, sajt Večernje Novosti online, <http://www.novosti.rs/vesti/naslovna/aktuelno.293.html:390535-Internet-Svi-smo-u-Velikom-Bratu>, 15. 10. 2017.

225 Viviane Reding, *Herausforderungen an den Datenschutz bis 2020: Eine europäische Perspektive*, ZD Zeitschrift für Datenschutz, beck.de Zeitschriften, <http://rsw.beck.de/cms/main?docid=321429>, 2. 8. 2012.

226 Jakob Steinschaden, *Datenschutz-EU: Facebooks Geschäftsmodell unter Beschuss*, futurzone.at, <http://futurezone.at/netzpolitik/6129-eu-facebooks-geschaeftsmodell-unter-beschuss.php>, 3. 8. 2012.

227 Martin Stepanek, *Cebit 2012, Facebook sieht kein Datenschutzproblem*, futurzone.at, <http://futurezone.at/netzpolitik/7871-facebook-sieht-kein-datenschutzproblem.php>, 3. 8. 2012.

Koliko su podaci korisnika važni Fejsbuku govori i to da ih je Maks Šrems upravo nazvao „naftom“. Da bi se izbegla trgovina podataka korisnika, odnosno da se oni ne bi tretirali kao roba odnosno kao valuta, bilo je neophodno usvajanje Opšte uredbe. Međutim glavni problem predstavlja sprovođenje predložene uredbe, koja bi prema Maksu Šremsu bila u slučaju Fejsbuka nesprovodiva. Naime, pre svega zbog toga što je za firme poput Fejsbuka češće jeftinije da plate propisanu kaznu, nego da se pridržavaju zakona.²²⁸

Fejsbuku je važna tehnologija prepoznavanja lica, naročito u deljenju podataka i obeležavanju (tagovanju) prijatelja na mobilnim telefonima. Tako je na osnovu aplikacije Klik omogućena identifikacija prijatelja na Fejsbuku, koji su uslikani mobilnim uređajem. Ovime se Fejsbuk trudi da i u oblasti mobilnih telefona uspostavi vodeću ulogu na tržištu. Treba imati u vidu da se dnevno na ovu društvenu mežu postavi oko 300 miliona fotografija.²²⁹

Možda je i najinteresantnije upravo kako će Fejsbuk uspeti da funkcioniše u budućnosti. S obzirom na trend tehnologije da se razvija u pravcu mobilnih uređaja. Upravo zbog toga je Fejsbuk u velikom problemu, pošto oglašavanje na ovoj društvenoj mreži za sada nije moguće preko mobilnih telefona.²³⁰ To predstavlja i glavni razlog, koji prosto tera Fejsbuk da napravi svoj mobilni telefon. Na taj način bi pokušali da iz trke izbace glavne konkurente u ovoj branši poput Epla, Gugla ili Majkrosofta.²³¹ Fejsbuk može svoje prednosti iskoristiti, pošto poseduje ogromnu količinu podataka. Na taj način može da razvija nove aplikacije i mogućnosti za svoje korisnike. Tako je za očekivati da zbog podataka o tome koja interesovanja, aktivnosti i veze imaju korisnici, može stvoriti usluge kojima bi npr. bilo moguće izabrati odgovarajući hotel ili restoran, kupiti određeni automobil, pronaći odgovarajućeg poslodavca itd.²³²

Može se zaključiti da je svako u krajnjoj liniji sam odgovoran, koje podatke o sebi objavljuje na Fejsbuku. Da bi se ova društvena mreža pravilno koristila, potrebno je najpre izučiti njeno funkcionisanje, pa tek onda započeti sa njenim korišćenjem. Pravna zaštita predstavlja krajnju mogućnost ostvarenja prava pojedinaca, ali ne i dovoljnu da bi se u potpunosti zaštitilo osnovno ljudsko pravo na privatnost. S obzirom na ubrzan napredak tehnologije, nemoguće je regulisati i predvideti u praksi svaku moguću situaciju povrede prava privatnosti korisnika Fejsbuka. Stoga svest korisnika Fejsbuka mora biti na povećanom nivou, pošto mogućnosti zloupotrebe njihovih najintimnijih podataka ne može u potpunosti sprečiti nijedan pravni sistem.

228 *Diskussion– „User-Daten sind das neue Öl“*, futurzone.at, <http://futurezone.at/netzpolitik/10349-user-daten-sind-das-neue-oel.php>, 3. 8. 2012.

229 *Zašto su vaša lica važna Facebooku?*, sajt B92, http://www.b92.net/tehnopolis/aktuelno.php?yyyy=2012&mm=06&nav_id=620307, 2. 8. 2012.

230 Fejsbuk je do sada beležio konstantan rast broja korisnika. Poslednji podaci pokazuju da se broj korisnika u SAD smanjio za skoro milion (sa 158,9 miliona na 158 miliona). *SAD: Broj korisnika Facebook-a pao za milion*, Izvor: Tanjug, sajt Večernje Novosti online, <http://www.novosti.rs/vesti/naslovna/aktuelno.236.html:388955-SAD-Broj-korisnika-Facebook-a-pao-za-milion>, 3. 8. 2012.

231 Molly Wood, *Odakle će stići ubica Facebooka?*, Izvor: CNET, sajt B92, http://www.b92.net/tehnopolis/aktuelno.php?yyyy=2012&mm=06&nav_id=615171, 3. 8. 2012.

232 Jakob Steinschaden, *Interview– Facebook: „Werbung kratzt nur an Oberfläche“*, futurzone.at, <http://futurezone.at/b2b/9648-facebook-werbung-kratzt-nur-an-oberflaeche.php>, 3. 8. 2012.

4. SUDSKA NADLEŽNOST I FEJSBUK

4.1. Uvod

Pravne norme bez ostvarivanja pravne zaštite predstavljaju samo mrtvo slovo na papiru. Stoga je potrebno pored adekvatnih normi uspostaviti mehanizme zaštite. Oni se u modernim pravnim sistemima ostvaruju putem suda.

Problematika sudske nadležnosti je u slučaju Fejsbuka veoma kompleksna, pošto dolazi do preplitanja više pravnih grana i mnoštva pravnih sistema. Treba razlikovati tri odnosa po pitanju ustanovljavanja sudske nadležnosti: međunarodno-privatnopravni, javnopravni, međunarodni (ugovorni).

Kod *međunarodno-privatnopravnog* odnosa Fejsbuk korisnika treba odgovoriti na pitanja sukoba teritorijalne nadležnosti i pitanja čije će se pravo primeniti i pred sudom koje države će se to pravo primeniti u slučaju spora sa Fejsbukom. Ova pitanja se postavljaju kada se radi o ugovornom odnosu sa Fejsbukom.

Kod *javnopravnog* odnosa sa Fejsbukom tu su pitanja koja su vezana za suverenitet jedne države odnosno ostvarivanja teritorijalne nadležnosti sudova. Pošto zaštita podataka o ličnosti predstavlja ustavnu kategoriju i osnovno ljudsko pravo u većini evropskih zemalja za razliku od SAD, postavlja se pitanje podizanja upravnih, građanskih i ustavnih tužbi od strane pojedinca u državi iz koje on potiče. Pravo je pitanje, da li je uopšte moguće primeniti teritorijalno pravo države iz čije pojedinac potiče u slučaju Fejsbuka? Koji mehanizmi postoje?

Kod međunarodnog *ugovornog* odnosa radi se o međudržavnom sporazumu *Privacy Shield* između EU i SAD, nasledniku sporazuma *Safe Harbour*. Na osnovu sporazuma *Privacy Shield* je regulisana međusobna razmena i zaštita podataka. Specifičnosti ovog sporazuma imaju dalekosežne posledice na celokupnu pravnu problematiku i u odnosu na Fejsbuk.

4.2. Međunarodno-privatnopravni odnos sa Fejsbukom

U slučaju Fejsbuka dolazi do sklapanja ugovora sa ovom društvenom mrežom, sa kojom korisnici prihvataju opšte uslove poslovanja ove kompanije. Iako većina ljudi i ne zna, oni su zapravo samim svojim pristupanjem ovoj mreži ušli u ugovorni odnos sa Fejsbukom. Međutim, ugovorni odnos ne može i nema jaču pravnu snagu od ustavnih i zakonskih odredbi jedne države.

Na ovom mestu je potrebno razmotriti kakve pravne posledice ovaj ugovorni odnos ima na korisnike koji se nalaze u SAD (gde se nalazi sedište Fejsbuka) i one van SAD. Pored toga je zanimljivo razmotriti eventualne tužbe sa stanovišta zaštite potrošača (građansku tužbu).

Fejsbuk u svojim opštim uslovima poslovanja navodi u tački 16 (1) „Svaku tužbu, uzrok za pokretanje pravnog postupka ili spor sa nama koji proistekne ili ima veze sa ovom izjavom ili veb lokacijom Fejsbuka rešavaće se isključivo u državnom ili saveznom sudu u okrugu Santa Klara. Ova Izjava se tumači u skladu sa zakonima države Kalifornije, a isto važi i za bilo koju tužbu do koje dođe između vas i nas, bez obzira na sukobe zakonskih odredbi. Prihvatate nadležnost sudova u okrugu Santa Klara, Kalifornija, u svrhe rešavanja takvih tužbi“.²³³

Time je svaki korisnik obavezan da svoju sudsku zaštitu ostvari u SAD. Međutim, ukoliko se radi o korisnicima, koji dolaze izvan SAD i Kanade, nadležnost suda se reguliše na sledeći način „Ako živite u SAD ili Kanadi ili je sedište vašeg preduzeća u nekoj od ove dve zemlje, ova Izjava predstavlja ugovor između vas i kompanije Facebook, Inc. U suprotnom, ova izjava predstavlja ugovor između vas i kompanije Facebook Ireland Limited. Reči „mi“, „nas“ i „naše“ odnose se na kompaniju Facebook, Inc. ili kompaniju Facebook Ireland Limited, u zavisnosti od situacije“.²³⁴ Na ovaj način su svi korisnici koji žive izvan SAD i Kanade obavezni da se se u slučaju eventualnih sporova (bilo u privatnopravnom bilo u javnopravnom odnosu sa Fejsbukom) obrate sudovima u Irskoj.

Ukoliko se razmotri pravni aspekt nadležnosti u pogledu parnične tužbe za sve potrošače na nivou EU, ovu problematiku reguliše uredba Brisel I u svojim članovima 15 i 16.²³⁵ Pošto je potrošač ugovorna strana, koja ima svoj boravak ili uobičajeni boravak u jednoj od država članica EU, a Fejsbuk Irska predstavlja firmu ćerku Fejsbuk Inc iz odredbi člana 15 proizlazi da „ugovorna strana prema potrošaču, koja nema sedište firme u nekoj od država članica EU, ali ima predstavništvo, agenciju, ogranak ili već neki poseban oblik filijale odnosno predstavništva, u slučaju sporova dolazi do ustanovljavanja nadležnost sudova zemlje u kojima se nalazi predstavništvo“. Iz člana 16 proizlazi da se tužba potrošača protiv ugovornog partnera može podneti ili pred sudovima članica EU u kojima ovaj ugovorni partner ima sedište firme, ili pred sudom mesta, u kojem potrošač ima svoje boravište. Obrnuto tužba protiv potrošača se može podneti isključivo pred sudom one države članice EU u kojem potrošač ima boravište.

Može se zaključiti da EU potrošač može biti tužen od strane Fejsbuka samo pred sudom države članice u kojoj ima boravište, dok Fejsbuk može biti tužen ili u Irskoj ili pred sudom države članice u kojoj potrošač ima boravište.

Sva ova pitanja i tačke vezivanja u slučaju spora sa Fejsbukom dolazile bi do primene da Fejsbuk korisnici ne prihvataju automatsku nadležnost sudova bilo u SAD bilo u Irskoj svojim pristupanjem ovoj društvenoj mreži.

Potrošači koji dolaze van EU, bi mogli biti tuženi od strane Fejsbuka i tužiti Fejsbuk isključivo pred sudovima u Irskoj. Ovo se odnosi isključivo na ostvarenje prava putem parnične tužbe u eventualnom sporu sa Fejsbukom.

233 *Opšti uslovi poslovanja Fejsbuka*, tačka 16(1), Fejsbuk, <http://www.facebook.com/legal/terms>, 24. 2. 2013.

234 *Ibidem*, tačka 19(1).

235 EuGVVO (Brüssel I-Verordnung): Verordnung (EG) Nr. 44/2001 vom 22.12.2000., über die gerichtliche Zuständigkeit und die Anerkennung und Vollstreckung von Entscheidungen in Zivil- und Handelssachen, Abl. 2001, L 12/1, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:012:0001:0023:de:PDF>, 24. 1. 2013.

Tužbe između privatnih lica su moguće i biće u daljem tekstu navedene kao primeri.

4.3. Javnopravni odnos sa Fejsbukom

Pravo zaštite podataka na nivou EU proizlazi iz tzv. primarnog prava EU, regulisanim u Konvencija o zaštiti ljudskih prava i osnovnih sloboda²³⁶ kao i u Povelji o ljudskim pravima.²³⁷ Na taj način ovo pravo predstavlja ustavnu kategoriju koja ima primat u svakoj državi članici EU. Za razliku od oblasti zaštite potrošača koja je regulisana uredbom (zakoni EU), oblast zaštite podataka, dugo vremena nije bila regulisana uredbom, već direktivama koje imaju slabiju pravnu snagu. Na taj način svaka država članica EU je imala svoj zakon o zaštiti podataka o ličnosti (oslanjajući se na Direktivu iz 1995.godine), pa se nadležnost u ovoj pravnoj oblasti određivala teritorijalno za svaku državu članicu EU pojedinačno. Pošto je sedište Fejsbuka za evropske korisnike u Irskoj, time se uspostavlja nadležnost sudova u Irskoj za sve države članice EU. Fejsbuk je izabrao sudsku nadležnost Irske, jer je važila za zemlju sa najnižim standardom u pogledu zaštite podataka u okviru EU, ali i brojnim poreskim olakšicama.²³⁸

Dalji problemi su se odnosili na to gde se podaci faktički obrađuju. Obrada podataka se delom vrši u Dublinu a najvećim delom u SAD. I pored toga stav većine eksperata ide u pravcu da je za obradu podataka odgovoran Fejsbuk Irska. Stoga je i Maks Šrems svoje ustavom zagarantovano pravo morao da potraži u Irskoj.

Pravo na zaštitu podataka pre svih dužna je da garantuje država. Kao osnovno ljudsko pravo, država je ta, koja je dužna da svakom pojedincu omogući ostvarenje prava na zaštitu podataka i privatnost. S obzirom na ubrzani tehnološki razvoj i mogućnosti interneta i elektronskih komunikacija, država nije u stanju da adekvat-

236 Pravo na poštovanje privatnog i porodičnog života regulisano u članu 8 Konvencije. *Konvencija o zaštiti ljudskih prava i osnovnih sloboda*, Rim, Savet Evrope, 1950, http://www.echr.coe.int/NR/rdonlyres/EA13181C-D74A-47F9-A4E5-8A3AF5092938/0/Convention_BOS.pdf, 4. 3. 2013.

237 Zaštita podataka lične prirode regulisana je u članu 8 Povelje. *Povelja o osnovnim pravima Evropske Unije.*, 2007, http://www.skupstina.me/cms/site_data/DOC24/913/913_Povelja%20o%20osnovim%20pravima%20EU.pdf, 4. 3. 2013.

238 Finansijski izveštaj Fejsbuk ogranka u Irskoj, pokazao je da je ovo predstavništvo na preko 800 miliona funti profita ostvarog u 2013. godini, platilo svega 2.9 miliona funti poreza. Fejsbuk je omogućio da kompanije koje se reklamiraju preko ove socijalne mreže u bilo kojoj zemlji van SAD i Kanade, plaćaju naknadu Fejsbuku Irskoj. Ova filijala uspeła da ostvari bruto dobit za 2011. godinu od 840 miliona funti, odnosno 3.1 miliona funti po svakom od 287 zaposlenih. Iako je bruto dobit izuzetno visoka, irski Fejsbuk je uspeo da smanji svoj porez na samo 2.9 miliona funti, koristeći računovodstvenu tehniku „Dupla Irska“ (Double Irish). Na ovaj način su multinacionalne kompanije u mogućnosti da premeste velike količine novca na svoje filijale u formi autorskih prava. Tako je Fejsbuk prebacio 750 miliona funti na Kajmanska ostrva i na svoje matično preduzeće u Kaliforniji za licenciranje i autorska prava. Nakon transfera je Fejsbuk Irska prijavio godišnji gubitak od 15 miliona funti. U 2012. godini Fejsbuk je platio svega 238.000 funti poreza na dobit korporacije u Irskoj, što je manje nego prosečna plata i bonus zaposlenih u ovoj filijali. Procena je da su prošlogodišnji prihodi Fejsbuka u Irskoj bili oko 175 miliona funti. Izvor: *Facebook „zaradio“ na poreskim tehnikama u Irskoj*, Tanjug, sajt Novosti.rs, <http://www.novosti.rs/vesti/naslovna/tehnologije/aktuelno.236.html:411981-Facebook-quotzaradioquot-na-poreskim-tehnikama-u-Irskoj>, 28. 7. 2013.

no efikasnim pravnim mehanizmima spreči i zaštiti pojedince na Fejsbuku i na internetu uopšte. Korisnici Fejsbuka koji ovu društvenu mrežu koriste u EU, uz primenu Opšte uredbe o zaštiti podataka mogu da se nadaju da će Fejsbuk svoje ponašanje prilagoditi privatnosti korisnika. Preduslov za to je da su sve društvene mreže pa i Fejsbuk dužne da svoju politiku privatnosti prilagode evropskim standardima, ukoliko to ne učine, neće moći da posluju na prostoru EU.²³⁹

Ako uzmemo za primer Srbiju kao državu van EU i ustanovljavanje sudske nadležnosti vezane za Fejsbuk, može se ustanoviti da je zaštita podataka garantovana ustavom, ali i važećim međunarodnim ugovorima, koje je Srbija potpisala.²⁴⁰ To znači da je Srbija kao članica Saveta Evrope dužna da neposredno primenjuje, shodno ustavu, Konvenciju o zaštiti ljudskih prava i osnovnih sloboda. Građani se u poslednjoj instanci mogu obratiti i Evropskom sudu za ljudska prava u Strazburu, ali ta pravna zaštita se odnosi na slučaj kada država Srbija nije ispoštovala Konvenciju i kada su iscrpljena sva pravna sredstva pred domaćim sudovima. Međutim, pošto Srbija ne može ostvariti teritorijalnu nadležnost u odnosu na Fejsbuk (uglavnom ne, osim u slučaju nadzora komunikacija, otvaranja predstavništva u Srbiji, i postavljanja servera u Srbiji), srpski državljani su ostavljeni bez pravne zaštite. Mogućnost za ostvarenje njihovih prava se može tražiti isključivo u Irskoj, pošto je tamo predstavništvo Fejsbuka za Evropu. Identično kao i za navedeni slučaj zaštite srpskih potrošača, kod eventualnih građanskih tužbi.

Pitanje *krivičnih tužbi* kao dela javnog prava i ustanovljenje sudske nadležnosti u krivičnopravničkim postupcima *protiv Fejsbuka* se može ustanoviti isključivo pred sudovima u Irskoj.

U ostalim odnosima *između pojedinaca, između pojedinaca i države* dolazi do ustanovljavanja *teritorijalne nadležnosti sudova, na čijoj teritoriji je izvršeno određeno krivično delo*. Tada je moguće npr. tužiti državu Srbiju u Strazburu, ukoliko je došlo do povrede Konvencije o zaštiti ljudskih prava i osnovnih sloboda, ali ako su u Srbiji najpre iscrpljena sva pravna sredstva.

U ovakim slučajevima se države oslanjaju na pružanje pravne pomoći od strane Fejsbuka. Kolika je snaga Fejsbuka se ogleda upravo u tome, da u ovom slučaju ima skoro atribute državnosti, pošto je u stanju da odobri ili ne odobri pravnu pomoć.

4.4. Međunarodni ugovorni odnos sa Fejsbukom

4.4.1. *Safe Harbour*

Pre nego što se objasni značenje ugovora *Safe Harbour* po celokupnu problematiku sudske nadležnosti ne samo u odnosu na Fejsbuk, već i u odnos između EU i SAD, potrebno je razmotriti suštinske razlike u ova dva pravna sistema po pitanju zaštite podataka i privatnosti uopšte.

239 Nažalost pod ogromnim uticajem Gugla, Fejsbuka, Skajpa i drugih tehnoloških giganta, malo šta je ostalo od prvobitnog Predloga uredbe o zaštiti podataka EU.

240 Član 16 reguliše međunarodne odnose. *Ustav Republike Srbije*, 2006, Narodna Skupština Republike Srbije (Službeni Glasnik RS 48/94 i 11/98), http://www.parlament.rs/upload/documents/Ustav_Srbije_pdf.pdf, 4. 3. 2013.

U SAD je pojam privatnosti shvaćen potpuno drugačije u odnosu na EU. „Privacy and Freedom“ pojam, koji je uspostavio Alan Westin definiše privatnost kao mogućnost pojedinca, grupe ili institucije da odrede, kada, kako i koje podatke želi da podeli o sebi.²⁴¹ Kao što se može primetiti ovaj koncept u svoj fokus stavlja pojedinca, i izveden je iz liberalnog koncepta, koji je ustanovio Džon Lok (John Lock).

Ipak suštinska razlika u odnosu na EU zakonodavstvo je nemešanje države u privatni sektor. Na taj način su pojedinci u mogućnosti da sami odrede, koje podatke žele da iznesu o sebi, kome i kojim putem. Država je dakle dužna da obezbedi građanima zaštitu po pitanju zaštite podataka samo u odnosu na javni sektor što proizlazi iz liberalnog koncepta države. Tako da Privacy Act iz 1974 reguliše isključivo obradu podataka u javnom sektoru. Može se zaključiti da je država dužna da se uzdrži od svakog mešanja u privatni sektor po ovom pitanju.

U SAD je pravo na privatnost priznato pojedincima kroz tumačenje ustava, odlukom Vrhovnog suda SAD u slučaju *Griswold v. Connecticut* iz 1965 godine. Ipak i pored toga samo je američka država Kalifornija ovo tumačenje donekle u svom ustavu prihvatila. Postoji malo koji zakon ili pravilo koje regulišu ovu materiju.

Takođe u Sjedinjenim Američkim Državama ne postoji institucija za zaštitu podataka. Povremeno se ovim problemom bavi FTC (Federal Trade Commission), koja pošto ne postoje zakonske odredbe, deluje samo ukoliko se zainteresovane strane svojevolski obavežu na poštovanje standarda zaštite podataka. Ono što je takođe vredno pomena je da na tlu SAD uopšte ne postoje prava pojedinaca u pogledu brisanja, ispravljanja podataka, zahteva o informacijama koji se podaci obrađuju kao i dužine obrade podataka.²⁴²

U EU je situacija potpuno drugačija, te je iz svega proizašao i ovaj hibridni sporazum. Treba imati u vidu da na nivou EU postoji drugačiji koncept u pogledu mešanja države pre svega kada je u pitanju zaštita prava pojedinaca i njenom aktivnom učešću u tome kako u javnom tako i u privatnom sektoru.

Država je dužna da interveniše i upravlja i u privrednim odnosima, te predstavlja jednu kvazi pravnu ličnost, koja je u obavezi da omogući dobrobit čitavom društvu. Ova doktrina potiče od Hegela po kome: „Država je kao realizacija supstancionalne volje, koju ona ima za to u svojem javnom mnjenju prikupljeno samopouzdanje, koje je samo po sebi racionalno“.²⁴³ Pored Hegela i Ruso je doprineo ovom shvatanju evropskog pravnog regulisanja, po kome je država institucija sprovođenja volje javnosti.²⁴⁴

241 „Privacy is the claim of individuals, groups, or institutions, to determine for themselves when, how, and to what extent information about them is communicated to others.“ Alan F. Westin, *Privacy and Freedom*, New York: Atheneum, January 1, 1967. strana 7.

242 Datenschutz, Wikipedia, samostalna enciklopedija <http://de.wikipedia.org/wiki/Datenschutz>, 8. 8. 2013.

243 „Der Staat ist als die Wirklichkeit des substantiellen Willens, die er in dem zu seiner Allgemeinheit erhobenen besonderen Selbstbewusstsein hat, das an und für sich Vernünftige.“ Georg Wilhelm Friedrich Hegel, *Grundlinien der Philosophie des Rechts*, Dritter Abschnitt, Der Staat, 1821. godine, član 258.

244 *Datenschutz zwischen Staat und Markt (Die „Safe Harbor“-Lösung als Ergebnis einer strategischen Interaktion zwischen der EU, den USA und der IT-Industrie)*, Universität Konstanz, 2002, Magisterarbeit, Simon Fink, str. 38.

Sam Safe Harbour (Safe Harbor Agreement 2000) regulisao je međusobni transfer podataka i zaštitu podataka između EU i SAD. Sporazum je proistekao iz brojnih političkih, ekonomskih i tehničkih razloga, a pre svega iz ubrzanog razvoja interneta i neophodnosti njegove regulacije. Njime su prihvaćeni osnovni principi zaštite podataka o ličnosti i osnovna tri principa: svrsishodnost obrade, transparentnost, posebna zaštita naročito osetljivih podataka. Međutim, nije prihvaćen možda i najvažniji princip, a to je sprovođenje sporazuma i uspostavljanje nezavisne institucije za nadzor i kontrolu podataka. Bez mogućnosti kažnjavanja ovaj sporazum nije u mogućnosti da ostvari suštinske principe zaštite podataka. Međutim, iako predstavlja jedan od najznačajnijih osnova za regulaciju ove materije, zapravo predstavlja slobodnu volju kompanija tzv. samoregulaciju u SAD.²⁴⁵ Pored toga što su potpisnici sporazuma dve države, ovaj sporazum ne predstavlja obavezu za privatni sektor u SAD, a i sudski mehanizmi zaštite su ograničeni. Razlozi za to su mnogobrojni i proističu iz već navedenih suštinskih razlika između evropskog i američkog pravnog sistema u pogledu zaštite podataka i shvatanja privatnosti uopšte.

Pošto na nivou EU postoje izuzetno strogi zahtevi u pogledu zaštite podataka (već napomenuto spada u ustavnu kategoriju i jedno je od osnovnih ljudskih prava), jedan vid kompromisa u ovom pogledu postignut je u vidu Safe Harbour sporazuma tzv. sigurne luke, u kojoj se nalaze firme, koje su ovaj sporazum prihvatile. Za uplovljavanje u „sigurnu luku“ potrebno je bilo poslati pismo američkom Ministarstvu trgovine i na taj način prihvatiti obaveze koje su potpisale EU i SAD, a koje odgovaraju evropskom standardu zaštite podataka.

Prihvatanjem sporazuma, firme iz SAD dolazile su u nadležnost američke Federalne trgovinske komisije (Federal Trade Commission), koja je zadužena da nadzire i kontroliše primenu sporazuma. Ono što je zanimljivo je da ova institucija može sankcionisati kompanije, ukoliko one ne primenjuju standarde i prekrše princip konkurencije i fer ponašanja na tržištu.

Takođe je uočljivo da se izvršenje u SAD ne ostvaruje na osnovu zakona o zaštiti podataka i da ovaj sporazum ne podleže institucionalnim promenama sistema SAD. Federalna trgovinska komisija (Federal Trade Commission) vrši svoje dužnosti u pogledu zaštite od neloyalne konkurencije i fer ponašanja na tržištu, što je i inače obaveza ove institucije. Lista kompanija koje su prihvatile ovaj sporazum mogla se pronaći na internetu.²⁴⁶ Svojevoljno je oko 3000 američkih kompanija prihvatilo ovaj sporazum.²⁴⁷ Sami principi iz sporazuma su bili isuviše uopšteno formulisani i ostavljali su kompanijama mogućnost pogodnog formulisanja obaveza.

Zemlje EU su se našle pred jednom dilemom da li prihvatiti ovakav sporazum na nižem nivou zaštite podataka EU građana u SAD ili blokirati transport odnosno transfer podataka u SAD.²⁴⁸ U oba slučaja ishod je prema mnogim ekspertima identičan — standardi EU neće biti ispoštovani.

245 *Ibidem*, str. 8.

246 URL adresa: <http://safeharbor.export.gov/list.aspx>, 6. 8. 2013.

247 *Endlich! EU-Kommissarin stellt „Safe Harbor“-Abkommen in Frage*, [unwatched.org](http://www.unwatched.org), http://www.unwatched.org/EDRigram_11.15_Endlich_EU-Kommissarin_hinterfragt_Safe-Harbor-Abkommen, 7. 8. 2013.

248 Tada se razmišljalo kao i sa protokom kapitala u zemlje sa nižim poreskim obavezama, postojala je opasnost 90-tih godina prošlog veka da podaci budu transferisani u zemlje sa većim stepenom

Fejsbuk je prihvatio načela Safe Harbour sporazuma u svojoj politici o privatnosti. Izričito je u ovom dokumentu napisano da ova društvena mreža prihvata sporazum i njegove principe u odnosu na podatke o zaposlenima, zastupnike klijenata, pružaoce usluga, trgovce, marketing klijente i druge partnere Fejsbuka ili njegove firme ćerke sa prostora EU.²⁴⁹

Delovanje Safe Harboura je Fejsbuk ograničio na osobe koje imaju prebivalište na teritoriji Švajcarske i EU. Od sporazuma su izuzeti podaci o zaposlenima u Fejsbuku kao i lični podaci osoba, koje oni sami na ovu društvenu mrežu postavljaju.

Utvrđene su bile i kategorije podataka, doduše uopšteno, kao i svrha njihove obrade. Svrha kao ključan zahtev za obradu je postavljena isuviše široko i neprecizno. Fejsbuk je naveo da je praktično moguće da se podaci EU građana obrađuju u svim njihovim ugovorima, ako su potrebni za njihovo izvršenje. Koji su to ugovori, koje firme obrađuju podatke, koje konkretno podatke, nije navedeno. Tačna kategorizacija je izvršena samo za klijente koji koriste ovu društvenu mrežu za oglašavanje i za partnere Fejsbuka. Korisnicima iz EU i Švajcarske je priznato pravo na prigovor za obradu podataka u marketinške svrhe. Nedostajalo je i objašnjenje značenja ovog prigovora kao i jasno formulisana adresa i kontakta u slučaju prigovora. Uopšteno je bila ustanovljena obaveza postojanja kontakt osobe, ali takođe bez jasnog navođenja o kome se radi i upućuje se na politiku o privatnosti Fejsbuka. Na taj način prosečnom korisniku Fejsbuka nije bilo jasno, šta zapravo donosi ovo obavezivanje Fejsbuka. Transparentnost i fer ophođenje prema korisnicima i informisanost, koje predstavlja jedan od temelja za zakonitu obradu podataka, dakle nije bila ispoštovana.

Ono što je u totalnoj suprotnosti sa načelima zaštite podataka u EU a izričito je propisano u sporazumu Safe Harbour, je da podaci pripadaju i postaju vlasništvo Fejsbuka, što je potpuno neprihvatljivo. Naime, oni postaju umesto ličnog prava pojedinca, svojina Fejsbuka. Upravo se i na ovom primeru vidi suštinska razlika zakonodavstva EU i SAD.

Posle 13 godina postojanja sporazum je sazreo da bude preispitan od strane Evropske Komisije, pogotovu posle događaja vezanih za PRSIM (u daljem tekstu: PRIZMA) programa američke agencije NSA (National Security Agency) za špijunažu.²⁵⁰

Na ovom mestu treba istaći suštinski odnos države prema uopšte zaštititi podataka i celokupnom skandalu o špijunaži.

Zahvaljujući Edvardu Snoudenu (Edward Snowden) Evropa je saznala ono što do sada nije znala, da su građani EU špijunirani od strane SAD na osnovu PRIZMA programa američke agencije NSA (National Security Agency). Na taj način EU ulazi u novu paranoju i potrebu za daljim regulisanjem i donošenjem novih,

rizika i neadekvatnom zaštitom podataka. Ovo je predstavljao još jedan povod za donošenje Safe Harbour sporazuma.

249 ALLGEMEINE DATENSCHUTZRICHTLINIE EWR/CH-USA, SAFE HARBOR RECHTS-HINWEIS, <https://www.facebook.com/safeharbor.php>, 7. 8. 2013.

250 *Endlich! EU-Kommissarin stellt „Safe Harbor“-Abkommen in Frage*, [unwatched.org](http://www.unwatched.org), http://www.unwatched.org/EDRigram_11.15_Endlich_EU-Kommissarin_hinterfragt_Safe-Harbor-Abkommen, 7. 8. 2013.

strožih zakona o terorizmu, i zadržavanju podataka. Sve to naravno na štetu običnih i nedužnih građana.

Svakako sa ovim saznanjem, a i alchajmerom o dosadašnjoj pravnoj regulaciji u ovoj oblasti u EU, može se zaključiti, da postoji povećana potreba za donošenjem novih „sigurnih luka“, u kojima bi bilo prikupljeno još više podataka EU građana. Na taj način bi „veliki brat“ u ovom slučaju SAD, pružio „sigurnih luku“ u zaštiti podataka, koji dolaze iz EU.

SAD zapravo ne čine ništa loše, one sprovode sopstvene zakone. Već spomenuti Patriot Act dozvoljava pristup podacima, kada je cilj sigurnost i bezbednost SAD. Potpuno je nevažno da li se radi o internet podacima ili u papirnoj formi i da li su oni prikupljeni u SAD ili u bilo kojoj drugoj zemlji na svetu. Dakle jedino ograničenje je faktička nemogućnost institucija SAD da dopru do podataka. Stoga je logično zaključiti da je svako korišćenje podataka od strane SAD legalno.

Zaboravlja se da i na nivou EU postoje slični projekti poput INDECT koji ima za cilj da svaki pokret običnih građana u javnosti automatski obradi, kategorizuje i proceni i na taj način oceni da li je neko sumljiv ili nije. Ovaj program je ispraćen i plaćen sa milionima evra, da bi se brzo došlo do navodnih potencijalnih terorista. Postavlja se prosto pitanje, zašto o ovom u Evropi niko ne diskutuje? Ili možda treba diskutovati o ponovnom vraćanju direktive EU o zadržavanju podataka, kojom je predviđeno da se celokupan internet i telefonski saobraćaj procenjuje i čuva minimum 6 meseci ?

Jedno je sigurno, onaj ko planira da kroz prikupljanje podataka obezbedi sigurnost, moraće neminovno da prikupi još više podataka.²⁵¹

4.4.2. Tužba zbog afere PRIZMA i uticaj na sporazum Safe Harbour

Već poznati protivnik Fejsbukovog ophođenja prema zaštiti podataka Maks Šrems i njegova organizacija „europe-v-facebook.org“, iskoristili su priliku i aferu PRIZMA da tuže Fejsbuk.²⁵² I ova tužba protiv ove društvene mreže podneta je u Irskoj u Dablinu, iz poznatog razloga, zbog toga što je tu sedište Fejsbuka za evropske korisnike. Ovom prilikom su pored ove društvene mreže tuženi i Epl (takođe u Irskoj), Skajp i Majkrosoft (u Luksemburgu) i Jahu (u Bavarskoj). Tužbe su bile usmerene i na zaštitu podataka i na transfer podataka evropskih građana od strane sedišta navedenih firmi američkoj NSA službi.

Ovim gigantima se u tužbama osporava transfer podataka od strane firmi ćerki u SAD, zbog neadekvatnog nivoa zaštite podataka u SAD. Pošto se ne može shodno direktivi EU o zaštiti podataka govoriti o adekvatnoj zaštiti (u smislu člana 25 Direktive o zaštiti podataka iz 1995. godine), ukoliko se radi o prisluškivanju. Do

251 Hans Zeger, *Wir sind Paranoistaat!*, Arge Daten, http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=50762roe, 20. 8. 2013.

252 Šrems je dobio podršku i od 5 političara iz Evropskog parlamenta, koji su zahtev u vidu parlamentarnog pitanja uputili Evropskoj komisiji, u kojoj se eksplicitno traži objašnjenje za situaciju sa Fejsbukom u Irskoj. Pored ovog zahteva su i drugi aktivisti za zaštitu podataka podneli Komisiji žalbu protiv države Irske zbog ne sprovođenja prava EU. Još uvek se čeka na reakciju Komisije. *Facebook-Streit: Schrems kriegt Unterstützung*, futurezone.at, <http://futurezone.at/netzpolitik/facebook-streit-schrems-kriegt-unterstuetzung/> 24.595.941, 24. 10. 2013.

tužbe je došlo zbog učešća Fejsbuka u aferi PRIZMA. U suštini radi se o tome, da li jedna firma može bez dozvole i odobrenja evropskih institucija za zaštitu podataka da prosledi podatke u zemlje koje nemaju odgovarajući nivo zaštite podataka i tajnim službama u tim zemljama (u konkretnom slučaju u SAD). Šrems tvrdi da taj „adekvatan nivo zaštite podataka“ više ne postoji, nakon otkrivanja špijunaže od strane Snoudena.²⁵³

Ovaj postupak je ličio na slučaj sa tzv. SWIFT konvencijom u kome je 2006. godine odbor evropskih institucija za zaštitu podataka odlučio, da je masovan prenos podataka institucijama u SAD nelegalan. SWIFT konvencija reguliše bankarske podatke i njihov prenos između SAD i EU. Tada je ustanovljeno da u okviru programa nije dozvoljeno da se ministarstvu finansija SAD prosleđuju podaci u svrhu borbe protiv terorizma. Identično bi trebalo prema mišljenju udruženja europe-v-facebook da važi i u slučaju PRIZMA. Šrems i njegovi pobornici želeli su da postignu dva cilja ovom tužbom: Najpre da ustanove da li je masovan prenos podataka američkoj službi NSA legalan ili nije, odnosno da li jedna evropska firma sme da prosleđuje i daje pristup stranim tajnim službama. Ukoliko je to moguće, onda bi trebalo promeniti zakone EU, smatra organizacija. I konačno, drugi cilj možda i ključni je da u postupcima tužene firme saopšte tačno, šta rade sa podacima evropskih građana. Ukoliko bi blokirale pristup, došle bi u opasnost da sudovi odluče da uopšte više ne mogu da prenose podatke u SAD.²⁵⁴

Upravo tužbe protiv Fejsbuka i Epla su shodno odluci irske institucije za zaštitu podataka oglašene kao neosnovane, te nije ni otvoren dalji postupak. Ovom odlukom je transfer podataka od strane navedenih firmi proglašen legalnim i sa odgovarajućim nivom zaštite podataka. Irska institucija za zaštitu podataka smatra da je na nivou EU ovo odlučeno još 2000. godine u okviru već spomenute Safe Harbour konvencije i da su time zapravo Evropljani još tada predvideli i prihvatili PRIZMA program. Stoga proizlazi i da sve firme, koje su prihvatile ovaj sporazum, smeju da šalju podatke evropskih građana američkim tajnim službama.

Inače najnovija istraživanja su pokazala da je ogroman broj kompanija sa sedištem u SAD, koje obrađuju podatke građana EU, lažno prikazivao da su prihvatili Safe Harbour i da imaju sertifikat Safe Harbour sporazuma. Ovu vest obelodanio je Christopher Connolly, direktor Galexia, konsultantske kompanije sa sedištem u Australiji koja se bavi pravom na privatnost na internetu. Prema njegovom rezultatu istraživanja je jedna od svakih sedam tvrdnji članstva u Safe Harbour bila je lažna. Rezultati istraživanja pokazali su i da postoji više od 200 lažnih potraživanja u 2008. godini, a ovaj broj je porastao na 427 u septembru 2013. Prema tvrdnji ovog istraživača se u broju 427 organizacija nalaze podaci o ogromnom broju domaćinstava u Evropi, sa stotinama miliona korisnika. Pored toga i da ova zloupotreba bude još uočljivija, neke od kompanija su postavile neovlašćeno Safe Harbour pečate i oznake na njihovom sajtu, iako nikada nisu potpisale taj sporazum.²⁵⁵ Za ova-

253 *Klage gegen irische Datenschutzbehörde zugelassen*, portal futurezone.at, <http://futurezone.at/netzpolitik/klage-gegen-irische-datenschutzbehoerde-zugelassen/32.390.982>, 24. 10. 2013.

254 *NSA/PRISM: Anzeigen gegen europäische Tochterunternehmen von Facebook, Apple, Microsoft, Skype und Yahoo eingebracht*, europe-v-facebook.org, <http://europe-v-facebook.org/DE/de.html>, 19. 10. 2013.

255 Pored ovih navoda istraživanje je pokazalo da 30 odsto svih kompanija ne pruža nikakve informacije o mogućnostima za rešavanje sporova, suprotno pravilima Safe Harbour. Kompanije

kvo ponašanje podneto je 6 tužbi nadležnoj Federalnoj komisiji za trgovinu (FTC), koja bi trebalo da sprovodi Safe Harbour sporazum. Međutim, ni jedan od ovih prestupa nije bio sankcionisan.²⁵⁶ Svakako je jasno, da Safe Harbour nema odredbe kojima bi se sprečile aktivnosti tipa NSA za špijuniranje građana EU.

Kolika je razlika u pristupu pojedinih država članica EU pokazuje i to da nemačka kancelarka Angela Merkel, a i nemačke institucije imaju potpuno suprotno mišljenje od irske službe za zaštitu podataka. Tako su nemačke nadležne institucije saopštile da Safe Harbour više ne predstavlja adekvatnu zaštitu za evropske građane i da više ne žele da primenjuju ovu konvenciju, nakon saznanja o aferi PRIZMA.

Pošto irske institucije, kojima se Šrems obratio nisu želele da donesu odluku u ovom slučaju, time još uvek nisu iscrpljena sva pravna sredstva u Irskoj. Tako se Šrems odlučio da u međuvremenu pokrene spor pred Vrhovnim sudom „High Court“ u Dublinu. Cilj ove tužbe je bio da prinudi irske sudove da pokrenu postupak protiv Fejsbuka.²⁵⁷ Međutim Šremsu je za taj postupak potrebna velika finansijska pomoć, pa prikuplja novac da bi mogao da plati sudske troškove. Radi se o sumi između 100.000 i 300.000 evra.²⁵⁸ Čim više ne bude postojala mogućnost žalbe višem sudu, kao najbolje moguće rešenje za ostvarenje pravde u ovom slučaju bilo je moguće još podneti tužbu protiv države Irske pred Evropskim sudom za ljudska prava u Strazburu. „Jedno je činjenica, da Evropljani upiru prstom na SAD, a drugo je da i sami ne spovode sopstvene zakone“, govorio je tada Maks Šrems.²⁵⁹ Upravo je promena nivou zaštite u okviru EU donošenjem Opšte uredbe o zaštiti podataka stvorila dobru pravnu bazu za jednak pristup ovakvim pravnim pitanjima.

4.4.3. Presuda Evropskog suda slučaj Safe Harbour

Jedina tužba, koju Šrems u Irskoj nije povukao ticala se programa PRIZMA i masovnog nadzora komunikacija EU građana. Ova tužba završila je pred Evropskim

koje prikazuju mogućnosti za rešavanje sporova, upućuju na agencije koje naplaćuju hiljade dolara za podnošenje tužbe. Preko 460 članova navodi američko udruženje za arbitražu kao svog provajdera za rešavanje sporova, koje naplaćuje podnošenje tužbe između 120 i 1.200 dolara po satu sa četiri sata minimalne naknade, uz dodatnih 950 dolara administrativnih troškova. Nikolaj Nielsen, *Stotine kompanija iz Sjedinjenih država navodilo neistine o zaštiti podataka*, Partneri za demokratske promene Srbija, Portal zaštita podataka o ličnosti, izvor: euobserver, <http://partners-serbia.org/privatnost/aktuelno/stotine-us-kompanija-pribeglo-neistinitim-izjavama-o-zastiti-podataka/>, 19. 10. 2013.

256 Nikolaj Nielsen, *Stotine kompanija iz Sjedinjenih država navodilo neistine o zaštiti podataka*, Partneri za demokratske promene Srbija, Portal zaštita podataka o ličnosti, izvor: euobserver, <http://partners-serbia.org/privatnost/aktuelno/stotine-us-kompanija-pribeglo-neistinitim-izjavama-o-zastiti-podataka/>, 19. 10. 2013.

257 *Behörde will jetzt auch „Facebook“-Verfahren abdrehen*, Studenten gezwungen Datenschutzbehörde zu verklagen. europe-v-facebook.org, <http://europe-v-facebook.org/DE/de.html>, 19. 10. 2013.

258 Dosada je Šrems prikupio 47500 evra. Pokrenuta je onlajn akcija za skupljanje priloga. Na veb stranici se može videti kolio je trenutno sredstava uplaćeno, a putem veb stranice se može i dati prilog. <https://www.crowd4privacy.org/?lang=en>, 19. 10. 2013.

259 *PRISM: Facebook und Apple dürfen nach EU-Recht Daten an NSA liefern. Irische Behörde sagt, dass USA ‚angemessenen‘ Datenschutz bieten.*, europe-v-facebook.org, http://www.europe-v-facebook.org/PA_de_25_7.pdf, 19. 10. 2013.

sudom, pošto je irski Vrhovni sud zatražio mišljenje u vezi sa masovnim nadzorom EU građana.²⁶⁰

Sudska odluka po ovom pitanju imala je dalekosežne posledice na globalnu privredu. Nije se radilo samo o Fejsbuku, nego i o Amazonu, Eplu, Ebeju, Guglu, Tviteru i preko 4000 američkih kompanija, koje svakodnevno koriste podatke evropskih građana. Osim toga ova sudska odluka imala je uticaja na prenos podataka između svih EU država i SAD. Radi se pre svega o podacima klijenata i zaposlenih od strane velikih kompanija kao što su Fejsbuk, Gugl, Majkrosoft itd, ali takođe i o podacima malih i srednjih kompanijama (kompanije koje su prenele svoje servise u SAD npr. računarstvo u oblacima „cloud“, knjigovodstvo itd.), koje su se pouzdale u ovaj sporazum.

Presudi Evropskog suda predhodilo je mišljenje Evropskog advokata. Evropski advokat Yves Bot je utvrdio da serveri u SAD ne predstavljaju „sigurnu luku“ za evropske građane.²⁶¹

Radilo se generalno o zaštiti podataka o ličnosti evropskih građana u slučaju njihovog prenosa na servere koji se nalaze u SAD.

U pogledu nivoa zaštite podataka u SAD, nakon obelodaljivanja Edvarda Snoudena advokat je ustanovio da: „pristup američkih tajnih službi predstavlja mešanje u pravo privatnosti i pravo zaštite podataka o ličnosti“.

Što se tiče sporazuma „sigurna luka“, irski Vrhovni sud je tražio od Evropskog suda da se izjasni da li ovaj sporazum pruža dovoljan nivo zaštite podataka u zemljama trećeg sveta (zemljama van EU).

Prema mišljenju evropskog advokata to bi značilo za evropske građane, da oni nemaju nikakve mogućnosti da se suprotstave špijuniciranju njihovih podataka u SAD, što predstavlja povredu Povelje Evropske unije o temeljnim pravima po pitanju prava na delotvornu žalbu.

Osim toga evropski advokat smatra da „shodno Direktivi o zaštiti podataka opstanak odluke Evropske komisije, sa kojom je utvrđen adekvatan nivo zaštite podataka građana EU, ne može niti da odstrani niti da umanjí ovlašćenja nacionalnih institucija za zaštitu podataka“.

Sama odluka Evropske komisije prema njegovom mišljenju ne sadrži adekvatne garancije, da će masovan i generalni pristup podacima biti sprečen. Advokat je i mišljenja da je odluka Evropske komisije nevažeća.²⁶²

Presuda Evropskog suda je sledila mišljenje Evropskog advokata Yves Bot. Ovom presudom je sporazum „Safe Harbour“ proglašen nevažećim.²⁶³

260 Facebook-“Datenschutz-Sammelklage“ vor dem EuGH, portal futurezone.at, <https://futurezone.at/netzpolitik/facebook-datenschutz-sammelklage-vor-dem-eugh/275.932.118>, 20. 9. 2017.

261 Pressemitteilung Nr. 106/15, Luxemburg, den 23. September 2015, Schlussanträge des Generalanwalts in der Rechtssache C-362/14 Maximilian Schrems / Data Protection Commissioner, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106de.pdf>, 20. 10. 2017.

262 Thomas Pany, *EuGH-Generalanwalt: Daten von Europäern in USA unsicher*, <https://www.heise.de/tp/features/EuGH-Generalanwalt-Daten-von-Europaeern-in-USA-unsicher-3375632.html>, 20. 10. 2017.

263 Pressemitteilung Nr. 117/15, Luxemburg, den 6. Oktober 2015, Urteil in der Rechtssache C-362/14, Maximilian Schrems / Data Protection Commissioner, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117de.pdf>, 20. 10. 2017.

U presudi je izričito naglašeno da kada su u pitanju osnovna ljudska prava pri transferu privatnih podataka ne mogu se isključiti niti ograničiti ovlašćenja nacionalnih institucija za zaštitu podataka.

Sudije su dakle sporazum iz 2000. godine „Safe Harbour“ proglasile nevažećim. Prema mišljenju sudija „Sama Evropska komisija je morala da ustanovi da SAD zbog svojih unutrašnjih propisa ili međunarodnih obaveza nije u stanju da garantuje nivo zaštite podataka identičan kao u EU shodno Povelji EU i Direktivi EU o zaštiti podataka“.

Kao što je advokat Yves Bot ustanovio, nivo zaštite osnovnih ljudskih prava pri transferu podataka u SAD nije garantovan. Snoudenova obelodanjivanja su ukazala na zadiranje američkih institucija u osnovna prava evropskih građana. Pri tome odlukom Evropske komisije nije utvrđeno da u SAD postoje pravni mehanizmi da se ta zadiranja ograniče, niti da postoji delotvorna pravna zaštita protiv ovakvih zadiranja u prava evropskih građana.²⁶⁴ Građani EU nisu u mogućnosti da tuže, ukoliko dođe do zloupotrebe njihovih podataka. To mora da se omogući daljim sporazumima sa SAD po pitanju zaštite podataka.²⁶⁵

4.4.4. Privacy Shield

Nakon što je sporazum Safe Harbour proglašen nevažećim, Evropska komisija je usvojila Privacy Shield. Sporazum je stupio na snagu 12.7.2016., a počeo da važi od 1.8.2016. godine.²⁶⁶

Prema Evropskoj komisiji sporazumom su predviđena stroga pravila za firme, koje obrađuju podatke. Vodiće se lista firmi, koje su se svojevotjno priključile sporazumu. Ukoliko se firme ne pridržavaju pravila moraće da računaju na sankcije i brisanje sa liste.

Osim toga je osigurano da će institucije SAD pristupati podacima samo u najužim mogućim granicama i uz maksimalne zaštitne mere. Ova garancija stoji samo na papiru, pošto faktički nije sprovedena ni jedna zakonska promena. Time bi trebalo da bude isključeno masovno špijuniranje evropskih građana.

Pored toga će Ministarstvo spoljnih poslova SAD konstituisati instituciju ombudsmana, koji je nadležan za žalbe evropskih građana u pogledu tema vezanih za nacionalnu bezbednost.²⁶⁷

264 Thomas Pany, *Safe-Harbour-Abkommen zwischen EU und USA für ungültig erklärt*, <https://www.heise.de/tp/features/Safe-Harbour-Abkommen-zwischen-EU-und-USA-fuer-unguelteig-erklart-3375857.html>, 20. 10. 2017.

265 Hauke Gierow, *EuGH erklärt Safe Harbor für ungültig*, <https://www.golem.de/news/klage-um-facebook-daten-eugh-erklart-safe-harbour-fuer-unguelteig-1510-116712.html>, 20. 10. 2017.

266 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.207.01.0001.01.ENG&toc=OJ:L:2016:207:FULL, 1. 11. 2017.

267 Martin Holland, *Privacy Shield: Umstrittene Regeln für Datentransfers in die USA treten in Kraft*, <https://www.heise.de/newsticker/meldung/Privacy-Shield-Umstrittene-Regeln-fuer-Datentransfers-in-die-USA-treten-in-Kraft-3264988.html>, 1. 11. 2017.

Ukoliko pojedinac smatra da su mu prava shodno sporazumu povređena, on svoja prava može ostvariti bez previsokih troškova. Postoji mogućnost da sama firma reši problem, potom mogućnosti arbitražnog rešenja spora, a moguće je i da se EU građani obrate svojim nacionalnim institucijama za zaštitu podataka. U ovom poslednjem slučaju se nacionalna institucija za zaštitu podataka u saglasnosti sa Federalnom trgovinskom komisijom SAD (Federal Trade Commission) stara da se omogući pravo na žalbu. Ukoliko se i ova mogućnost istroši, postoji mogućnost sudskog postupka.²⁶⁸

Funkcionalnost sporazuma će se svake godine zajednički ocenjivati. Posebno će biti ispitani pristup podacima građana EU kao i sprovođenje sporazuma. Ova ispitivanja obavljaće zajedno Evropska komisija i Ministarstvo trgovine SAD uz saradnju veštaka tajne službe SAD i veštaka za zaštitu podataka evropskih institucija za zaštitu podataka.²⁶⁹

Prema mišljenju Maksa Šremsa ovaj sporazum je „miljama udaljen od onoga, šta je Evropski sud presudio“. Jan Filip Albreht jedan od ključnih stručnjaka u donošenju Opšte uredbe o zaštiti podataka je sporazum ocenio kao „blanko ček za transfer podataka u SAD bez adekvatne zaštite podataka“.²⁷⁰ Kao i Safe Harbour i ovaj sporazum nudi nedovoljno mogućnosti za pravnu zaštitu evropskim građanima.²⁷¹

Prema Đovani Butareliju nezavisnom savetniku evropskih institucija ovaj sporazum zahtevao je od starta značajna poboljšanja. Uopšte glavni cilj Privacy Shield sporazuma je da zaštiti evropske građane od masovnog nadzora. Mogućnost nadzora institucija za zaštitu podataka, transparentnost i garancije prava zaštite podataka su u ovom kontekstu neophodne. Osim toga sam sporazum ne nudi izmenu zakonodavstva, već predstavlja jednu vrstu samoobavezivanja SAD.²⁷²

Ekspertska grupa za zaštitu podataka EU (Article 29 Working Party) izdala je saopštenje povodom donošenja ovog sporazuma. U saopštenju se između ostalo pozdravlja donošenje sporazuma, ali se i ukazuje na bitne nedostatke u njemu. Najviše problema je prema mišljenju ove grupe u pogledu komercijalnih aspekata i u pogledu pristupa državnih organa SAD podacima evropskih građana.

Kada su u pitanju komercijalni aspekti zamera se npr. nedostatak pravila vezanih za automatsku obradu podataka i generalno nedostatak prava na prigovor.

268 Evropska komisija je izdala i vodič za sporazum Privacy Shield, koji objašnjava prava pojedinaca, mogućnost žalbe protiv firmi i mogućnost žalbe protiv institucija SAD. European Commission, Directorate-General for Justice and Consumers, Guide to the EU-US Privacy Shield, 2016., http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf, 1. 11. 2017.

269 Europäische Kommission — Pressemitteilung, Europäische Kommission lanciert EU-US-Datenschutzschild: besserer Schutz für den transatlantischen Datenverkehr, Brüssel, 12. Juli 2016, http://europa.eu/rapid/press-release_IP-16-2461_de.htm, 1. 11. 2017.

270 Jan Philipp Albrecht, Press release, *EU-US Privacy Shield, EU Commission signs blank cheque for data transfers*, <https://www.greens-efa.eu/en/article/eu-us-privacy-shield/>, 1. 11. 2017.

271 Marc Störing, *Privacy Shield: EU-Parlament sieht Defizite beim transatlantischen Datenaustausch*, <https://www.heise.de/newsticker/meldung/Privacy-Shield-EU-Parlament-sieht-Defizite-beim-transatlantischen-Datenaustausch-3677682.html>, 1. 11. 2017.

272 Press release, Privacy Shield: more robust and sustainable solution needed, Brussels, 30 May 2016, https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2016-11-privacysield_en.pdf, 1. 11. 2017.

Ostalo je nejasno i to kako će se sam sporazum i njegovi principi primeniti na odgovorna lica za obradu podataka o ličnosti.

U pogledu pristupa državnih organa SAD podacima evropskih građana grupa „Article 29 Working Party“ je očekivala striktno garancije vezane za nezavisnost i ovlašćenja ombudsmana. Osim toga u pogledu masovnog prikupljanja podataka o EU građanima i pored uveravanja američkih tajnih službi, ne postoje konkretne garancije da se masovna prikupljanja podataka ne sprovode.²⁷³

Američka administracija je po stupanju sporazuma na snagu napravila veb sajt www.privacyshield.gov na kome se može pogledati, koje firme žele da ispune ovaj sporazum. Pri tome se dakle radi o tome da žele, a ne moraju.²⁷⁴ Fejsbuk, Gugl, Majkrosoft se nalaze na listi firmi koje su se samoobavezale na poštovanje ovog sporazuma.

Jedno je nesumljivo, da će praksa pokazati sve prednosti i nedostatke novog sporazuma.

273 Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf, 1. 11. 2017.

274 Christiane Schulzki-Haddouti, *Provisorium für Privatsphäre*, <https://www.heise.de/tr/artikel/Provisorium-fuer-Privatsphaere-3538477.html>, 1. 11. 2017.

5. FEJSBUK I SUDSKA PRAKSA

U ovom poglavlju će biti razmatrani najzanimljiviji slučajevi iz postojeće sudske prakse.

5.1. Fejsbuk zaštita prava ličnosti i autorskih prava

Slučaj 1: Preuzimanje slika sa Fejsbuk profila koji nisu javni predstavlja povredu ličnih prava

Preuzimanje slika sa sa Fejsbuk profila koji nisu javni u svrhu objavljivanja novinskog izveštaja predstavlja povredu ličnih prava.²⁷⁵

Suprug je zbog seksualnog uznemiravanja svoje žene krajem 2011. godine osuđen na 6 godina zatvora. Novinsku kuću tužila je supruga osuđenog. Tužena novinska kuća je izveštavala o istrazi tužilaštva o ovom slučaju i između ostalog objavila fotografije na kojoj se mogla videti supruga osuđenog. Fotografije su poticale sa Fejsbuk profila supruge osuđenog, koji nije bio javno dostupan. Iako su objavljene fotografije bile zamagljene, bilo je moguće prepoznati suprugu osuđenog. Pored toga je supruga osuđenog i navedena u novinskom izveštaju.²⁷⁶

Sud za radne sporove u Minhenu je presudio da je povređeno pravo ličnosti tužioca zbog objavljivanja fotografija. Tužilac ne samo da se nije saglasio sa objavljivanjem fotografija, nego se ne radi o fotografiji javne ličnosti. Iako kod muža nije ustanovljeno da li se radi o javnoj ličnosti, njegova supruga u svakom slučaju nije bila javna ličnost. Stoga je objavljivanje u novinama bilo protivpravno. Novinska kuća je osuđena na novčanu kaznu od 1200 evra shodno čl. 823 st. 1 nemačkog Građanskog zakonika.²⁷⁷

Ova sudska odluka je otvorila pitanje, kada je uopšte dozvoljeno upotrebljavati slike sa Fejsbuk profila. U osnovi upotreba nije dozvoljena, ukoliko fotografije potiču iz profila, koji nije javno dostupan. Stoga se polazi od toga da je korisnik

275 Presuda iz 2012. godine (Urteil vom 15. 6.2012, Az.: 158 C 28716/11), Sud za radne sporove Minhen (AG München).

276 Portal aufrecht.de, *Wann dürfen Fotos aus Facebook-Profilen in Zeitungsberichten verwendet werden?*, <http://www.aufrecht.de/beitraege-unsere-anwaelte/medienrecht-presserecht/ag-muenchen-fotos-aus-nichtoeffentlichem-facebook-account-duerfen-nicht-von-der-presse-verwendet-werden.html>, 4. 9. 2017.

277 Portal kostenlose-urteile.de, *Private Fotos auf Facebook: Veröffentlichung in der Zeitung von nicht der Öffentlichkeit bestimmten Fotos stellt Verletzung des allgemeinen Persönlichkeitsrechts dar*, http://www.kostenlose-urteile.de/AG-Muenchen_158-C-2871611_Private-Fotos-auf-Facebook-Veroeffentlichung-in-der-Zeitung-von-nicht-der-Oeffentlichkeit-bestimmten-Fotos-stellt-Verletzung-des-allgemeinen.news15371.htm, 4. 9. 2017.

Fejsbuka želeo da podeli svoje fotografije sa krugom prijatelja, a ne sa javnošću. Zbog toga se može smatrati i da ne postoji saglasnost korisnika za dalju upotrebu.

Slučaj 2:

Javne fotografije sa Fejsbuka se smeju kopirati u privatne svrhe

Spor se ticao međusobnih tužbi bivših kolega, koji su izbačeni iz jedne firme. U sporu vezanom za fotografije je jedan kolega posedovao fotografije drugog kolege sa njegovog Fejsbuk profila. Iste je iskopirao radi obezbeđenja dokaza protiv kolege.²⁷⁸

Fotografije, koje Fejsbuk korisnici objavljuju, a koje su javno dostupne, smeju se kopirati u privatne svrhe, odlučio je Sud za radne sporove u Kelnu.²⁷⁹ Dalje objavljivanje istih dopušteno je samo uz saglasnost korisnika. Presuda je izečena početkom 2015. godine.

Kopiranje u privatnu svrhu regulisano je čl. 53 nemačkog Zakona o autorskim pravima. Kopiranje važi i u onlajn svetu i samim time važi i na Fejsbuku. Ova norma ni u kom slučaju ne dozvoljava komercijalno korišćenje ili publikovanje na sopstvenoj veb stranici.

Slučaj 3:

Korišćenjem funkcije podeli („share“) se ne prisvajaju tuđa autorska dela kao svoja

Krajem 2015. godine Viši sud u Frankfurtu je presudio, da onaj ko koristi funkciju podeli „eng. share“ na Fejsbuku ne prisvaja kao svoje time protivpravne tuđe sadržaje i samim tim ne odgovara.²⁸⁰ Radi se o protivpravnim sadržajima koje postavljaju drugi Fejsbuk korisnici, a koji krše lična prava, autorska prava ili su u suprotnosti sa odredbama krivičnog prava.

Tužilac je bio Savez za zaštitu životinja koji je kritičko mišljenje jednog danskog Saveza za zaštitu životinja podelio putem Fejsbuka. Tuženi je urednik i operator jednog internet sajta, koji je na deljenje od strane Saveza za zaštitu životinja napisao da je Savez sam izjavio ovo kritičko mišljenje. Takođe je objavio naslov, koji je glasio: „XXX Savez je uporedio danske pse sa Jevrejima“. Na ovo se žalio Savez sudu i tužio urednika i operatora veb sajta.²⁸¹

Sud je Savezu dao za pravo, da sa time što je korištena funkcija „podeli“ ne znači da je korisnik Fejsbuka uzео kao svoje tuđe sadržaje.

278 Frank Weiß, *Kopieren von Facebook-Fotos kann zulässig sein*, <https://www.ratgeberrecht.eu/urheberrecht-aktuell/kopieren-von-facebook-fotos-kann-zulaessig-sein.html>, 4. 9. 2017.

279 Presuda iz 2015. godine (Urteil vom 19. 1. 2015 — Az.: 2 Sa 861/13), Sud za radne sporove Keln (LAG Köln).

280 Presuda iz 2015. godine (Urteil vom 26. 11. 2015 — Az.: 16 U 64/15), Viši sud u Frankfurtu (OLG Frankfurt).

281 Jan Gerth, *OLG Frankfurt am Main: Kein Zueigenmachen durch Teilen eines Beitrags auf Facebook*, portal jurablogs, <https://www.jurablogs.com/2016/11/15/olg-frankfurt-am-main-kein-zueigenmachen-durch-teilen-eines-beitrags-auf-facebook>, 7. 9. 2017.

Funkcija dugmeta „podeli“ je doduše slična u tehničkom smislu funkciji linka, ali se više radi o mogućnosti da se ukaže na privatne sadržaje drugih Fejsbuk korisnika. U odnosu na dosadašnju sudska praksu vezanu za linkove se ne može smatrati da se sadržaji podeljeni putem linkova prisvajaju kao sopstveni sadržaji. Postavljač linka prisvaja sadržaje koje je putem linka postavio, tek onda kada se sa njima identifikuje, tako da se mogu smatrati kao da su njegovi.

Drugačije u odnosu na „lajk“ funkciju, kod funkcije „podeli“ se radi o isključivo o širenju sadržaja. Sa druge strane kod „lajk“ funkcije se radi više o izražavanju saglasnosti sa određenim sadržajem.²⁸²

Slučaj 4:
Funkcijom podeli se ne prisvajaju tuđi sadržaji,
osim u posebnim slučajevima

Početnom 2017. godine Viši sud u Drezdenu je prosudio, da u osnovi samo deljenje preko Fejsbuka ne vodi ka tome da se prisvajaju tuđi sadržaji. Prisvajanje postoji onda kada Fejsbuk korisnik sadržaje pozitivno komentariše ili se o njima pozitivno izražava (npr. putem lajk dugmeta) i kada se sa sadržajima identifikuje.²⁸³

U slučaju se radilo o pitanju, da li korisnik Fejsbuka odgovara za sadržaje koje deli, ukoliko ih prisvoji kao svoje. Viši sud u Drezdenu je negirao ovo pitanje, jer se samo deljenje smatra kao napomena da se sadržaji drugih pogledaju i ništa više od toga. Redovno se ova funkcija koristi da bi se sadržaji brže proširili. Situacija se menja kada korisnik podeljene sadržaje komentariše ili se na poseban način sa istim identifikuje.²⁸⁴

U ovom slučaju je Fejsbuk korisnik napisao, da je veb stranica pisca „vredna razmatranja, toliko da se zaobiđe“. Na stranici, koja je podeljena je poistovećena nemačka kancelarka Angela Merkel sa Adolfom Hitlerom. Samim komentarisanjem se korisnik izjasnio i izrazio o sadržaju i identifikovao sa istim, tako da se može smatrati da postoji prisvajanje.

Pri deljenju sadržaja treba obratiti pažnju, da samo deljenje ne uzrokuje odgovornost. Ipak se savetuje oprezno deljenje sadržaja, jer se svaka dodatna aktivnost u ovom kontekstu npr. uz korišćenje lajk dugmeta ili uz komentarisanje može smatrati kao poistovećivanje sa sadržajem i prisvajanje tuđih izjava kao svojih. Na taj način se ustanovljava odgovornost u pravnom smislu. Da bi se to izbeglo preporučuje se samo koršćenje deljenja bez dodatnih aktivnosti.²⁸⁵

282 Frank Weiß, *Kein Zueigenmachen fremder Inhalte bei Facebook durch „Teilen“*, <https://www.ratgeberrecht.eu/internetrecht-aktuell/kein-zueigenmachen-fremder-inhalte-bei-facebook-durch-teilen.html>, 7. 9. 2017.

283 Presuda iz 2017. godine (Urteil vom 07. 2. 2017 — Az.: 4 U 1419/16), Viši sud u Drezdenu (OLG Dresden).

284 Sascha Leyendecker, *OLG Dresden: Haftung für „Teilen“ bei Facebook*, <http://www.jus-kanzlei.de/fachbeitrag/unternehmen-handel-und-technologie/olg-dresden-haftung-fuer-teilen-bei-facebook.html>, 8. 9. 2017.

285 Dennis Tölle, *OLG Dresden: „Teilen“ ist kein Zueigenmachen*, <https://www.tw-law.de/2017/03/13/medien-presserecht/olg-dresden-facebook-teilen-ist-kein-zueigenmachen/>, 4. 9. 2017.

Slučaj 5:
***Vlasnik Fejsbuk naloga odgovara za zloupotrebu svog
Fejsbuk naloga***

Polovinom 2016. godine Viši sud u Frankfurtu je presudio da vlasnik Fejsbuk naloga odgovara za protivpravne sadržaje, koje neovlašćeno treće lice postavi, ako pritom vlasnik naloga nedovoljno čuva svoje pristupne podatke.²⁸⁶

Na Fejsbuk profilu su se nalazili protivpravni, uvredljivi sadržaji. Tuženi se branio tako što je rekao da sadržaji nisu njegovi i da je njegov nalog od strane trećih lica zloupotrebjen. Sud je ustanovio da tuženi nije obratio dovoljno pažnje i da se nije adekvatno starao o tome da nikome svoje pristupne podatke ne prosleđuje. Tako se on često prijavljivao na Fejsbuk sa kompjutera prijatelja i poznanika, a da pritom nije mario za svoje pristupne podatke. Tuženi ne samo da nije vodio računa o tome da se nakon korišćenja tuđeg računara odjavi, nego je čak na tuđem kompjuteru aktivirao automatsku funkciju da taj računar zapamti njegove pristupne podatke.²⁸⁷

Viši sud u Frankfurtu je zbog zanemarivanja dužne pažnje ustanovio odgovornost vlasnika naloga za sprovedene protivpravne radnje trećeg lica. Stoga je vlasnik Fejsbuk naloga osuđen na novčanu kaznu u iznosu od 3.000 evra.

Onaj ko svoje pristupne podatke svog Fejsbuk naloga nedovoljno zaštiti od pristupa trećih lica, odgovara za zloupotrebu svog naloga od strane trećih lica. Ovo naročito važi za uvredljive sadržaje, povredu autorskih prava i povredu konkurencije.²⁸⁸

Slučaj 6:
Privatne Fejsbuk poruke se ne smeju javno objavljivati

Danas malo ko komunicira putem faksa ili pisma, već najčešće putem e-mejla i društvenih mreža. U ovoj sudskoj odluci, je odgovoreno na pitanje da li objavljivanje privatnih poruka na Fejsbuku krši lična prava autora.²⁸⁹

Korespondencija između autora (tužioca) i objavljivača (tuženog) je počela najpre na jednom portalu. Tu je autor imao izvesnu objavu, na koju je objavljivač reagovao i obratio se privatnom porukom autoru. Autor je potom poslao odgovor objavljivaču privatnom porukom na Fejsbuku. U toj poruci je autor naveo razloge, na osnovu kojih on ističe svoje pravo, da se njegova titula i poreklo ne smeju navoditi. Osim toga sam tekst poruke je obilovao jezičkim greškama.

286 Presuda iz 2016. godine (Urteil vom 21. 7. 2016 — Az.: 16 U 223/15), Viši sud u Frankfurtu (OLG Frankfurt).

287 Denise Himburg, *Inhaber von Facebook-Account haftet für Postings Dritter bei verschuldetem Accountmissbrauch*, https://www.anwalt.de/rechtstipps/inhaber-von-facebook-account-haftet-fuer-postings-dritter-bei-verschuldetem-accountmissbrauch_086140.html, 8. 9. 2017.

288 Martin Bahr, *OLG Frankfurt a.M.: Account-Inhaber bei Facebook haftet für missbräuchliche Nutzung durch Dritten*, <http://www.dr-bahr.com/news/urheberrecht/account-inhaber-bei-facebook-haftet-fuer-missbraeuchliche-nutzung-durch-dritten.html>, 8. 9. 2017.

289 Presuda iz 2013. godine (Beschluss vom 4. 2.2013 — 7 W 5/13), Viši pokrajinski sudi u Hamburgu (OLG Hamburg).

Tuženi je ovu privatnu poruku objavio u jednoj javnoj Fejsbuk grupi pod nazivom „Pošaljimo prevaranta u pakao“, pa je autor smatrao da je povređeno njegovo lično pravo i tužio objavljiivača.²⁹⁰

Hamburški sud je početkom 2013. godine zbog objavljiivanja poruke klasifikovao ovaj postupak kao kršenje zakona. Baš kao i svako iskazivanje misli, sadržaja i Fejsbuk poruka predstavlja manifestaciju ličnosti autora. Samom autoru ostaje da odluči u kojoj meri i formi njegove beleške želi da objavi u javnosti.

Izuzetak od prava raspolaganja pravom ličnosti i saglasnosti autora predstavlja opravdan interes za objavljiivanje. U ovom slučaju bi se to moglo opravdati javnim interesom, da se radilo o javnom službeniku kao autoru ove Fejsbuk poruke. Nasuprot tome je objavljiivanje iz čisto privatnih razloga nedopušteno.

Pošto interes javnosti u ovom slučaju nije uočen, radi se o povredi prava ličnosti autora. Navođenje porekla i titule autora ne predstavlja opravdan javni interes. Osim toga autor ne predstavlja ličnosti od javnog interesa. Stoga je sudija konstatovao povredu prava ličnosti autora.²⁹¹

Privatne poruke se generalno smatraju privatnim odnosno tajnim. Kod privatnih poruka ne igra nikakvu ulogu o kojoj se vrsti medija radi i koji je bio povod za njihovo objavljiivanje. Naročito se ovo odnosi na to kada autor poruke nije računao na to da će one biti objavljiivene. Isto kao i e-mailovi, ovakav način elektronske komunikacije je priznat i zakonski zaštićen u vidu poverljivosti reči i komunikacije uopšte. Drugačije se naravno tretiraju poruke koje su već objavljiivene na nekom od foruma.

Ukoliko ne postoji dobar razlog objavljiivača za objavljiivanje poruke, ne sme se poruka objavljiivati. Osim toga u ovom slučaju trebalo je obratiti pažnju i uzeti u obzir i to da je zbog jezičkih grešaka autor, kao posledica objavljiivanja, i javno osramoćen.

Jedno je nesumljivo, da niko ne bi prosledio i kopirao privatnu poštu i ostavio je na ulici. Onaj ko pošalje privatnu poruku putem Fejsbuka, treba da računa na to da ona neće biti objavljiivena. Ukoliko se dakle privatne poruke bez saglasnosti autora javno objave, mora se računati na tužbu zbog nečinjenja, kao i na zahteve za naknadu štete.²⁹²

Slučaj 7: Operatori stranica odgovaraju za postove svojih obožavatelja, koji krše autorska prava

U ovom slučaju je jedan Fejsbuk korisnik zaštićenu autorsku fotografiju jednog istaknutog građanina objavio na Fejsbuku. Operator stranice, na čijem profilu

290 Andrej Diligenski, *Privatne Fejsbuk poruke se ne smeju javno objavljiivati*, portal Zaštita podataka o ličnosti, <http://partners-serbia.org/privatnost/o-projektu/>, 10. 9. 2017.

291 Arno Lampmann, *OLG Hamburg: Private Facebook-Nachrichten dürfen nicht veröffentlicht werden*, <http://www.lhr-law.de/magazin/private-facebook-nachrichten-durfen-nicht-veroeffentlicht-werden>, 10. 9. 2017.

292 Martin Bahr, *OLG Hamburg: Private Facebook-Nachrichten dürfen nicht veröffentlicht werden*, <http://www.dr-bahr.com/news/datenschutzrecht/private-facebook-nachrichten-duerfen-nicht-veroeffentlicht-werden.html>, 10. 9. 2017.

se mogla videti sporna fotografija je bio upozoren na postojanje autorskih prava na fotografiji putem e-mejila. Pošto je reakcija operatora Fejsbuk stranice izostala došlo je do opomene od strane imaoca autorskog prava. Nakon što je i ova reakcija operatora izostala, autor je podneo tužbu za nečinjenje.

Polovinom 2012. godine sud u Štutgartu je odlučio, da operator Fejsbuk stranice treba da se uzdrži od prikazivanja sporne fotografije. Operator Fejsbuk stranice je takođe spornu fotografiju lajkovao i komentarisao, što sud nije uzeo ovom prilikom u obzir po pitanju odgovornosti.²⁹³

Treba imati u vidu i da je ova presuda proizašla iz propuštanja, te da se radi o tzv. propuštajućoj presudi. To znači da tuženi nije odreagovao na vreme u pogledu činjenja ili nečinjenja, pa se stoga nije ni ulazilo u utvrđivanje činjeničnog stanja, već se uzete činjenice smatraju kao tačne.²⁹⁴

Sud je ovom presudom naime potvrdio dosadašnju sudsku praksu u sličnim slučajevima, da operatori Fejsbuk stranice odgovaraju kada uprkos saznanju o protivpravosti sadržaja ne reaguju aktivno i protivpravni sadržaj bez odlaganja ne uklone. Tako je u ovom slučaju fotografija, koja krši tuđa autorska prava bila postavljena na jednu stranicu, a operator stranice je nije ukolonio, kada je saznao da se njom krše autorska prava.²⁹⁵

5.2. Fejsbuk i zaštita konkurencije

Slučaj 1:

Lajk dugme krši i pravo konkurencije i pravo zaštite podataka

Upotreba lajk dugmeta na veb stranici firme je u suprotnosti sa pravom zaštite podataka, ali i sa pravom lojalne konkurencije.²⁹⁶

Centrala za zaštitu potrošača Severne Rajne-Festfalije (Verbraucherzentrale NRW) pokrenula je inicijativu protiv postavljanja Fejsbukovog lajk dugmeta na veb stranicama firmi. Zaštitnici potrošača su bili stanovišta da Fejsbuk nedozvoljeno prenosi podatke.

Početakom 2015. godine sud u Dizeldorfu je presudio da operateri veb sajtova, treba da se uzdrže od upotrebe lajk dugmeta, pošto se već prilikom pozivanja veb stranice podaci prenose Fejsbuku. Tom prilikom se između ostalog prenose podaci o ličnosti kao što je IP-adresa. Ova vrsta prenosa zahteva predhodnu saglasnost korisnika, a pošto nje nije bilo, ovaj prenos podataka je nedozvoljen.

293 Presuda iz 2012. godine (Urteil vom 20. 7. 2012 — Az.: 17 O 303/12), Sud u Štutgartu (LG Stuttgart).

294 Robert Golz, *LG Stuttgart: Haftung für urheberrechtsverletzungen von User-Postings auf Facebook*, <https://www.haerting.de/neuigkeit/lg-stuttgart-haftung-fuer-urheberrechtsverletzungen-von-user-postings-auf-facebook>, 9. 9. 2017.

295 Arno Lampmann, *Weiteres Facebook-Urteil bezüglich von Dritten geposteter Inhalte — diesmal aus Stuttgart*, <https://www.lhr-law.de/magazin/weiteres-facebook-urteil-bezuglich-von-dritten-geposteter-inhalte-diesmal-aus-stuttgart>, 9. 9. 2017.

296 Presuda iz 2015. godine (Urteil vom 9. 3. 015, Az.: 12 O 151/15), Pokrajinski sud Dizeldorf (LG Düsseldorf).

Operateri veb stranica su odgovorni takođe, pošto oni integrišu ovaj društveni dodatak (eng. social plugin) u njihovim internet prezentacijama. Ovime se krši zakon o zaštiti podataka, ali se na ovaj način vrši povreda prava lojalne tržišne utakmice tj. konkurencije.²⁹⁷

Sud je za ocenjivanje nelojalne konkurencije uzeo u obzir normu čl. 2 br. 11 Zakona o tužbama za nečinjenje pri prekršajima o zaštiti potrošača.²⁹⁸ U obrazloženju svoje presude sud je naveo „da se radi o članovima 12 i 13 Zakona o elektronskim medijima, koji uzima u obzir ne samo član 2 br. 11 Zakona o tužbama za nečinjenje pri prekršajima o zaštiti potrošača, nego i član 3 a Zakona o zaštiti konkurencije. Upravo član 3 a Zakona o zaštiti konkurencije štiti ne samo lojalnu konkurenciju, nego i lična prava, pravo na informaciono samoodređenje. Takođe treba imati u vidu naglašen ekonomski značaj prikupljanja elektronskih podataka, koji se ne pojavljuju samo kao ekonomsko dobro, već prouzorkuju razvoj razumevanja prava zaštite podataka“.²⁹⁹

Inače je već dugo vremena u Nemačkoj bilo sporno, da li kršenja prava zaštite podataka istovremeno predstavljaju nedozvoljene radnje i kršenje prava konkurencije. Zakonom o poboljšanju sprovođenja građanskopravnih propisa vezanih za zaštitu podataka i zaštitu potrošača, koji je stupio na snagu 24.02.2016 dato je ovlašćenje savezima za zaštitu potrošača da opominju i tuže za povrede zaštite podataka. Ovom sudskom presudom je omogućeno da zaštitnici potrošača pored propisa vezanih za zaštitu podataka zaštite i tržište od nelojalne konkurencije.

Početakom 2017. godine, po žalbi na ovu presudu Viši sud u Dizeldorfu doneo je odluku da prekine postupak i obrati se Evropskom sudu sa sledećim pitanjima:³⁰⁰

1. Da li je shodno Direktivi o zaštiti podataka dopušteno da pored regulatornog tela za zaštitu podataka i prava pojedinaca na žalbu, mogu i neprofitna udruženja shodno nacionalnim propisima da postupaju protiv prekršioca Direktive o zaštiti podataka (shodno čl. 22, 23, 24 Direktive 95/46/EU)?

U slučaju negativnog odgovora pod br.1:

2. Da li se u slučaju ugrađivanja programskog koda u jednu veb stranicu, koju korisnici putem brauzera aktiviraju, a čiji sadržaji se zahtevaju i prenose trećim licima, može lice koje ugrađuje programski kod smatrati „odgovornim licem“ u smislu Direktive o zaštiti podataka (shodno čl. 2d Direktive

297 Martin Bahr, LG Düsseldorf: *Like-Button von Facebook datenschutzwidrig = Wettbewerbsverstöß*, <http://www.dr-bahr.com/news/wettbewerbsrecht/lg-duesseldorf-like-button-von-facebook-datenschutzwidrig-wettbewerbsverstoss.html>, 31. 8. 2017.

298 Zakon o tužbama za nečinjenje pri prekršajima o zaštiti potrošača, Gesetz über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (Unterlassungsklagengesetz — UKlaG) vom 27. August 2002 (BGBl. I S. 3422, 4346), das zuletzt durch Artikel 4 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2446) geändert worden ist. <https://www.gesetze-im-internet.de/uklag/BJNR317300001.html>, 2. 9. 2017.

299 Jan Lennart Müller, *LG Düsseldorf doesn't like Facebook: Der „Gefällt-mir“ bzw. „Like“-Button von Facebook ist nicht mehr ohne Weiteres verwendbar!*, <http://www.it-recht-kanzlei.de/lg-duesseldorf-facebook-like-button-datenschutzwidrig.html>, 1. 9. 2017.

300 Odluka iz 2017. godine (Beschluss vom 19.01.2017, Az.: I-20 U 40/16), Viši sud Dizeldorf (OLG Düsseldorf).

- 95/46/EU), a da pritom ono samo na ovaj postupak obrade podataka (prenos podataka) ne može da utiče?
3. U slučaju negativnog odgovora pod br. 2: Da li se na osnovu Direktive o zaštiti podataka (shodno čl. 2d Direktive 95/46/EU) može protumačiti, da je odgovornost isključivo regulisana, da se u tom smislu suprotstavlja građanskopravnim zahtevima protiv trećeg lica, koji se ne smatra „odgovornim licem“ u smislu Direktive o zaštiti podataka, ali predstavlja osnov za obradu podataka, bez da istu sam prouzrokuje?
 4. Da li „opravdani interesi“ u smislu Direktive o zaštiti podataka (shodno čl. 7f Direktive 95/46/EU) postoje na strani ugrađivača ili na strani trećih lica?
 5. Kome treba da se izjavi saglasnost u datim okolnostima (shodno čl. 2h i 7a Direktive 95/46/EU)?
 6. Da li obaveza obaveštavanja pojedinica u smislu Direktive o zaštiti podataka (shodno čl. 10 Direktive 95/46/EU) pogađa operatera veb stranice, koji ugrađuje sadržaje trećih lica i tako prouzrokuje obradu ličnih podataka od strane trećih lica?

Odgovor na sva ova pitanja imaće veliki uticaj na primenu u praksi i po pitanju zaštite podataka, ali i po pitanju zaštite lojalne tržišne utakmice. U zavisnosti kakva odluka Evropskog suda bude bila, biće osnažena ili oslabljena prava zaštite potrošača, ali i prava na zaštitu podataka o ličnosti. Osim toga odluka u ovom slučaju će definitivno potvrditi ili negirati vezu zaštite konkurencije i zaštite podataka.³⁰¹

Slučaj 2: **Lajk dugme ne krši pravo konkurencije kao uslov** **slobodne tržišne utakmice**

Nemačka firma Allmedia GmbH je opomenula onlajn prodavce, koji nisu u njihovoj politici privatnosti ukazali na upotrebu društvenih dodataka „eng. Social Plugin“ od strane Fejsbuka. Ovo su obrazložili time da su suparnici na tržištu pogođeni zbog nelojalne konkurencije. Pošto je ovo upozorenje ignorisano, došlo se do sudskog spora.³⁰² Početkom 2011. godine po ovom pitanju sudsku odluku je doneo pokrajinski sud za zaštitu konkurencije (kartela) grada Berlina.³⁰³ Ovime je odbijen zahtev firme Allmedia GmbH za privremenu zabranu onlajn prodavnica, koje su koristile lajk dugme.³⁰⁴ U ovom slučaju radilo se o dva veb sajta, koji su bili onlajn prodavci. Konkurent na tržištu je na svom veb sajtu postavio lajk dugme. Podnosilac zahteva je zastupao stanovište da izostavljeno uputstvo za posetioce sajta

301 Martin Bahr, *OLG Düsseldorf legt Fragen zum Like-Button von Facebook dem EuGH vor*, <http://www.dr-bahr.com/news/olg-duesseldorf-legt-fragen-zum-like-button-von-facebook-dem-eugh-vor.html>, 31. 8. 2017.

302 *Like-Button nicht wettbewerbswidrig*, RA Daniel Dingeldey, domain recht.de, KG Berlin (Odluka od 29. 4. 2011 Az.: 5W 88/11), <http://www.domain-recht.de/magazin/domain-news-2011/kg-berlin-like-button-nicht-wettbewerbswidrig-id667963.html>, 7. 8. 2012.

303 Thomas Schwenke, *Erste Abmahnung wegen Facebooks Like-Button (und wie man sie vermeidet)*, <http://spreerecht.de/abmahnung/2011-02/erste-abmahnungen-wegen-facebooks-like-button-und-wie-man-sie-vermeidet>, 7. 8. 2012.

304 LG Berlin Az. 91 O 25/11 odluka od 14. 3. 2011.

od strane suparnika o vrsti, obimu i svrsi prikupljanja ličnih podataka, predstavlja povredu prava konkurencije. Sud je obrazložio njegovu odluku, da bi podneti zahtev za prestanak uznemiravanja veb prostora protiv suparnika (konkurenta) na tržištu bio prihvaćen, da se radilo o povredi ponašanja na tržištu shodno nemačkom pravu. Ipak, treba imati u vidu da se sud u ovom slučaju nije bavio zaštitom podataka, već je ispitao aspekte slobodne tržišne utakmice na internetu i da se radi o starijoj sudskoj odluci iz 2011. godine u odnosu na predhodni slučaj, gde je nemačko pravo u međuvremenu regulisalo ovu tematiku.

Slučaj 3:
Lajk dugme ne krši pravo konkurencije kao uslov za učešće u nagradnoj igri

Početakom 2013. godine sud u Hamburgu je odlučio da preduzeća ne krše pravo konkurencije, ukoliko učešće u nagradnoj igri uslove klikom na lajk dugme.³⁰⁵

Sudski postupak pokrenuo je Savez za zaštitu potrošača, koji je video u ovom ponašanju dovođenje u zabludu od strane holadnskog prodavca, koji je putem Fejsbuka pokušao da uslovi učešćem u nagradnoj igri. Sud je negirao povredu prava konkurencije, pošto sudije nisu prepoznale dovođenje u zabludu.³⁰⁶

Lajk dugme po njima ima samo jedno neutralno dejstvo, pošto ni Fejsbuk ni korisnici ne mogu da u toj opciji razaznaju važno od nevažnog. Da se dopadne i može i sme Fejsbuk korisnicima zaista sve. Fejsbuk korisnici su stoga dobro upoznati, da klikom na lajk dugme dolazi do uopštenog izražavanja o sviđanju. Ovo izražavanje sviđanja nečega nije ipak neobavezujuće. Za bliže kvalifikovanje dopadanja nečega zasigurno treba uzeti stavljanje na zid „postovanje“. Ukoliko Fejsbuk korisnik ne postuje nešto, nego samo lajkuje, ostaće sakriveni bliži razlozi ili motivi za klik na lajk dugme. Stoga se lajk dugmetu ne može prepisati relevantno značenje, pa se putem ovog dugmeta ne može dovesti u zabludu, jer je tuženi spajanjem sa učešćem u nagradnoj igri sakupljao lajkove.³⁰⁷

Slučaj 4:
Friend Finder opcija krši pravo lojalne konkurencije, kao i kazna od 100.000 evra zbog IP klauzule

Odlukom Vrhovnog suda Nemačke presuđeno je da je opcija „Friend Finder“ predstavlja jednu maltretirajuću reklamu u suprotnosti sa pravom konkurencije, kojom Fejsbuk šalje pozivnice putem e-mejla licima, koje nisu članovi ove društvene mreže.³⁰⁸ Sud je takođe ustanovio, da je Fejsbuk u okviru svog postupka regi-

305 Presuda iz 2013. godine (Urteil vom 10. 1. 2013 — Az.: 327 O 438/11) Sud Hamburg (LG Hamburg).

306 Portal absatzwirtschaft.de, *Gewinnspiel-Teilnahme durch Klicken des „Gefällt mir“-Buttons ist legitim*, <http://www.absatzwirtschaft.de/gewinnspiel-teilnahme-durch-klicken-des-gefällt-mir-buttons-ist-legitim-14441/>, 3. 9. 2017.

307 Benedikt Adams, *LG Hamburg: Gewinnspiel-Teilnahme durch Klicken des „Gefällt mir“-Buttons nicht wettbewerbswidrig*, <http://raschlegal.de/aktuelles/lg-hamburg-gewinnspiel-teilnahme-durch-klicken-des-gefällt-mir-buttons-nicht-wettbewerbswidrig/>, 3. 9. 2017.

308 Presuda iz 2016. godine (Urteil vom 14. Januar 2016 — I ZR 65/14), Vrhovni sud Nemačke (BGH).

stracije iz novembra 2010. godine dovedio u zabludu sa ovom funkcijom korisnike na način što je koristio podatke iz njihovih kontakata. Sudska odluka donešena je početkom 2016. godine.

Tužiocima su bili najvažniji savezi udruženja potrošača Nemačke, dok je tužena strana bila Fejsbuk Irska. Zaštitnici potrošača su podneli tužbu za nečinjenje. Slanje e-mail pozivnica korisnicima koji nisu članovi Fejsbuk društvene mreže predstavljalo je po njima maltretirajuću reklamu u smislu čl. 7 st. 2 i 3 br. 3 nemačkog Zakona o zaštiti konkurencije. Osim toga tuženi obmanjuju korisnike u okviru postupka registracije na društvenu mrežu Fejsbuk, tako što koristi e-mail adrese korisnika na nedozvoljen način ubacivanjem korisnika u reklame Fejsbuka.

Osim povrede zaštite podataka, ova opcija slanja pozivnica od strane Fejsbuka korisnicima, koji se nisu izričito sa takvim mejlovima saglasili, predstavlja nedozvoljeno uznemiravanje u smislu čl. 7 st. 2 br. 3 nemačkog Zakona o zaštiti konkurencije.³⁰⁹ Pozivnice putem e-mejllova od strane Fejsbuka, služe da se ostali internet korisnici privuku na ponudu Fejsbuka. Stoga se ove pozivnice ne mogu tretirati kao privatna saopštenja Fejsbuk korisnika, nego kao reklama od strane Fejsbuka.

Osim toga tuženi Fejsbuk je u novembru 2010. godine putem navoda vezanih za registraciju korišćenjem opcije Friend Finder prekršio i čl. 5 nemačkog Zakona o zaštiti konkurencije, pošto je registrovane korisnike obmanuo o vrsti i obimu korišćenja podataka vezanih za e-mejllove. Prvi korak u registraciji bila je napomena „Da li su tvoji prijatelji već na Fejsbuku?“. Međutim tom prilikom nije objašnjeno da će podaci o svim mejlovima korisnika iz kontakata biti prosleđeni Fejsbuku i da će Fejsbuk ove podatke obraditi i poslati pozivnice trećim licima, kao da ih šalju njihovi prijatelji.³¹⁰

Odluci Vrhovnog suda Nemačke predhodile su odluke nižih sudova (Osnovni sud Belin presuda iz 2012. godine i Apelacioni sud Berlin presuda iz 2014. godine), koje su ustanovile i kršenje klauzule transparentnosti i zabranile upotrebu IP klauzule.³¹¹ Radilo se o tzv. IP klauzuli o licenci u opštim uslovima poslovanja Fejsbuka, koja je bila nejasno formulisana i time negativno uticala na nemačke korisnike Fejsbuka. Sa ovom „IP licencom“ je sebi Fejsbuk pribavio neeksluzivna, važeća za ceo svet prava na sadržajima svojih korisnika. Ovakvo pribavljanje autorskih prava na slikama korisnika je u suprotnosti sa čl. 307 st. 2 br. 1 nemačkog Građanskog zakonika.³¹²

309 Janina Voogd, *BGH: Funktion „Freunde-Finden“ bei Facebook nicht zulässig*, <https://www.noerr.com/de/newsroom/News/bgh-funktion-%E2%80%9Efreunde-finden%E2%80%9C-bei-facebook-nicht-zul%C3%A4ssig.aspx>, 1. 9. 2017.

310 Saopštenje za štampu Vrhovnog suda Nemačke, Bundesgerichtshof Mitteilung der Pressestelle, Nr. 7/2016, Bundesgerichtshof zur Facebook-Funktion „Freunde finden“, <http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2016&Sort=3&nr=73328&pos=0&anz=7m>, 1. 9. 2017.

311 Presuda iz 2012. godine (Urteil vom 6. 3. 2012. Az.: 16 O 551/10), Sud Berlin (LG Berlin) i Presuda iz 2014. godine (Urteil vom 24. 1. 2014, Az.: 5 U 42/12), Apelacioni sud Berlin (KG Berlin).

312 Čl. 307 st. 2 br. 1 nemačkog građanskog zakonika, Bürgerliches Gesetzbuch (BGB), § 307 Inhaltskontrolle, https://www.gesetze-im-internet.de/bgb/_307.html, 3. 9. 2017.

U decembru 2015. godine je Centrala za zaštitu podataka ispitala, da li se Fejsbuk pridržava zabrane upotrebe IP klauzule. Ustanovljeno je da je klauzula promenjena, ali da je i dalje protivpravna i zbog toga su zaštitnici potrošača zahtevali od suda da obaveže Fejsbuk da plati kaznu u iznosu do 250.000 evra.³¹³

Sud u Berlinu je početkom 2016. godine sledio argumentaciju zaštitnika podataka.³¹⁴ Nova klauzula nije u svojoj suštini korektna i zbog toga Fejsbuk krši zabranu upotrebe ove klauzule. Fejsbuk je doduše najavio da će istu iznova promeniti, ali to više nema uticaja na ovaj već učinjeni prekršaj. Prema tvrdnji suda „Držanje klauzule koju je sud označio kao nedozvoljenu, navodi na zaključak da Fejsbuk sudsku zabranu nije uzeo za ozbiljno.“. Stoga je sud dosudio kaznu u iznosu od 100.000 evra i poručio sa time da sankcija takođe mora da bude delotvorna i za ekonomski jake privredne subjekte kao što je Fejsbuk.³¹⁵

Slučaj 5:

Kazna za Fejsbuk od 110 miliona evra zbog dovođenja u zabludu pri preuzimanju Votsapa (WhatsApp)

Zbog pogrešnih navoda pri preuzimanju Votsapa, Evropska komisija je kaznila Fejsbuk sa čak 110 miliona evra. Društvena mreža Fejsbuk je uprkos obećanju datom Evropskoj komisiji pri preuzimanju Votsapa, korisničke podatke međusobno upoređivala sa podacima od Votsapa.³¹⁶

Prema navodima Komisije, visoka kazna je određena iz preventivnih i zastrašujućih razloga, da bi se izbegli budući pogrešni navodi u postupcima spajanja preduzeća. Osim toga Evropska komisija mora da svoje odluke bazira na uticaju i vezi sa zaštitom prava konkurencije, koje zahteva sveobuhvatne i precizne informacije u slučaju spajanja preduzeća.³¹⁷

Prema Uredbi EU o fuzijama preduzeća moraju u okviru ovih postupaka da daju tačne navode i navode koji ne dovode u zabludu. Ovo je za Komisiju od značaja, da bi ona mogla da blagovremeno ispita ovaj postupak. Obaveza davanja tačnih navoda važi nezavisno od toga, da li navodi imaju uticaja na konačni rezultat ispitivanja spajanja. Izrečena kazna je bazirana na Uredbi EU o fuzijama. Ova odredba inače predviđa za namerno ili nepažljivo pogrešno izdate navode kaznu od 1 % ukupnog prihoda preduzeća.

Fejsbuk je 2014. godine izjavio da sigurno i pouzdano automatsko upoređivanje podataka od strane oba servisa nije tehnički moguće. Avgusta 2016. godine je

313 Alexander Grundmann, *Landgericht Berlin: Facebook muss 100.000 Euro Ordnungsgeld wegen rechtswidriger AGB zahlen*. 5. September 2016.

314 Presuda iz 2016. godine (Urteil vom 11. 2. 2016, Az.: 16 O 551/10), Sud Berlin (LG Berlin).

315 Holger Bleich, *LG Berlin: Facebook muss 100.000 Euro Ordnungsgeld zahlen*, <https://www.heise.de/newsticker/meldung/LG-Berlin-Facebook-muss-100-000-Euro-Ordnungsgeld-zahlen-3120265.html>, 3. 9. 2017.

316 Evropska Komisija — saopštenje za medije, Europäische Kommission — Pressemitteilung, Brüssel, 18. Mai 2017, *Fusionskontrolle: Kommission verhängt gegen Facebook Geldbuße von 110 Mio. EUR wegen irreführender Angaben zur Übernahme von WhatsApp*, http://europa.eu/rapid/press-release_IP-17-1369_de.htm, 11. 9. 2017.

317 Simon Rebiger, *WhatsApp: Datenschutz-Lüge bringt Facebook Millionen-Strafe ein*, <https://netzpolitik.org/2017/whatsapp-datenschutz-luege-kostet-facebook-millionen-strafe/>, 11. 9. 2017.

Fejsbuk najavio nasuprot tome da će telefonske brojeve korisnika Votsapa povezati sa Fejsbuk profilima.³¹⁸ Upravo u tome Komisija je i videla obmanu.³¹⁹

Slučaj 6:

Postupak protiv Fejsbuka zbog sumnje vezane za zloupotrebu položaja na tržištu pri povredi prava zaštite podataka

Nemački Savezni sud za karte (zaštita konkurencije) otvorio je 2. 3. 2016. godine postupak protiv Fejsbuka zbog sumnje vezane za zloupotrebu položaja na tržištu pri povredi prava zaštite podataka. Sud je pokrenuo postupak protiv Fejsbuka, uključujući firme ćerke u Irskoj i Nemačkoj. Postoji osnovana sumnja da Fejsbuk sa njegovim Politikama o korišćenju podataka krši propise o zaštiti podataka.³²⁰

Sam postupak se vodi u bliskoj saradnji sa nadležnim poverenicima za zaštitu podataka, savezima za zaštitu potrošača, Evropskom komisijom i institucijama za zaštitu konkurencije.

Nije relevantno za zaštitu konkurencije svako kršenje pravnih propisa od strane firme sa dominantnim položajem na tržištu. U ovom slučaju moglo bi se raditi o upotrebi protivpravnih Politika o korišćenju podataka od strane Fejsbuka, koji predstavljaju tzv. zloupotrebu korisničkih propisa. Stoga ovaj sud želi da ispita vezu između moguće dominantne pozicije na tržištu i korišćenja takvih klauzula.

„Firme sa dominantnom pozicijom na tržištu podležu posebnim obavezama. Između ostalih tu spada i proporcionalna upotreba ugovornih odredbi, ukoliko je to relevantno za tržište“, istakao je predsednik Saveznog suda za kartele Andreas Mundt. Pošto se kod internet operatera kao što je Fejsbuk prihoditi ostvaruju iz reklama, podaci korisnika su od izuzetnog značaja. Stoga navode iz suda da „upravo zbog toga moraju da ispituju iz ugla zloupotrebe moći na tržištu, da li je potrošačima dovoljno razjašnjena vrsta i obim prikupljanja podataka“. ³²¹

Fejsbuk kao što je ukazano koristi podatke svojih korisnika u velikom obimu iz različitih izvora. Od toga izgrađuje profile korisnika, da bi ponudio ciljane reklame. Stoga svaki korisnik mora da se složi sa takvim korišćenjem podataka, da bi uopšte dobio pristup Fejsbuku. Sud izražava veliku sumnju da je takvo postupanje u skladu sa važećem nemačkim pravom o zaštiti podataka. Ukoliko veza sa dominantnim položajem na tržištu postoji, mogao bi se takav prestup kvalifikovati kao zloupotreba u smislu prava konkurencije.

318 EU verdonnert Facebook zu Strafe in Millionenhöhe, portal futurezone.at, <https://futurezone.at/netzpolitik/eu-verdonnert-facebook-zu-strafe-in-millionenhoehe/264.605.063>, 15. 10. 2017.

319 Peter Steinlechner, *EU-Kommission will 110 Millionen Euro Strafe von Facebook*, <https://www.golem.de/news/wegen-whatsapp-eu-kommission-will-110-millionen-euro-strafe-von-facebook-1705-127902.html>, 11. 9. 2017.

320 Saopštenje za javnost nemačkog Saveznog suda za kartele, Bundeskartellamt eröffnet Verfahren gegen Facebook wegen Verdachts auf Marktmachtmissbrauch durch Datenschutzverstöße, Meldung vom 2. 3. 2016, http://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2016/02_03_2016_Facebook.html;jsessionid=6BE002F55A1B879910F6A3ABC34AA023.1_cid378, 9. 9. 2017.

321 Urs Mansmann, *Datenschutzverstöße: Kartellamt ermittelt gegen Facebook*, <https://www.heise.de/newsticker/meldung/Datenschutzverstoesse-Kartellamt-ermittelt-gegen-Facebook-3123977.html>, 9. 9. 2017.

Pravo zaštite konkurencije predviđalo je daleko veće kazne nego nemački Zakon o zaštiti podataka. Dok je po nemačkom Zakonu o zaštiti podataka maksimalna zaprećena kazna bila u iznosu od 300.000 evra, za prekršaje prava konkurencije u najtežim slučajevima se može dosuditi kazna do jedne desetine svetskog prihoda ostvarenih u predhodnoj godini. To bi u slučaju Fejsbuka bilo za 2015. godinu do 1,8 milijardi dolara.

Ukoliko postupak pokaže da je Fejsbuk zloupotrebio dominantan položaj upotrebom Politika o korišćenju podataka, po pravilu se dosuđuje novčana kazna. Pored toga morala bi se i zloupotreba popraviti, a to u ovom slučaju znači izmena Politika o korišćenju podataka.³²²

Slučaj 7:
Preduzeća su odgovorna za izjave svojih zaposlenih koje su u suprotnosti sa pravom konkurencije

Sud u Frajburgu je krajem 2013. godine odlučio da preduzeća odgovaraju za izjave svojih zaposlenih koje su u suprotnosti sa pravom konkurencije.³²³

Jedan radnik tužene autokuće je na svom privatnom Fejsbuk nalogu postavio sledeće:

„Ćao svima,

„Sreća jedanput“, tako glasi naša nova akcija za auto

Od 02.07. dobićete za izabrani novi auto uz 18% popusta!!! Takođe i popust na dnevne registracije vozila od 24%!!!

U ponudi su Up, Polo, Golf, Golf Cabrio, Tiguan, Touran, Sharan, CC i Touareg (dakle za svakog po nešto).

Npr: Scirocco, 2.0l TDI, 170PS:40.930,00 € sada za samo 31.000,00 € !!

[Slika modela Scirocco]

... Za kontakt vam stoji na raspolaganju telefon³²⁴

Centrala za zaštitu konkurencije tužila je za više povreda prava konkurencije i opomenula autokuću. Primera radi nije uredno navedena potrošnja reklamiranog modela automobila. Autokuća je odbacila tvrdnje da ima bilo kakve veze sa postupanjem svog radnika.

Ipak sud u Frajburgu nije sledio ovu argumentaciju, već je potvrdio odgovornost preduzeća. Radnik je u ovom slučaju jasno napustio privatni okvir, pošto nije prodavao svoj privatni automobil već je ponudio i reklamirao poslovni. Osim toga pri postu navedeni telefon je bio poslovni a ne privatni telefon radnika.

322 Jan Schmidbauer, Matthias Huber, *Kartellamt kommt Datenschützern gegen Facebook zu Hilfe*, <http://www.sueddeutsche.de/wirtschaft/internet-konzern-kartellamt-kommt-datenschuetzern-gegen-facebook-zu-hilfe-1.2888395>, 6. 9. 2017.

323 Presuda iz 2013. godine (Urteil vom 4. 11. 2013 — Az.: 12 O 83/13), sud Frajburg (LG Freiburg).

324 LG Freiburg Urteil vom 4. 11. 2013, 12 O 83/13, http://lrwb.juris.de/cgi-bin/laender_rechtsprechung/document.py?Gericht=bw&Art=en&Datum=2013&Sort=12290&nr=17380&pos=0&anz=670, 2. 9. 2017.

Čl. 8 st. 2 Zakona o zaštiti konkurencije određuje da reklamirana autokuća odgovara i bez znanja za postupanje svojih radnika. Na taj način je sud isključio uopšte problematiku da li se radi o privatnim ili javnim izjavama radnika. Svaka forma ponašanja u suprotnosti sa pravom konkurencije kao u ovom slučaju kao skrivena reklama treba biti sprečena. Preduzeća treba da informišu radnike na odgovarajući način o ophođenju sa društvenim mrežama.³²⁵

Slučaj 8: **Stranica preduzeća na Fejsbuku mora imati impresum**

U sudskoj praksi je u više navrata (odluka suda u Frankfurtu iz 2011. godine i u Ašafenburgu iz 2011. godine) u Nemačkoj ustanovljeno da prezentacije firmi odnosno stranica firme na Fejsbuku mora imati uredan impresum.³²⁶ Ne vođenje urednog impresuma predstavlja kršenje prava konkurencije.³²⁷

Tako je sud u Ašafenburgu ustanovio po tužbi konkurenske firme informacije koje su nedostajale u impresumu. Na stranici tužene firme na Fejsbuku je bio naveden naziv firme i adresa, ali su nedostajale dalje informacije kao što je pravna forma, ime generalnog direktora. Takođe stranica na Fejsbuku je sadržala samo link ka svojoj veb stranici. Sud je smatrao da je povezivanje putem linka nedovoljno i da korisnici određene informacije mogu da dobiju tek pošto kliknu na link. Informacije treba tim pre da budu dostupne direktno na Fejsbuk stranici firme. Informacije koje treba da sadrži impresum su date u čl. 5 nemačkog Zakona o elektronskim medijima. Tužena firma je postupala u suprotnosti sa pravom konkurencije (shodno čl. 3 u vezi sa čl. 4 tč. 11 Zakona o zaštiti konkurencije), pošto nije na svojoj Fejsbuk prezentaciji učinila lako i neposredno dostupnim informacije iz čl. 5 Zakona o elektronskim medijima. Ove informacije služe u svrhu zaštite potrošača i transparentnosti poslovnog delovanja, pa stoga i predstavljaju propise o ponašanju na tržištu u smislu čl. 4 br. 11 Zakona o zaštiti konkurencije.³²⁸

Pošto se stranica na Fejsbuku jasno koristila u svrhu marketinga, samim tim postoji poslovna aktivnost. Fejsbuk stranica predstavlja elektronski medijum za koji se zahteva da sadrži u poslovnom smislu impresum.³²⁹

325 Martin Bahr, *LG Freiburg: Unternehmen haftet für wettbewerbswidrige Facebook-Äußerungen seiner Mitarbeiter*, <http://www.dr-bahr.com/news/unternehmen-haftet-fuer-wettbewerbswidrige-facebook-aeusserungen-seiner-mitarbeiter.html>, 2. 9. 2017.

326 Odluka iz 2011. godine (Beschluss vom 19. 10. 2011 — Az.: 3–08 O 136/11), Sud Frankfurt (LG Frankfurt).

327 Presuda iz 2011. godine (Urteil vom 19. 8. 2011 — Az.: 2 HK O 54/11), Sud Ašafenburg (LG Aschaffenburg).

328 Carsten Ulbricht, *LG Aschaffenburg bestätigt Impressumspflicht bei geschäftsmäßig genutzten Facebookprofilen*, <http://www.rechtzweinull.de/archives/188-LG-Aschaffenburg-bestaetigt-Impressumspflicht-bei-geschaeftsmaessig-genutzten-Facebookprofilen.html>, 3. 9. 2017.

329 Sebastian Ehrhardt, *Neues Urteil: Gericht bestätigt erneut Impressumspflicht auf Facebook*, <https://www.e-recht24.de/news/facebook/6959-urteil-lg-frankfurt-impressum-auf-facebook.html>, 3. 9. 2017.

U sudskoj praksi je pokazan i zabranjen način ubacivanja impresuma na Fejsbuk stranicama firmi. Tako je Viši sud u Dizeldorfu odlučio da nije dovoljno da sama Fejsbuk stranica firme sadrži impresum pod opcijom „informacije“ i da to ne govori dovoljno da se tu nalazi impresum, već treba da se nedvosmisleno označiti sa „impresum“ ili „kontakt“.³³⁰ Informacije iz impresuma moraju takođe biti lako dostupne korisnicima. Ukoliko se one ne nalaze na početnoj strani, to znači da su ponudiodci usluga izabrali linkove koji su razumljivi korisnicima bez daljeg pojašnjavanja. Iz sudske prakse Vrhovnog suda Nemačke pokazalo se da su to pojmovi „impresum“ i „kontakt“.³³¹ Ovi pojmovi su poznati prosečnim korisnicima, da bi potražili neophodne informacije.³³²

5.3. Koordinisane akcije institucija za zaštitu podataka protiv Fejsbuka

Fejsbuk je 13. novembra 2014. najavio da će izmeniti svoju politiku privatnosti i ophođenje sa „kolačićima“. Ovaj čin Fejsbuka je inicirao koordinisanu akciju ispitivanja načina poslovanja Fejsbuka od strane institucija za zaštitu podataka Holandije, Francuske, Španije, Belgije i grada Hamburga. Ispitivanja postupanja Fejsbuka u pogledu zaštite podataka odnose se na kvalitet informacija, koje korisnici dobijaju, verodostojnost izjave saglasnosti na obradu ličnih podataka u svrhe marketinga.³³³

Zaštitnici podataka smatraju da Fejsbuk generiše ogromne prihode od reklama u nekim evropskim zemljama (kao npr. Nemačka, Francuska). Osim toga firma poseduje i kancelarije tamo. Aktivnosti vezane za reklamiranje su „neraskidivo povezane“ sa prikupljanjem i obradom podataka. Stoga se Fejsbuk po njima ne može pozivati samo na predstavništvo u Irskoj. Ova problematika će biti rešena od maja 2018. godine, kada će važiti tzv. *princip tržišnog mesta* (čl. 3 st. 3 Opšte uredbe o zaštiti podataka). Po ovom principu će se primenjivati pravo zaštite podataka u onoj zemlji u kojoj kompanije imaju aktivnosti.³³⁴ Na taj način se pitanje primene prava EU neće više vezivati za filijale ili predstavništva u EU, već da li se roba i usluge nude evropskim građanima.³³⁵

330 Presuda iz 2013. godine (Urteil vom 13. 8. 2013 — Az.: I-20 U 75/13), Viši sud Dizeldorf. (OLG Düsseldorf).

331 Felix Barth, *Bitte melde dich: Facebook-Impressum verschwunden — was tun?*, <http://www.it-recht-kanzlei.de/impresum-facebook-verschwunden.html>, 3. 9. 2017.

332 Presuda iz 2006. godine (NJW 2006, 3633 (3634 f)), Vrhovni sud Nemačke (BGH).

333 Zajednička izjava institucija za zaštitu podataka iz 2017. godine, *Common Statement by the Contact Group of the Data Protection Authorities of The Netherlands, France, Spain, Hamburg and Belgium*, 16 mai 2017, <https://www.cnil.fr/fr/node/23602>, 25. 9. 2017.

334 Ingo Dachwitz, *Französische Datenschutzbehörde verhängt Höchststrafe gegen Facebook*, <https://netzpolitik.org/2017/franzoesische-datenschutzbehoerde-verhaengt-hoehchststrafe-gegen-facebook/>, 25. 9. 2017.

335 Lukas Bühlmann, *EuGH-Urteil zur Missbräuchlichkeit der Amazon-Rechtswahlklausel und zum anzuwendenden Datenschutzrecht*, <https://www.mll-news.com/eugh-urteil-zur-missbraeuchlichkeit-der-amazon-rechtswahlklausel-und-zum-anzuwendenden-datenschutzrecht/>, 1. 10. 2017.

Belgijska komisija za zaštitu podataka je već dala više preporuka Fejsbuku za poboljšanje njihovog poslovanja u pogledu praćenja korisnika i ostalih internet korisnika putem kolačića, društvenih dodataka itd. Trenutno Komisija pokušava sudski da svoje preporuke sprovede u delo. Zahtevi su slični kao kod francuskih kolega.

Holandska institucija za zaštitu podataka se takođe žalila na rad Fejsbuka. Radilo se između ostalog i o tome da se osetljivi podaci kao što su npr. podaci o seksualnoj orijentaciji Fejsbuk korisnika koriste za ciljane reklame. Oспорava se da 9,6 miliona holandskih korisnika nije dovoljno informisano, kako se njihovi podaci koriste. Trenutno se ispituje mogućnost sankcionisanja ovih prestupa, pošto je Fejsbuk napravio određene promene kako bi zaustavio ovakav način korišćenja podataka.³³⁶

Slučaj 1: Fejsbuk kažnjen sa 1,2 miliona evra u Španiji

Polovinom 2017. godine je Fejsbuk kažnjen sa čak 1,2 miliona evra zbog propusta vezanih za zaštitu podataka u Španiji.³³⁷

Društvena mreža Fejsbuk je bez izričite saglasnosti svojih korisnika, koristila njihove podatke u reklamne svrhe „eng. targeted advertising“. Fejsbuk je po oceni španske intitucije za zaštitu podataka (Agencia Española de Protección de Datos — AEPD) komercijalno koristio podatke, koji su posebno zaštićeni po španskom pravu. Tom prilikom se radilo o informacijama vezanim za religijsku i ideološku pripadnost kao i seksualnu orijentaciju.³³⁸ O tome Fejsbuk korisnici nisu dovoljno informisani. Podaci i Fejsbuk korisnika i onih koji to nisu prikupljeni su od trećih strana, sa ostalih internet sajtova. Podaci Fejsbuk korisnika prikupljeni su i onda, kada korisnici nisu bili ni ulogovani na ovu društvenu mrežu. Pritom podatke Fejsbuk uopšte nije brisao i kada korisnici obrišu njihove naloge ili kada zahtevaju brisanje podataka.³³⁹

Osim toga Fejsbuk je kupovao podatke od specijalizovanih trgovaca o ponašanju korisnika van internet mreže kao i o visini njihovih zarada.

Izjavu saglasnosti o korišćenju podataka Agencija za zaštitu podataka je ocenila kao nejasnu, sa uopštenim formulacijama i da se njoj može pristupiti uz puno kli-kova. Fejsbuk koristi pritom neprecizne informacije vezane za korišćenje podataka

³³⁶ *Ibidem*.

³³⁷ Agencija za zaštitu podataka, Agencija za zaštitu podataka kažnjava Fejsbuk zbog kršenja pravila zaštite podataka, La AEPD sanciona a Facebook por vulnerar la normativa de protección de datos, 11 de septiembre, Agencia Española de Protección de Datos, http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2017/notas_prensa/news/2017_09_11-ides-idphp.php, 30. 9. 2017.

³³⁸ Michael Pohlgeers, *Datenschutzverstöße: Facebook muss Millionenstrafe zahlen*, <https://www.online-haendler-news.de/handel/internationales/29893-datenschutzverstoesse-facebook-millionenstrafe-spanien.html>, 30. 9. 2017.

³³⁹ Datenschutzverstöß: 1,2 Millionen Euro Strafe für Facebook in Spanien, portal heise.de, <https://www.heise.de/newsticker/meldung/Datenschutzverstoess-1-2-Millionen-Euro-Strafe-fuer-Facebook-in-Spanien-3826957.html>, 30. 9. 2017.

korisnika, tako da prosečnom korisniku koji nije tehnički kompetentan nije jasno koji se podaci prikupljaju, kako se snimaju i kako se obrađuju.³⁴⁰

Slučaj 2: **Fejsbuk kažnjen sa 150.000 evra u Francuskoj**

Nacionalna francuska Komisija za informatiku i slobode (Commission Nationale de l'Informatique et des Libertés — CNIL) je početkom 2016. godine pozvala Fejsbuk da se pridržava važećih francuskih propisa. Pošto je izostala adekvatna reakcija Fejsbuka, Nacionalna francuska Komisija za informatiku i slobode izrekla je polovinom 2017. godine kaznu od 150.000 evra. Ovo je najviša kazna koju trenutno institucija za zaštitu podataka može da izrekne.³⁴¹

Visina kazne će se promeniti od maja 2018. godine sa početkom primene Opšte uredbe o zaštiti podataka. Tada će biti moguće da se izrekne kazna do 20 miliona evra ili do 4 % svetskog prometa preduzeća.

Upravo visina kazne u iznosu od samo 150.000 ilustruje problem sprovođenja prava zaštite podataka. Pri godišnjem prometu od 25 milijardi dolara i 10 milijardi dolara čistog prihoda (po izveštaju za 2016. godinu), Fejsbuk može izrečenu kaznu da plati bez velikih problema.

Nacionalna francuska Komisija za informatiku i slobode je ustanovila da je Fejsbukovo ciljano reklamiranje (eng. targeted advertising) nelegalno. Fejsbuk je bez pravnog osnova kombinovao informacije svojih korisnika da bi im slao ciljane reklame. Korisnici su morali da budu u mogućnosti da ulože prigovor protiv ovog sveobuhvatnog pravljenja profila, na kome je uopšte baziran Fejsbukov model poslovanja.³⁴²

Osim toga Fejsbuk uz pomoć svog datr-kolačića (eng. Cookie) neovlašćeno prati ponašanje korisnika vezano za njihovo surfovanje po internetu. Fejsbuk je informisao korisnike samo o tome da je ovaj kolačić u upotrebi da bi se prikupile informacije sa spoljnih platformi. Korisnici Fejsbuka nisu informisani o tome po mišljenju Nacionalne francuske komisija za informatiku i slobode, da Fejsbuk tom prilikom svaki put prikuplja informacije o njima kada posete neki veb sajt, koji sadrži društvene dodatke „social-plugin“. Osim toga ovim kolačićem se prikupljaju i podaci ostalih internet korisnika, koji nisu korisnici Fejsbuka, kada posećuju veb sajtove koji sadrži društvene dodatke „social-plugin“.

Fejsbuk može da uloži žalbu na ovu odluku u roku od 4 meseca Vrhovnom upravnom sudu Francuske.³⁴³

340 Ingo Dachwitz, Spanien: *Millionenstrafe für Facebooks illegale Datensammlung*, <https://netzpolitik.org/2017/spanien-millionenstrafe-fuer-facebook-s-illegale-datensammlung/>, 25. 9. 2017.

341 Presuda iz 2017. godine (Délibération n°SAN — 2017–006 du 27 avril 2017), Nacionalna francuska Komisija za informatiku i slobode (Commission Nationale de l'Informatique et des Libertés — CNIL). <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000034728338&fastReqId=390211096&fastPos=2>, 25. 9. 2017.

342 Andreas Wilkens, *Französische Datenschützer verhängen Strafe gegen Facebook*, <https://www.heise.de/newsticker/meldung/Franzoesische-Datenschuetzer-verhaengen-Strafe-gegen-Facebook-3715052.html>, 25. 9. 2017.

343 Ingo Dachwitz, *Französische Datenschutzbehörde verhängt Höchststrafe gegen Facebook*, <https://netzpolitik.org/2017/franzoesische-datenschutzbehoerde-verhaengt-hoehchststrafe-gegen-facebook/>, 25. 9. 2017.

Slučaj 3: **Obaveza navođenja pravog imena na Fejsbuku slučaj I**

Iako ovaj slučaj nema direktne veze sa koordinisanom akcijom institucija za zaštitu podataka, biće predstavljen iz razloga sličnosti sa slučajem br. II u nastavku.

Pravni spor između Fejsbuka i nezavisne Institucije za zaštitu podataka nemačke pokrajine Šlesvig-Holštajn pred Upravnim sudom ove pokrajine, rešen je u prvoj instanci u korist Fejsbuka.³⁴⁴

Nakon blokiranja pojedinih korisnika Fejsbuka, koji su na svojim profilima koristili pseudonime umesto navođenja isključivo pravih imena korisnika prilikom otvaranja profila (registracije) na ovoj društvenoj mreži, Poverenik za zaštitu podataka nemačke pokrajine Šlesvig-Holštajn je krajem 2012. godine doneo odluku protiv Fejsbuka u kojoj se navodi:

(1) Fejsbuk Inc. kao odgovorna institucija za obradu podataka se na osnovu Saveznog zakona o zaštiti podataka obavezuje da fizičkim licima koji žele da koriste ovu platformu uz pomoć tehničke podrške, koju ostvaruje putem svoje organizacije na teritoriji Nemačke obezbedi:

- Mogućnost izbora prilikom registracije na platformi www.facebook.com umesto navođenja pravih podataka (ime, prezime, e-mail adresa, pol, datum rođenja) da se korisnici registruju putem pseudonima.
- Odblokiranje profila registrovanih korisnika na platformi www.facebook.com, koji su blokirani isključivo i samo zbog ne navođenja ili nepotpunog navođenja pravih podataka (ime, prezime, e-mail adresa, pol, datum rođenja).
- Obaveštenje na platformi www.facebook.com, kojim korisnici moraju biti obavешteni pre registracije u jednostavnoj, razumljivoj formi i na nemačkom jeziku o mogućnostima registracije uz navođenje pseudonima.

(2) Naredbu iz stava (1) treba izvršiti odmah.

(3) Ukoliko Fejsbuk Inc. u roku od 2 nedelje nakon dostavljanja ove naredbe ne postupi po njoj, kazniće se novčanom kaznom od 20.000 evra“.

Fejsbuk je podneo žalbu na ovu odluku Poverenika pred Upravnim sudom pokrajine Šlesvig-Holštajn.

U nastavku postupka pred Upravnim sudom suštinsko pitanje je bilo da se razjasni, da li uopšte treba primeniti nemački Zakon o zaštiti podataka ili važi irski Zakon o zaštiti podataka?

Institucija za zaštitu podataka nemačke pokrajine Šlesvig-Holštajn obrazložila je primenu nemačkog prava time da Fejsbuk ima firmu ćerku na teritoriji Savezne Republike Nemačke — Facebook Germany GmbH. Na ovaj način podleže Saveznom zakonu o zaštiti podataka kao i Direktivi EU o zaštiti podataka o ličnosti (član 4, stav 1, Direktive). Osim toga u nemačkom Zakonu o elektronskim komunikacijama je upotreba pseudonima moguća i dozvoljena.

³⁴⁴ Andrej Diligenski, *Obaveza navođenja pravog imena na Fejsbuku*, portal Zaštita podataka o ličnosti, <http://partners-serbia.org/privatnost/blog/obaveza-navođenja-pravog-imena-na-fejsbuku/>, 15. 10. 2017.

Fejsbuk se ovim argumentima suproststavio tvrdnjom da Facebook Germany GmbH svoju delatnost ostvaruje samo u oblasti marketinga kao i u cilju oglašavanja (privlačenja novih korisnika) uopšte, tako da se putem ove firme čerke u Nemačkoj ne obrađuju podaci o ličnosti korisnika.

Upravni sud je zaključio da je argumentacija Fejsbuka u skladu sa Mišljenjem irskog poverenika za zaštitu podataka. U tom Mišljenju je konstatovano da se u slučaju ovog predstavništva (filijale) ne radi o mestu u kome se podaci o ličnosti obrađuju. Tumačenjem primene nemačkog Saveznog zakona o zaštiti podataka kao i Direktive o zaštiti podataka dolazi se do zaključka da je nemačko pravo primenljivo, samo ukoliko se obrada podataka o ličnosti zaista ostvaruje u ovom predstavništvu (filijali). U ovom slučaju se to ne dešava.

Fejsbuk Irska Ltd. predstavlja jedino predstavništvo van teritorije Severne Amerike, koje vrši kontrolu podataka korisnika Fejsbuka. Pravo na odblokadu korisničkih profila, koji žele da koriste pseudonime dakle ne postoji u ovom slučaju, pošto korišćenje pseudonima u irskom Zakonu o zaštiti podataka nije predviđeno.

Treba imati u vidu da prinuda navođenja imena na društvenim mrežama poseduje takođe i druge dimenzije. Izostavljanje pseudonima stavlja u težak pravni, socijalni, ekonomski položaj mnoge aktiviste za zaštitu ljudskih prava kao i novinare, koji imaju otežane uslove rada u obavljanju svojih dužnosti, pošto je moguć njihov politički, socijalni, ekonomski progon.³⁴⁵

Poverenik za zaštitu podataka pokrajine Šlesvig-Holštajn je uložio žalbu na ovu odluku Upravnog suda i kritikovao Fejsbuk da pokušava da ukine pravo na privatnost korisnika, koje je garantovano zakonima.

Po žalbi na odluku Upravnog suda je Viši upravni sud pokrajine Šlesvig-Holštajn polovinom 2013. godine potvrdio odluku prvostepenog upravnog suda.³⁴⁶ Nemačko pravo ne važi u ovom slučaju shodno Direktivi EU o zaštiti podataka, već je važeće irsko pravo. Glavni razlog za to je što se obrada podataka dešava u Irskoj. Sud je ukazao i na to da se ova odluka bazira na aktivnosti irske filijale u pogledu obrade podataka Fejsbuk korisnika. Sve aktivnosti shodno Direktivi EU o zaštiti podataka i Saveznog zakona o zaštiti podataka su dovoljne da bi se isključivo primenilo irsko pravo. Nemačko pravo nije primenljivo i pored aktivnosti vezanih za marketing i oglašavanje. Nezavisna Institucija za zaštitu podataka nemačke pokrajine Šlesvig-Holštajn nije uložila žalbu na ovu odluku suda.³⁴⁷

Slučaj 4:

Obaveza navođenja pravog imena na Fejsbuku slučaj II

Slično kao u nemačkoj pokrajini Šlesvig-Holštajn i upravni sud u Hamburgu je odlučivao po naredbi poverenika za zaštitu podataka nemačkog grada Hamburga

345 Odluka Upravnog suda nemačke pokrajine Šlesvig-Holštajn iz 2012. godine: Az.: 8 B 61/12.

346 Odluka (broj akta: 4 MB 10/13 i 11/13), Viši upravni sud pokrajine Šlesvig-Holštajn (OVG Schleswig).

347 Saopštenje za javnost Nezavisne Institucije za zaštitu podataka nemačke pokrajine Šlesvig-Holštajn, Pressemitteilung des ULD, OVG Schleswig-Holstein: Für Facebook gilt kein deutsches Datenschutzrecht, <https://www.datenschutzzentrum.de/presse/20130424-facebook-klarnamen-ovg.htm>, 1. 10. 2017.

o mogućnosti koršćenja pseudonima prilikom otvaranja profila tj. registracije na društvenoj mreži Fejsbuk. Fejsbuk naime dozvoljava upotrebu samo pravog imena prilikom registracije.³⁴⁸

Upravni sud u Hamburgu je početkom 2016. godine u ubrzanom postupku po žalbi Fejsbuka, odlučio da Fejsbuk ne mora za sada da implementira naredbu poverenika vezanu za korišćenje pseudonima.³⁴⁹

Spor je započeo nakon što je Fejsbuk blokirao nalog, koji je bio napravljen pod pseudonimom. Za poverenika za zaštitu podataka nemačkog grada Hamburga ovo je bio povod da obaveže Fejsbuk da omogući korisnicima upotrebu pseudonima. Naredba se odnosila na Fejsbuk Irsku, koji je nadležan za Fejsbuk korisnike izvan Severne Amerike. Na ovu naredbu se Fejsbuk žalio.³⁵⁰

Upravni sud je odlučio, da naredbu privremenog raspolaganja ne treba sprovesti. Osim toga sud je ukazao i na to da nemačko pravo nema primenu u ovom slučaju, na osnovu koga poverenik njegovu naredbu bazira i na osnovu koje su internet ponudnici u obavezi da omoguće anonimno ili pod pseudonimom korišćenje njihovih usluga. Treba primeniti pravo one države članice EU, sa kojom je sporna obrada podataka u najtešnjoj vezi. To pravo je irsko pravo u pogledu obaveze navođenja pravog imena. Nemačka filijala Fejsbuka bazira svoje aktivnosti pretežno u oblasti reklamiranja.³⁵¹

Na ovu odluku žalio se poverenik za zaštitu podataka nemačkog grada Hamburga. Viši upravni sud grada Hamburga je polovinom 2016. godine odbio tužbeni zahtev poverenika kao neosnovan.³⁵² Sud je ustanovio da je ostalo otvoreno, da li je uopšte naredba poverenika bazirana na pravu. S obzirom na to sud smatra da odgovor na to pitanje predstavlja tumačenje čl. 4. st. 1 a Direktive EU o zaštiti podataka (95/46/EU).³⁵³ Osim toga po važećoj sudskoj praksi Evropskog suda nije jasno, da li Direktiva o zaštiti podataka dozvoljava poverenicima za zaštitu podataka da postupaju po nacionalnim odredbama svojih zemalja protiv podnosioca zahteva iz Irske.³⁵⁴

348 Christian Solmecke, *VG Hamburg — Facebook darf Klarnamen verlangen*, <https://www.wbs-law.de/it-recht/facebook-braucht-laut-vg-hamburg-keine-anonymisierten-profile-zulassen-66530/>, 1. 10. 2017.

349 Odluka iz 2016. godine (br. akta 15 E 4482/15) Upravni sud grada Hamburga (VG Hamburg).

350 Saopštenje za javnost Upravnog suda Hamburga, Verwaltungsgericht Hamburg entscheidet: Anordnung des Datenschutzbeauftragten zur Nutzung von Facebook unter einem Pseudonym darf nicht vollzogen werden, Pressemitteilung des VG Hamburg vom 3. 3. 2016, <http://justiz.hamburg.de/aktuellepresseerklarungen/5359286/pressemitteilung/>, 1. 10. 2017.

351 Martin Bahr, *VG Hamburg: Facebook muss Pseudonym-Anordnung des Hamburgischen Datenschutzbeauftragten vorerst nicht umsetzen*, <http://www.dr-bahr.com/news/datenschutzrecht/facebook-muss-pseudonym-anordnung-des-hamburgischen-datenschutzbeauftragten-vorerst-nicht-umsetzen.html>, 1. 10. 2017.

352 Odluka iz 2016. godine (broj akta AZ: 5 Bs 40/16), Viši upravni sud grada Hamburga (OVG Hamburg).

353 Alexander Bräuer, *Facebook muss vorerst keine Pseudonyme zulassen*, <https://www.ratgeberrecht.eu/internetrecht-aktuell/facebook-muss-vorerst-keine-pseudonyme-zulassen.html>, 1. 10. 2017.

354 Saopštenje za javnost Višeg upravnog suda grada Hamburga, Hamburgisches Oberverwaltungsgericht entscheidet: Klarnamenpflicht bei Facebook bleibt vorerst, Pressemitteilung des

Slučaj 5: *Fejsbuk ne sme koristiti podatke od Votsapa (WhatsApp-a)*

Fejsbuk je 2014. godine preuzeo Votsap. Krajem 2016. godine Fejsbuk je promenio Politiku o korišćenju, kojom je predvideo i prenos ličnih podataka sa Votsapa na Fejsbuk.

Sa izvršnim rešenjem od 23. septembra 2016. godine od strane hamburškog poverenika za zaštitu podataka zabranjeno je Fejsbuku Irska da bez saglasnosti prikuplja i snima podatke o ličnosti nemačkih građana korisnika Votsapa. Osim toga je u rešenju određeno Fejsbuku da mora da obriše podatke, koje je prikupio bez saglasnosti i da dokumentuje brisanje podataka.

Votsap vlasnički pripada Fejsbuku, ali nije Fejsbuk. Transfer podataka sa Votsapa Fejsbuku predstavlja prikupljanje podataka Fejsbuka. Ovakvo prikupljanje je zabranjeno. Pošto se prikupljaju podaci nemačkih korisnika Votsapa i to se obavlja u Nemačkoj, dolazi do primene nemačkog prava.

Slično je presudio i Evropski sud u slučaju austrijskog Saveza za zaštitu potrošača protiv Amazona.³⁵⁵ U ovom slučaju se između ostalog radilo i o problematici iz čl. 4 st. 1 Direktive o zaštiti podataka. Ovaj član se tiče nadležnosti u slučaju obrade podataka u okviru koncerna, kada koncern ima više filijala u različitim državama članicama EU. Pri ocenjivanju čije će se pravo primeniti, treba uzeti u obzir tržišnu i potrošačku orijentaciju filijale u državi članici EU na koju se odnosi obrada podataka.³⁵⁶

Protiv ovog rešenja Fejsbuk je uložio žalbu pred Upravnim sudom u Hamburgu.³⁵⁷ Upravni sud je polovinom 2017. godine odlučio da Fejsbuk trenutno može da koristi podatke nemačkih korisnika Votsapa samo uz njihovu saglasnost. Pored toga sud je ustanovio da u pogledu brisanja podataka i dokumentacije o brisanju, nije moguće sprovesti rešenje zbog formalnih propusta u rešenju.³⁵⁸

Još uvek po važećim propisima, dok ne krene primena Opšte uredbe o zaštiti podataka, nije dovoljno razjašnjeno da li nemačko pravo o zaštiti podataka treba primeniti. Svakako da izjave saglasnosti o korišćenju podataka od strane Votsapa nisu u skladu sa nemačkim pravom o zaštiti podataka.

Sud je do ove odluke došao uz procenu pretežnijeg interesa. Tom prilikom je uzeo u obzir interese korisnika Votsapa i interese društvene mreže. Pri proceni pretežnijeg interesa ustanovljeno je da preteže interes nemačkih Votsap korisnika. Pošto pravo na zaštitu podatka predstavlja osnovno ljudsko pravo, pri prenosu po-

OVG Hamburg vom 30. 6. 2016, <http://justiz.hamburg.de/aktuellepresseerklarungen/6471066/pressemitteilung/>, 1. 10. 2017.

355 Presuda iz 2016. godine (Urteil vom 28. 7. 2016, C-191/15) Evropski sud (EuGH).

356 EU-Online-Handel | EuGH bestätigt Rechtswahlmöglichkeit in AGB, Noerr LLP <https://www.noerr.com/de/newsroom/News/EU-Online-Handel-EuGH-bestaetigt-Rechtswahlmoeglichkeit-in-AGB.aspx>, 15. 10. 2017.

357 Andreas Scharnberg, *Verwaltungsgericht Hamburg untersagt Datenaustausch zwischen Facebook und WhatsApp*, <https://aus-suederelbe.de/wcf/index.php?article/208-verwaltungsgericht-hamburg-untersagt-datenaustausch-zwischen-facebook-und-whatsa/>, 8. 9. 2017.

358 Odluka iz 2017. godine (Beschluss vom 24. 4. 2017 — Az.: 13 E 5912/16), Upravni sud Hamburg (VG Hamburg).

dataka dolazi da značajnog zadiranja u prava pojedinaca. Na ovu odluku može se Fejsbuk žaliti Višem upravnom sudu u Hamburgu.³⁵⁹

5.4. Dobijanje otkaza zbog Fejsbuka

Koliko je lajk dugme opasno u praksi pokazuju mnogobrojni slučajevi.

Korisnici Fejsbuka često izgube kontrolu svojih objava, jer nisu svesni da ukoliko lajkuju određeni komentar, postoji mogućnost da se isti zbog nepažnje pojavi i na hiljade drugih profila i na taj način sazna i u široj javnosti. Posledica ovoga je da ostaju bez posla, pošto poslodavci saznaju za ovakve komentare.

Slučaj 1: Objave kao razlog za otkaz

Slučaj se desio 2013. godine u Dizeldorfu, gde je 11 vatrogasaca najpre bilo suspendovano sa posla, a potom tek opomenuto. Razlog za davanje otkaza je kritika na račun gradonačelnika Dizeldorfa. Jedan od njih je napisao da će „gradonačelnik umeti da ceni njihov neplaćen prekovremeni rad, kada se njegova kancelarija zapali“. „Verovatnoća da se tako nešto desi, je kao da dobijemo šesticu na lotu“. Ostali vatrogasci su ovaj komentar lajkovali. Iza ovakvog izliva nezadovoljstva vatrogasaca stoje neisplaćeni prekovremeni rad. Gradonačelnik je ubrzo posle ovih objava sazvao sednicu na kojoj je doneo odluku o suspendovanju.

Sindikati i opozicione partije kritikuju odluku gradonačelnika kao nesrazmernu. „Pošto se radi o prirodi njegove pozicije, političari na pozicijama moraju biti više spremni na kritiku“ bile su reči predstavnika opozicije. Neki su bili još oštrij i u kritikama „Svinjarija, da se vatrogascima ne plate prekovremeni sati. Dizeldorf je bogat grad u poređenju sa ostalim gradovima“.³⁶⁰

Slučaj 2: Neopravdani otkaz uz sporazumno rešenje spora

Naredni drastičan primer se desio kada je jedan zaposleni napisao za svoga šefa „da je on 32 godine u firmi i da je jedna lenja svinja, koja još ništa nikada nije radila u svom životu“. Osim toga ovaj radnik je pored uvreda objavio i više pretnji svom predpostavljenom, a šef je navodno dva puta opomenuo radnika zbog svog ponašanja. Ovo je predstavljalo jasan razlog za otkaz, a pored toga na listi prijatelja od 70 bilo je 36 kolega sa posla.³⁶¹ Odbrana radnika je argumentovala

359 Stephan Hansen-Oest, *WhatsApp-Nutzereinwilligungen unwirksam? Anmerkungen zur Entscheidung des VG Hamburg*, <https://www.datenschutz-guru.de/whatsapp-nutzereinwilligungen-unwirksam-anmerkungen-zur-entscheidung-des-vg-hamburg/>, 8. 9. 2017.

360 *Feuerwehrleute nach Facebook-Kritik an OB suspendiert*, Süddeutsche.de, <http://www.sueddeutsche.de/karriere/duesseldorf-feuerwehrleute-nach-facebook-kritik-an-ob-suspendiert-1.1591727>, 22. 8. 2013.

361 Andreas Wilkens, *Beschimpfungen auf Facebook sind Kündigungsgrund*, heise.de, <http://www.heise.de/newsticker/meldung/Beschimpfungen-auf-Facebook-sind-Kuendigungsgrund-1922112.html>, 12. 8. 2013.

njegove postupke time da njegov profil nije dostupan javnosti, da radnik nije bio ni svestan da su njegove objave na zidu profila, te da je on mislio da je on u internoj komunikaciji putem četa sa kolegom. Kao glavni argument odbrana je navela da se u privatnoj sferi mogu slobodno izražavati stavovi, te da oni ne predstavljaju razlog za otkaz. Poslodavac je tvrdio da je više puta opomenuo radnika i da je zbog njegovih objava takođe oštetio i firmu, pošto su objave uticale na reputaciju firme. Sud za radne sporove Hagen u Nemačkoj je u svojoj presudi potvrdio opravdanost otkaza.³⁶² Presuda je izrečena polovinom 2012. godine. Ovom presudom osporen je otkaz, bez otkaznog roka (momentalni otkaz). Prema mišljenju suda objave su u ovom slučaju bile javne i usmerene na posao firme, pa je otkaz opravdan. Osim toga radnik nije samo uvredio poslodavca, već mu je i pretio.

Ipak, radnik je uložio žalbu i žalbeni sud je uvažio radnikove tvrdnje. Tako je radnik vraćen na posao. Sukobljene strane su se nagodile, te je spor rešen povratkom radnika na svoje radno mesto.³⁶³

Slučaj 3: Opravdani otkaz šegrta

Iako je radnicima dozvoljeno da opravdano kritikuju poslodavce, veoma je važno kakve izraze koriste i gde kritike plasiraju. U ovom slučaju su najpre neopravdane konsekvence po radnika bile potvrđene, a u žalbenom postupku ukinute.

Slučaj se dogodio u nemačkom gradu Hamu u pokrajini Severnoj Rajni-Vestfaliji, gde je pokrajinski sud jednog šegrta najpre delimično osudio, a potom tu odluku preinačio u žalbenom postupku krajem 2012. godine.³⁶⁴

Šegrt je na svom Fejsbuk profilu napisao za svog nadređenog da je „izrabljivač, gonič robova i da ga drži kao kmeta“ i da on „mora da radi ova sranja za 20% manju naknadu od uobičajene“. Naravno za ove objave nisu saznali samo prijatelji već i sam poslodavac, koji je bez otkaznog roka šegrta otpustio. Pored toga je šegrt tužio firmu i tražio povratak na radno mesto zbog neosnovanog otkaza.

U svojoj odbrani šegrt je naveo „da on svog šefa nije nameravao da uvredi i da on uopšte nije sa time računao da će on videti uvrede na njegovom Fejsbuk profilu. Njegove objave su navodno bile samo preterane u izražavanju i šaljive, a nisu predstavljale realno stanje stvari. Osim toga njemu i njegovim prijateljima pripada pravo na slobodno mišljenje i izražavanje shodno zakonu“.

Sud je najpre delimično osudio šegrta i potvrdio razloge za otkaz i konstatovao da se radilo o uvredi poslodavca. Međutim istakao je da se radi o nezreloj osobi i ustanovio nedostatak ozbiljnosti kod šegrta. Stoga je trebalo da poslodavac prvo uputi opomenu, ili obavi razgovor upozorenja pre davanja otkaza.

362 Presuda iz 2012. godine (Urteil vom 16. 5. 2012, Az.: 3Ca 2597/11). Sud za radne sporove Hagen (Arbeitsgericht Hagen).

363 Marzena Sicking, *Chef-Beleidigung auf Facebook rechtfertigt Kündigung*, heiseResale, <http://www.heise.de/resale/artikel/Chef-Beleidigung-auf-Facebook-rechtfertigt-Kuendigung-1717856.html>, 12. 8. 2013.

364 Presuda iz 2012. godine (Urteil vom 10. 10. 2012, Az.: 3 Sa 644/12), Pokrajinski sud Ham (Landesarbeitsgericht (LAG) Hamm).

Poslodavac je smatrao da je on u pravu u potpunosti i uložio je žalbu na ovu odluku suda. Apelacioni sud nije imao razumevanja za šegrta, jer on nije imao sedamnaest godina već dvadesetsedam godina i imao je dovoljno zrelosti da je mogao da proceni značenje svojih objava. Sa time i uz to što je u rubrici „Poslodavac“ izneo navedene uvrede, nije prema odluci suda obuhvaćeno pravo na slobodno mišljenje i izražavanje. Na taj način je ovom odlukom suda opravdan otkaz i on je postao pravno obavezujući za obe strane.³⁶⁵

Slučaj 4: Uvrede klijenata, kolega, šefa

Sud za radne sporove u Duisburgu osudio je jednog radnika zbog toga što je svoje kolege na Fejsbuk profilu označio kao „debele slanine i sveznalice“. Pošto se radilo o teškoj uvredi kolega, šefova, klijenata, sud je momentalni otkaz opravdao i potvrdio, ali ga je kasnije proglasio nevažećim.³⁶⁶

U obrazloženju suda potvrđeno je i da je moguće da se zaposlenom uruči otkaz i bez opomene. „U ovom slučaju se prema mišljenju suda nije radilo o običnom ogovaranju između kolega, već o teškoj uvredi, koja direktno pogađa lica kojih se tiče. Sve dok se objava ne obriše, ona se može pročitati i time ne gubi na svojoj težini. Takođe je bez značaja da li je objava bila ograničena na samo krug prijatelja ili širu javnost. Sve dok su Fejsbuk prijatelji i kolege sa posla, ne može se govoriti o privatnoj sferi“ navodi se u odluci suda.

I pored ovoga sud je krajem 2012. godine ovaj otkaz proglasio nevažećim, pošto se radilo o afektu. Naime, radnik je uvredljivi komentar napisao, pošto je on saznao, da je on kod šefa od strane kolega bio oklevetan.³⁶⁷

Slučaj 5: Otkaz konobarici zbog tuđe Fejsbuk objave

Tuđa objava i obeležavanje na slici na Fejsbuk zidu koštala je radnog mesta jednu konobaricu bečkog hotela Palais Strudlhof, iako ona baš nikakve veze sa ovom objavom nije imala. Momentalni otkaz je sa stanovišta Komore rada neosnovan i potrebno je da radnica pokrene sudske postupak protiv ove odluke poslodavca.

Fejsbuk prijateljstvo sa jednim kolegom, koji je loše o šefu pisao, bilo je obrazloženje za otkaz. Kolega sa kojim je konobarica prijatelj na Fejsbuku i ostale kolege su nju ubacili u vidu linka tako da je i njeno ime bilo u ovoj uvredljivoj objavi, a ispod objave su ispisani bili komentari.

Inače sama objava se ticala programa štednje vlade. Kraj objave je glasilo „veliki pozdrav, generalni direktor hotela i vi možete da mi...“.³⁶⁸

365 *Beleidigung auf Facebook: Kündigung rechtens*, heiseResale, Marzena Sicking, <http://www.heise.de/resale/artikel/Beleidigung-auf-Facebook-Kuendigung-rechtens-1728766.html>, 20. 8. 2013.

366 *Lästern auf Facebook ein Kündigungsgrund?* heiseResale, Marzena Sicking, <http://www.heise.de/resale/artikel/Laestern-auf-Facebook-ein-Kuendigungsgrund-1737910.html>, 20. 8. 2013.

367 Presuda iz 2012. godine (Urteil vom 26. 9. 2012, Az.: 5 Ca 949/12), Sud za radne sporove Duisburg (Arbeitsgericht Duisburg).

368 *Österreich: Nach Facebook-Eintrag gefeuert*, futurezone.at, Anita Staudacher, <http://futurezone.at/digitallife/8419-oesterreich-nach-facebook-eintrag-gefeuert.php>, 22. 8. 2013.

Objava je inače koštala gubitka posla troje kolega — autora, komentatora i konobaricu, koja nije reagovala na objave, jer nije bila onlajn u trenutku objave.

Prema mišljenju Komore rada „otpuštanje sa posla je potpuno u ovom slučaju nerazumljivo, pošto konobarica nije imala nikakvu aktivnost, da bi joj se krivica mogla pripisati. Razlog u vidu ćaskanja preko Fejsbuka i gubitak poverenja ne predstavlja dovoljno jak argumenat za otkaz. Osim toga razlog za ovakve objave su neisplaćene zarade. Ipak radnici treba da obrate pažnju da poslovne tajne ne otkrivaju na Fejsbuku, pošto ih sa stanovišta poslodavaca može zadesiti otkaz zbog kršenja lojalnosti, poverenja ili dužnosti obzira prema drugim kolegama“.

Ostaje da se vidi da li će otpušteni tužiti poslodavca zbog otkaza.³⁶⁹ Jedno je sigurno postoji velika razlika da li je neko nešto privatno ispričao ili postavio na Fejsbuk.

Slučaj 6: Lajk dugme koštalo posla tri žene

U austrijskoj pokrajini Tirol su tri žene momentalno otpuštene, pošto su izrazile svoje nezadovoljstvo na poslu i nezadovoljstvo odnosom sa svojim predpostavljenim putem Fejsbuka. Jedna od njih je na svom profilu imenujući svoga šefa izrazila svoje nezadovoljstvo, dok su ostale kolegice tu objavu sa lajk dugmetom potvrdile. Iako šef nije imao veliki broj prijatelja na Fejsbuku oko 250, on je za ovu objavu saznao i momentalno svim učesnicama uručio otkaz.

Prema mišljenju Komore rada „za otpuštanje sa posla bio je neophodan bitniji razlog, pošto izražavanje nezadovoljstva među prijateljima na društvenim mrežama nije relevantno sa stanovišta radnog prava. Iako je naravno ostalo sporno, u kojoj meri tzv. lajkovanje predstavlja uvredu i kada se smatra kao uvreda. Osim toga trebalo bi se na Fejsbuku tako ponašati, kao da ste u javnosti, te je poželjno više obratiti pažnju šta se objavljuje. Iako su objave upućene užem krugu Fejsbuk prijatelja, ipak nije svaki prijatelj na Fejsbuku pravi prijatelj“.

U ovom slučaju su sve tri radnice svoje nezadovoljstvo i pravdu potražile pred sudom. Sudski postupak je u toku.³⁷⁰

Slučaj 7: Lajk dugme i pravo na slobodno mišljenje i izražavanje (slobodu govora)

U američkoj saveznoj državi Virdžiniji su zaposleni jedne firme lajkovali službene stranice protivnika izbora i zbog toga bili otpušteni.

U žalbi na ovu odluku istakli su kao argument pravo na slobodu govora. Sudija u ovom predmetu se nije složio sa ovim argumentom „jer lajkovanje ne može predstavljati formu koja se može smatrati govorom. Samo lajkovanje nije dovoljno.

369 *Die zehn kuriosesten Facebookfälle Österreichs*, heuteOnline.at, <http://www.heute.at/news/multi-media/art23657%2c743140>, 20. 8. 2013.

370 *FALL 2 — Facebook-“Like“ kostet drei Frauen den Job*, heute.at, <http://www.heute.at/news/multi-media/art23657%2c743140%2c2>, 21. 8. 2013.

To nije vrsta komentara koja je u prethodnim slučajevima omogućila zaštitu otpuštenima. Jedan klik i tekst nisu isto“.³⁷¹

U ovaj spor se umešao i sam Fejsbuk ali i Udruženje američkih građanskih sloboda (American Civil Liberties Union), tako da je ova odluka suda u žalbenom postupku ukinuta. Prema njihovim argumentima, koje je sud prihvatio „sloboda govora je ustavom zagarantovano pravo. Sa klikom na lajk dugme, ova aktivnost predstavlja slobodu govora. Sa klikom se inače može postaviti video na internet, donirati novac, proslediti e-mail, glasati ili potpisati peticija. Jednostavnost postupka ne ograničava značenje ovog prava. Svejedno je da li se napiše sviđa mi se ili klikne na lajk dugme. Takođe ove radnje su ustavom garantovane“.

Sud je ovom odlukom jasno ustanovio primenu prava na slobodu govora i važenje ovog prava u odnosu na sve forme u kojima se misli i mišljenja mogu izraziti.³⁷²

Slučaj 8: Bolovanje i Fejsbuk kao svedok

Ne tako redak slučaj u praksi, gde zaposleni bolovanje koriste za noćni provod i žurke, desio se u austrijskoj pokrajini Gornjoj Austriji u gradu Lincu. Za jednu konobaricu je objavljivanje slika na Fejsbuku bilo pogubno. Na ovaj način nepažljivi zaposleni pružaju dokaze za opravdano davanje otkaza.

Konobarica je otvorila bolovanje, ali je neposredno pre isteka bolovanja otišla u diskoteku. Potom je na svom profilu postavila slike sa komentarima „kako alkohol ubija i kako neće više nikada izlaziti“.

Za Privrednu komoru pokrajine Donja Austrija je ovo svakako opravdan razlog za davanje otkaza, pošto predstavlja zloupotrebu prava na bolovanje.³⁷³

5.5. Objavljivanje statusa na Fejsbuku

Slučaj 1: Osuda zbog rasističkih objava na Fejsbuku

U Beču je polovinom 2013. godine jedna 60 godišnjakinja zbog propagiranja progona Jevreja i Muslimana osuđena na 9 meseci uslovno. Kako je navela u svojoj objavi „Ekstremni Muslimani nam vladaju. Oni žele da zagospodare nama“. Pored toga nazvala je Muslimane „ruljom ološem, šljamom, žgadijom“, dok je islam kao veru nazvala „najvećom prljavštinom 21. veka“. Turske doseljenike je nazvala „anal-

371 *Kako su zbog lajkova ostali bez posla*, (Preuzeto sa sajta S media — 8. 5. 2012), sajt infostud.com, http://poslovi.infostud.com/vesti/Kako-su-zbog-lajkova-ostali-bez-posla/42237?utm_source=mejling_lista_poslovi&utm_campaign=vesti_2012-05-14&utm_medium=sadržaj_vest, 22. 8. 2013.

372 Andreas Wilkens, *Facebook: „Likes“ stehen unter dem Schutz der US-Verfassung*, heiseOnline, <http://www.heise.de/newsticker/meldung/Facebook-Likes-stehen-unter-dem-Schutz-der-US-Verfassung-1662776.html>, 22. 8. 2013.

373 *FALL 7 — Party im Krankenstand und Facebook als Zeuge*, heute.at, <http://www.heute.at/news/multimedia/art23657%2c743140%2c7>, 21. 8. 2013.

fabetama iz Anadolije“. Takođe je dodala da „Austriji ne trebaju varvari, i da treba da se liši otvorenih vrata za sve parazite“.

Njena odbrana pred sudom je išla u pravcu odbrane zapadne kulture i civilizacije. Kao psiholog i rođena Poljakinja, imala je navodno prilike da se uveri, koliko Turcima fali obrazovanje. Beč u kome ona živi od 1999. godine, je jedan biser i takav treba i da ostane. Prema njenoj predstavi „U Beču ne smeju da ostanu svi Muslimani, nego samo oni, koji mirno žive i ne ugnjetavaju žene“. „U džamijama se propagira mržnja prema hrišćanima, te kada se to oseti i vidi, dolazi do osećaja gorčine“.

Zastupnica osuđene je imala takođe komentare poput „Potamaniti, istrebiti! Poslati ih odakle su došli u jednom pravcu vagonima za stoku“.

Govora mržnje nisu bili pošteđeni ni Jevreji. Međutim, ona nije imala ništa protiv Jevreja, već „protiv cionizma“. Za sud su ovo bili dovoljni dokazi da se optužena oglasi krivom i dobije uslovnu osudu.³⁷⁴

Slučaj 2: Oslobađajuća odluka za Fejsbuk objavu

Sličan predhodnom slučaju desio se polovinom 2012. godine u Salcburgu, gde je jedan 39 godišnjak na svom Fejsbuk profilu objavio puno komentara u grupi „Amina treba da ode“ i te svoje izjave lajkovao. Osim toga imao je i lajkove protiv islama i Turaka.

„Amina treba da ode, bolje danas nego sutra. Dalje sa šljamom, odmah prote-rati i bez ako i ali“ napisao je ovaj bravar iz Salcburga. Već sutradan su se istražitelji pojavili ispred njegovih vrata. Neki od njegovih objava bili su i „Turski doseljenici moraju otići“, „Nama ne trebaju varvari iz Anadolije“, „Beč nije kloaka, nije turski bazar“.

Amina je inače devojčica iz Dagestana, kojoj je pretilo proterivanje iz Austrije. Iz tih razloga je podignuta optužnica za raspirivanje rasne i verske mržnje protiv ovog Salcburžanina.

On se branio da se njegova objava o šljamu nije odnosila na Aminu, već na objavu koja je u međuvremenu obrisana. Tvrdio je da nije želeo nikoga da uvredi i da podstakne na rasnu, versku mržnju i netrepeljivost.

Sud je smatrao da izloženi dokazi nisu dovoljni da bi došlo do osude za ovo delo. U njegovoj izjavi za Aminu, on nije izrazio netrepeljivost i podsticao na mržnju prema određenoj grupi, već je izrazio nezadovoljstvo protiv određene osobe. Ovde bi se moglo raditi o uvredi određene osobe te bi se krivično gonjenje moglo obaviti po privatnoj tužbi. Ipak, Amina sama nije podigla optužnicu, stoga je došlo do oslobađajuće presude.³⁷⁵

374 *Wienerin nach rassistischen Facebook-Posts verurteilt*, derStandard.at, <http://derstandard.at/1375625865894/Wienerin-nach-rassistischen-Facebook-Postings-verurteilt>, 8. 8. 2013.

375 *Hetze auf Facebook: Freispruch für Salzburger*, futurezone.at, apa, <http://futurezone.at/digital-life/10520-hetze-auf-facebook-freispruch-fuer-salzbuerger.php>, 11. 8. 2013.

Slučaj 3: **„Bezazlena šala“**

Zbog naivne i nesmotrene izjave objavljene u jednoj diskusiji na Fejsbuku osamnaestogodišnjem dečaku prethodi kazna od čak 8 godina zatvora. Da šale ne mogu od svakog biti pravilno shvaćene i da je smisao za humor individualan, pokazuje i ovaj slučaj.³⁷⁶

U Teksasu je jedan mladić igrajući igricu preko Fejsbuka u diskusiji na pitanje „da li je on lud? Odgovorio — Da, ja sam zaista zbunjen u mojoj glavi, ja ću celu školu punu dece pobiti i poješću njihova srca koja još uvek kucaju“. Iako je u nastavku ovog komentara stavio „LOL“ (laughing out loud) i „JK“ (just kidding) odnosno da umire od smeha i da se samo šali, granicu njegove šale očigledno nisu svi jednako razumeli. Stoga jedna Kanadanka, koja ovu objavu uopšte nije smatrala kao šalu, otkrila je da se u blizini mladića nalazi škola, pa je iz tih razloga kontaktirala policiju. Policija je takođe smatrala da je šala neumesna i zatvorila mladića. Iako proces još uvek nije okončan, mladiću ukoliko bude bio osuđen prethodi kazna do 8 godina zatvora.³⁷⁷ Anonimni donator je uplatio 500.000 dolara kaucije da se mladić pusti iz zatvora, pošto su njegovi roditelji pokrenuli onlajn peticiju da se njihov sin oslobodi.³⁷⁸

Slučaj 4: **Antisemitska karikatura na Fejsbuku**

Na sajtu najveće opozicione partije u Austriji Slobodarske partije Austrije (FPÖ), koju predvodi Hajc Kristijan Štrahe, objavljena je karikatura koja prikazuje jednog bankara, kojeg država tovi, dok narod gladuje. Sama karikatura po stilu, detaljima, podseća na antisemitske crteže kojima se širila mržnja za vreme nacističkog Trećeg rajha.

Pošto tužilaštvu nije bilo poznato, ko je karikaturu postavio, još uvek nije pokrenut postupak. Inače u međuvremenu je slika zamenjena i postavljena je blaža varijanta.

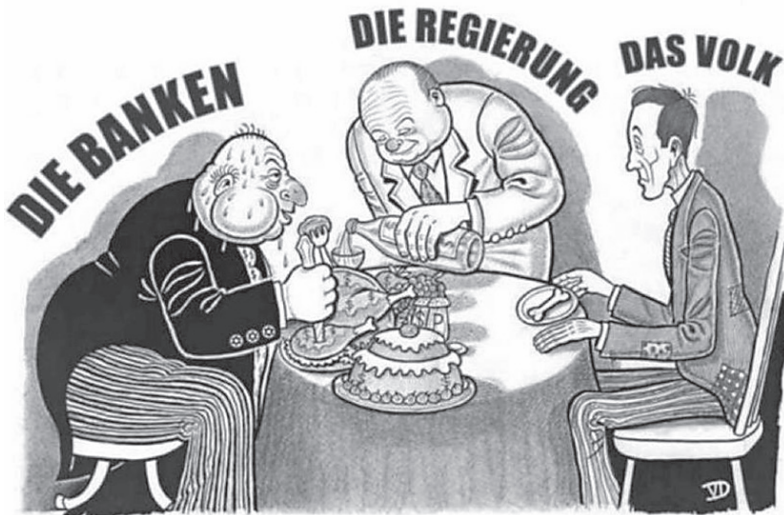
376 Nedavno se u Britaniji desio slučaj u kome je jedan Britanac najpre osuđen, jer je putem Tvitera poslao navodnu preteću poruku da će dići u vazduh jedan aerodrom. Razočaran jer je aerodrom zbog snega bio zatvoren a on žurio kod devojke, na Tviteru je napisao da će aerodrom dići u vazduh. Posle te objave je uhapšen i njegova žalba za oslobađanje odbijena, jer „poruka potencijalno može izazvati stvarnu zabrinutost javnosti“. Potom ga je sud oslobodio optužbi, ali je nesrećni čovek ostao zbog te osude i bez posla. Sud je u oslobađajućoj presudi konstatovao da „ukoliko će osoba ili osobe koje je prime ili pročitaju, ili osnovano očekuju da će je primiti ili pročitati, staviti na stranu kao glupu ili nekusnu šalu, ili shvatiti kao prazno, bombastično ili smešno šegačenje, onda bi bilo protivrečno opisati je kao poruku pretećeg karaktera“. I pored ove konstatacije, očigledno je da se pojam šale individualno doživljava. *Ukinuta presuda zbog šale na Twitteru*, MIKRO, sajt b92, http://www.b92.net/tehnopolis/aktuelno.php?yyyy=2012&mm=07&nav_id=630202, 12. 8. 2013.

377 *Facebook-Posting: 8 Jahre Haft für Teenager?*, öe24.at., <http://www.oe24.at/digital/Facebook-Posting-8-Jahre-Haft-fuer-Teenager/108845153>, 8. 8. 2013.

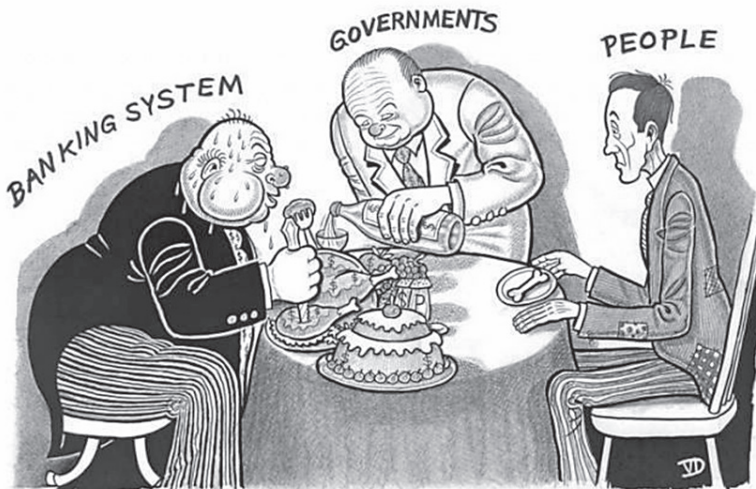
378 *19-Jähriger vorerst frei Facebook-Scherz: 500.000\$ Kaution für Teenie*, öe24.at., <http://www.oe24.at/digital/Facebook-Scherz-500-000Dollar-Kaution-fuer-Teenie/109940065>, 8. 8. 2013.

U verziji koju je Štrahe postavio na svom nalogu bankar ima ogroman nos, što se koristilo u nacističkim crtežima kao obeležje za Jevreje. Na bankarovom rukavu se nalaze dugmad sa Davidovom zvezdom.

Sam Štrahe je sve ove tvrdnje odbacio uz komentar „da on već godinama kritikuje svemoć bankarskog sistema, koji je postao sve deblji i moćniji i na račun građana“. „Kada potom postavim karikaturu na svom nalogu, koji su drugi korisnici već postavljali, onda mi se podmeće antisemitizam“ istakao je Štrahe.³⁷⁹ Davidovu zvezdu na bankarovom rukavu Štrahe nije uopšte ni primetio.³⁸⁰



Antisemitisička karikatura



Originalna karikatura

379 *Strache: Antisemitischer Cartoon auf Facebook*, futurzone.at, <http://futurezone.at/netzpolitik/10782-strache-antisemitischer-cartoon-auf-facebook.php>, 11. 8. 2013.

380 *Antisemitiska karikatura na Fejsbuk strani lidera opozicije*, blic.rs, <http://www.blic.rs/Vesti/Svet/338915/Antisemitiska-karikatura-na-Fejsbuk-strani-lidera-opozicije>, 11. 8. 2013.

Ovaj slučaj podstakao je i advokata Geoga Cangeru da podigne optužnicu protiv tužilaštva zbog nečinjenja i zloupotrebe službe.

Prema mišljenju ovog advokata, tužilaštvo je moralo smesta da blokira i obriše Fejsbuk stranicu Slobodarske partije Austrije zbog ove antisemitističke karikature. Time bi se Savezna vlada Austrije jasno distancirala od antisemitizma, rasizma i podsticanja mržnje i netrepeljivosti. Osim toga na stranici najveće opozicione partije Austrije je na ovu temu napisano na stotine komentara i sve to praćeno je od strane brojnih fanova ove partije. Stoga je sve ovo prema stavu advokata izgledalo kao nastup za vreme propagande nacional-socijalističke Nemačke. Nečinjenje tužilaštva podstreklo je i ohrabrilo simpatizere i fanove ove stranice i time stavilo u povoljan položaj ovo protivzakonito ponašanje. Očekuje se da nadležni državni organi provere ove tvrdnje.³⁸¹

Slučaj 5: Ubistvo devojčice zbog objave na Fejsbuka

U Holandiji u mestu Arnheim je jedna petnaestogodišnja devojčica ubijena, pošto je putem Fejsbuka širila loše vesti o svojoj drugarici. Petnaestogodišnji dečak je izvršio ubistvo devojčice po nalogu dva mladića i uvređene devojčice, koji su mu za ubistvo platili 100 evra.

Sve je počelo putem Fejsbuka gde je nesrećna devojčica napisala, da je njena drugarica imala seksualne odnose sa više mladića. Zbog ovih objava je njena drugarica htela da joj se osveti. Zajedno sa svojim drugarima je planirala ubistvo i za to platila 100 evra.³⁸² Ubistvo je izvršeno ubodima u lice i vrat.

Ubica je osuđen na godinu dana zatvora, što je najveća kazna za maloletnike u Holandiji i prinudno psihijatrijsko lečenje.³⁸³ Otac ubijene devojčice je bio zgrožen ovako niskom kaznom za ubistvo i istakao je da je on izgubio svoju ćerku, a da će ubica u zatvoru provesti svega godinu dana.³⁸⁴ Apelovao je na političare da pooštre kazne za ovakve slučajeve. Opasnosti koje nose sa sobom društvene mreže i čet portali se često podcenjuju istakao je otac ubijene devojčice. Na suđenje čekaju još uvek devojčica koja je dala nalog za ubistvo i još jedan mladić.

Slučaj 6: Pretnje potpredsedniku Vlade Srbije

Koliko su Fejsbuk objave opasne i gde je granica pravu slobodnog mišljenja i izražavanja pokazuje i slučaj objave novinara lista Pečat Pavla Ćosića. Novinar je na svojoj Fejsbuk stranici pozvao na ubistvo tada prvog potpredsednika Vlade Aleksandra Vučića i ponudio novac onome ko to učini.³⁸⁵

381 *Hetz-Cartoon: Anzeige gegen Staatsanwaltschaft*, APA, futurezone.at, <http://futurezone.at/netzpolitik/10883-hetz-cartoon-anzeige-gegen-staatsanwaltschaft.php>, 11. 8. 2013.

382 *Godinu dana zatvora za maloletnog „Fejsbuk ubicu“ u Holandiji*, Beta, blic.rs, <http://www.blic.rs/Vesti/Svet/340972/Godinu-dana-zatvora-za-maloletnog-Fejsbuk-ubicu-u-Holandiji>, 11. 8. 2013.

383 *Mord an 15-Jähriger wegen Facebook-Postings*, heute.at, <http://www.heute.at/news/welt/art23661,771005>, 11. 8. 2013.

384 *Höchststrafe für „Facebook-Mörder“ (15)*, heute.at, <http://www.heute.at/news/multimedia/art23657,779686>, 11. 8. 2013.

385 *Priveden zbog pretnje Vučiću*, Novosti online, <http://www.novosti.rs/vesti/naslovna/hronika/aktuelno.291.html:449395-Priveden-zbog-pretnje-Vucicu>, 20. 8. 2013.



„S obzirom na to da se na Fejsbuku pojavila ozbiljna pretnja upućena šticeñoj ličnosti, ne samo u smislu pretnje nego i nuđenja novca da se likvidira određena šticeña ličnost, policija je pronašla to lice, privela ga i „mi ćemo dalje preduzimati mere u skladu sa zakonom, odnosno u dogovoru sa tužilaštvom“ rekao je tadašnji direktor policije Veljović.

Čosić je posle privođenja saslušan i tom prilikom je izjavio da je bio pijan i da je ujutru kada je video šta je napisao to odmah obrisao. Osim toga izjavio je da mu ni na kraj pameti nije bilo da naruči ubistvo ili da ubije Vučića. Policija je tokom istrage zaplenila računar novinara da bi ispitala njegov sadržaj. Posle saslušanja Čosić je pušten na slobodu.³⁸⁶

Slučaj 7: Osuda zbog verskog opredeljenja

U Indoneziji je na ostrvu Sumatra jedan tridesetdvogodišnjak osuđen na dve ipo godine zatvora, zbog izjašnjavanja putem Fejsbuka o svojoj verskoj pripadnosti. Pošto je priznao da je ateista, osuđen je za bogohuljenje, jer je time uvredio proroka Muhameda. Ovaj čovek je putem Fejsbuka napravio grupu u kojoj je imao objave svoje religijske pripadnosti, odnosno osećanja.

Pored toga što je prihvatio osudu ovaj Indonežanin smatra „da je verovanje privatna stvar i da se on zbog svojih objava izvinio svojoj familiji i vernicima“. On je prvi čovek osuđen zbog toga što ne veruje u Boga. Indonezija je inače sekularna zemlja sa najvećom islamskom zajednicom na svetu. 88% od 240 miliona stanovnika čine muslimani.³⁸⁷

Slučaj 8: Osuda zbog vredanja monaha

U Grčkoj je jedan dvadesetsedmogodišnji muškarac uhapšen, zbog toga što je na Fejsbuku ismevao mrtvog pravoslavnog monaha. Uhapšeni je napravio Fejsbuk

386 *Uhapšen opasan ludak*: Nudio 10.000 evra za Vučićevo ubistvo!, kurirOnline, <http://www.kurir-info.rs/uhapšen-opasan-ludak-nudio-10000-evra-za-vucicevo-ubistvo-clanak-940653>, 20. 8. 2013.

387 *Indonesien: Atheist wegen Facebook verurteilt, apa*, futurezone.at, <http://futurezone.at/digitallife/9607-indonesien-atheist-wegen-facebook-verurteilt.php>, 12. 8. 2013.

stranicu na kojoj je ismevan otac Paisios. Ova stranica je bila posvećena „ocu Pastiosu“, što je aluzija na popularno grčko jelo od testa i mlevene govedine — pasticio. Na stranici je monah prikazan sa licem preliveanim pasticiom.

Policija je ovu Fejsbuk stranicu uklonila i objasnila da je sadržala „bogohuljenje i uvrede na račun oca Paisiosa i pravoslavnog hrišćanstva u celini“.

Otac Paisios je monah koji je umro je 1994., koji ima veliki broj sledbenika u Grčkoj. Njegove proročanske moći i učenja doprinela su njegovom velikom broju sledbenika. Poznavaoi njegovih dela i moći tvrde da je prerekao raspad Sovjetskog Saveza, tursku invaziju na Kipar i aktuelnu ekonomsku krizu u Grčkoj.³⁸⁸

5.6. Žurke i pozivi na veselja

Slučaj 1:

Na rođendansku žurku je došlo 48.000 gostiju

Četrnaestogodišnji Francuz je putem Fejsbuka pozvao na svoju rođendansku proslavu ni manje ni više nego 48.000 ljudi, iako je tom prilikom želeo svega njih 29 da pozove. Užasnuti roditelji su podigli tužbu i tvrdili da se ime njihovog sina zloupotrebilo prilikom pozivanja na proslavu. Zvanice su pretile da će sve porazbijati, ukoliko se žurka otkaže.

Mladić je prvobitno stupio u kontakt sa prijateljima telefonskim putem. Da bi mu olakšao i pomogao u zvanju prijatelja, njegov drugar je na Fejsbuku napravio grupu i poziv sa sloganom „Tajni događaj“. Pošto je grupa bila javnog karaktera ubrzo se 16.500 ljudi prijavilo u grupu. Od tog broja svako je pozvao po još 60 ljudi. Potom je u nekoliko dana taj broj narastao na 48.000 zvanica.³⁸⁹

Ovaj slučaj očekuje pravni epilog, ali je pravo pitanje čija je odgovornost u ovom slučaju.

Slučaj 2:

Šegrt treba da plati kaznu od 200.000 evra, zbog poziva na žurku

Zbog poziva na žurku na bazenu u nemačkom gradu Konstancu putem Fejsbuka, jednom dvadesetogodišnjem Nemcu je izrečena drakonska kazna. Koliko je bio iznenađen govore i njegove reči „Mislio sam da je to dozvoljeno, i sam sam bio na mnogo ilegalnih Fejsbuk žurki. Hteo sam da napravim bolju“.

Uprkos zabrani okupljanja, osuđeni je više puta pozivao putem Fejsbuka na okupljanje. Tom prilikom se okupilo 12.000 ljudi i došlo do oštećenja imovine, tuča, telesnih povreda i sukoba sa lokalnom policijom. Ceo ovaj događaj i šteta procenjeni su na 200.000 evra, koju treba po shvatanju suda da snosi onaj ko je

388 Uhapšen zbog vredanja mrtvog kaludera na Fejsbuku, Tanjug, sajt blic.rs, <http://www.blic.rs/Slobodno-vreme/Zanimljivosti/344443/Uhapšen-zbog-vredjanja-mrtvog-kaludjera-na-Fejsbuku>, 12. 8. 2013.

389 Facebook: 48.000 Gäste bei Geburtstagsfeier, oe24.at, <http://www.oe24.at/digital/Facebook-48-000-Gaeste-bei-Geburtstagsfeier/64108872>, 29. 7. 2013.

i izazvao događaj. Policija stoji iza toga da je nepravedno da troškove ove zabave snose poreski obveznici.³⁹⁰ Takođe tom prilikom je otkivena i rupa u zakonu. Da bi se uopšte nekome ispostavio račun za troškove npr. čišćenja prostora posle sličnih priredbi, potrebno je da dođe do intervencije ili komunalne službe ili policije da bi se ovi troškovi stavili na račun organizatora priredbe.

Treba imati u vidu da je u akciji policije bilo angažovano 5 helikoptera i 280 službenika policije. Pored toga naknadu štete tražili su i vlasnici kioska u iznosu od 20.000 evra i sam grad Konstanc od 15.000 evra. Poređenja radi, šegrt zarađuje mesečno 560 evra. Od čega će šegrt to i platiti, ostaje pitanje. Ono što se desilo potom, je da je policija iz preventivnih razloga zatvorila bazen, zbog mogućnosti ponavljanja ovog nemilog događaja.³⁹¹

Nemački policijski sindikat se zalaže da se zakonski uvede i odgovornost Fejsbuka. Obrazloženje za ovakvu inicijativu je da ova društvena mreža predstavlja platformu, koja omogućava korisnicima da pozivaju na ovakve manifestacije. Tako da po mišljenju sindikata Fejsbuk ne može da se ponaša, kao da ih ovi događaji ne interesuju. Naravno glavni odgovorni i dalje bi trebalo da ostane onaj koji poziva na ovakvu vrstu okupljanja. Podršku ovom predlogu sindikata pružili su i brojni nemački političari. Prema njihovom mišljenju Fejsbuk kao platforma, koja omogućava ovaj način okupljanja mora uvesti mehanizme zaštite kako bi se interesi javnosti zaštitili, pošto do ovakvih nemilih događaja može doći samo jednim klikom mišem. Velika je razlika da li će ceo svet biti pozvan ili samo određeni krug prijatelja.³⁹²

Slučaj 3: Povređeni na lovištu

U ovom slučaju umesto 20 gostiju došlo je 200. Radnja se odvijala u lovištu u blizini nemačkog grada Ingolštata. Tom prilikom je došlo do uboda nožem od strane jednog osamnaestogodišnjeg dečaka, koji je tom prilikom teško ranio drugog mladića, koji je sa teškim ranama u predelu ramena i ruku prebačen u bolnicu. Policija je podigla optužnicu protiv napadača za pokušaj ubistva. Jedan pijani mladić je na istoj žurci pao u logorsku vatru u bašti, dok je veliki broj gostiju završio u bolnici zbog trovanja alkoholom. Pored toga iza svega je ostala ogromna količina đubreta, a lovište je bil opustošeno.³⁹³

390 Jörg Wirtgen, *Polizei bemängelt Gesetzeslücke bei Kostenbeteiligung für Facebook-Partys*, heiseOnline, <http://www.heise.de/newsticker/meldung/Polizei-bemaengelt-Gesetzesluecke-bei-Kostenbeteiligung-fuer-Facebook-Partys-1665641.html>, 29. 7. 2013.

391 Harald Bögeholz, *Lehrling soll 200.000 Euro für Facebook-Party zahlen*, heiseOnline, <http://www.heise.de/newsticker/meldung/Lehrling-soll-200-000-Euro-fuer-Facebook-Party-zahlen-1655090.html>, 29.7. 2013.

392 Stefan Krempel, *Polizei will Facebook an Kosten illegaler Partys beteiligen*, heiseOnline, <http://www.heise.de/newsticker/meldung/Polizei-will-Facebook-an-Kosten-illegaler-Partys-beteiligen-1665220.html>, 29. 7. 2013.

393 *Verletzte bei Facebook-Party in Jagdhaus*, Dpa, heiseOnline, <http://futurezone.at/digitallife/11214-verletzte-bei-facebook-party-in-jagdhaus.php>, 30. 7. 2013.

Slučaj 4: **Preko Fejsbuka greškom pozvala 4.000 gostiju na žurku**

U Holandiji u gradiću Harenu se takođe desio slučaj gde je jedna 16 godišnja devojka pogrešnim klikom pozvala više od 30.000 ljudi na svoju rođendansku proslavu. Planiran je poziv za uži krug prijatelja. Toliki broj poziva usledio je jer su prijatelji obavestavali prijatelje o žurki, oni dalje svoje prijatelje, pa je tako došlo do ogromnog broja zvanica. Naravno i ovaj slučaj se desio zbog klika na javnu žurku. Pored toga nekoliko veb sajtova je pozvalo na žurku i doprinelo većem broju zvanica, a na jednom je stajalo „Projekat X Haren“ i odbrojalo se vreme do početka žurke uz navode da je pozvano 150.000 ljudi. Na istom veb sajtu je objavljena i adresa na kojoj je proslava uz napomenu „Gledajte kako umete da sa sobom povedete i prijatelje“.³⁹⁴

U Haren, gradić sa oko 18.000 stanovnika, došlo 4.000 gostiju. Tom prilikom intervenisala je i policija, a kada je pokušala da otera goste, bila je zasuta kamenicama, flašama, biciklima i saksijama za cveće. U centru grada su uništavani parkirani automobili, ulično osvetljenje, saobraćajni znaci, ograde od dvorišta privatnih kuća, kiosci i lokali. Bilans je da je 30 ljudi povređeno, od toga dvoje teško, a uhapšene su četiri osobe, a 500 pripadnika policije bilo je angažovano u intervenciji.³⁹⁵ Šteta je procenjena na milion evra.³⁹⁶

Slučaj 5: **Velika žurka u Beču nakon poziva preko Fejsbuka**

I Austriju nisu zaobišle žurke, koje su inicirane putem Fejsbuka. Pod sloganom „igraj preko dana“ okupilo se u bečkom dvadesetom okrugu Brigitenau preko 700 gostiju. Uz preglasnu muziku slavilo se od 17–22 h. Učesnici su se pentrali po ogradama kuća, mokrili po livadi i ostavili ogromnu količinu đubreta. Za ovaj događaj takođe je podignuta optužnica. Inicijatori poziva na ovu Fejsbuk žurku, još uvek nisu poznati.³⁹⁷

5.7. Cenzura na Fejsbuku zbog slike Gustava Kurbea „Poreklo sveta“

Ovaj slučaj je interesantan sa mnogo aspekata, a pre svega sa stanovišta zaštite javnog morala od strane Fejsbuka sa jedne strane i sudske nadležnosti sa druge strane.

³⁹⁴ Preko „Fejsbuka“ greškom pozvala 4.000 gostiju na žurku, blic.rs., <http://www.blic.rs/Slobodno-vreme/Zanimljivosti/344023/Preko-Fejsbuka-greskom-pozvala-4000-gostiju-na-zurku>, 30. 7. 2013.

³⁹⁵ Facebook-Party endete mit Polizeieinsatz, Dpa, heiseOnline, <http://futurezone.at/digitallife/11478-facebook-party-endete-mit-polizeieinsatz.php>, 30. 7. 2013.

³⁹⁶ 1 Million Euro Schaden nach Facebook-Party, ANP, weltHeute.at, <http://www.heute.at/news/welt/art23661%2c791737>, 30. 7. 2013.

³⁹⁷ Großparty in Wien nach Facebook-Aufruf, öe.24.at, <http://www.oe24.at/digital/Facebook-Aufruf-zu-Grossparty-in-Wien-Brigittenau/64700826>, 8. 8. 2013.

Spor se dogodio u Francuskoj početkom 2011. godine, pošto je Francuski profesor Frederik Duran Beso (fra. Frédéric Durand-Baissas) na svom Fejsbuk profilu postavio sliku „Poreklo sveta“ (L'Origine Du Monde), francuskog slikara Gustava Kurbea. Ova slika u krupnom planu prikazuje ženski polni organ.

Zbog strikne politike u pogledu objavljivanja pornografije Fejsbuk je blokirao nalog francuskog profesora. Ovaj postupak je iziritirao profesora, pa je odlučio da tuži društvenu mrežu, jer Fejsbuk ne razlikuje pornografiju od umetnosti. Profesor je smatrao da se svakodnevno na Fejsbuku mogu videti ubistva, nasilja, a da ti sadržaji nisu cenzurisani. Njegov tužbeni zahtev se odnosio na povredu prava na slobodu izražavanja i zahtevao je naknadu štete u iznosu od 20.000 evra.³⁹⁸

Pariski Viši sud se početkom 2015. godine oglosio kao nadležan za rešenje ovog spora, iako se Fejsbuk branio već pomenutim klauzulama o korišćenju ove društvene mreže (tačka 15.), koje regulišu isključivu nadležnost sudova u Kaliforniji u SAD.³⁹⁹ Klauzula o isključivoj nadležnosti suda u Kaliforniji je zloupotrebljena, po mišljenju suda.

Fejsbuk ima takođe svoju filijalu u Francuskoj i ima dovoljno mogućnosti i sredstava da bi se spor obavio u Francuskoj. Pored toga Fejsbuk je tvrdio da profesor nije potrošač, jer usluge koristi besplatno. I ovaj argument je sud negirao.⁴⁰⁰

Ovu sudsku odluku potvrdio je i Apelacioni sud u Parizu početkom 2016. godine.⁴⁰¹

Fejsbuk je tvrdio da francusko pravo o zaštiti potrošača ne može da važi u ovom slučaju na korisnike Fejsbuka iz Francuske, pošto je Fejsbukov servis dostupan u čitavom svetu. Ova odluka bi mogla da bude presedan, jer će ubuduće francuski građani moći u sličnim situacijama da se na nju pozivaju.⁴⁰²

Frapantno je to da su se francuski sudovi 5 godina bavili sudskom nadležnosti, a da zapravo o samom sadržaju tužbe još uvek nije bilo reči.

Ono što zabrinjava u vezi sa ovim slučajem je da se Fejsbuk postavlja kao arbitar, šta treba zabraniti, ukloniti, obrisati, blokirati. Tako Fejsbuk treba da procenjuje moral, dobre običaje i uvredljive standarde. Poznato je da se ti standardi, nivo uvredljivosti razlikuju od kulture, tradicije i shvatanja u određenoj sredini. Fejsbuk samim definisanjem pojma „pornografija“ na ovaj način diktira standard u globalnom ponašanju. Može se stoga reći da je i ovo još jedan od elemenata gde Fejsbuk dobija prorogative države ili neku vrstu globalne „internet izvršne vlasti“ ili „globalnog arbitra u internet svetu“.

398 Kirsten Fiedler, *Zensur: Facebook gegen den Ursprung der Welt*, <https://netzpolitik.org/2016/zensur-facebook-gegen-den-ursprung-der-welt/>, 15. 10. 2017.

399 Tačka 15 može se pronaći na stranici <https://www.facebook.com/terms>. 15. 10. 2017.

400 Kontosperrung wegen Nacktgemälde: Facebook muss in Frankreich vor Gericht, portal euronews.com, <http://de.euronews.com/2016/02/12/kontosperrung-wegen-nacktgemaelde-facebook-muss-in-frankreich-vor-gericht>, 15. 10. 2017.

401 Florian Reynaud, *La justice confirme que les tribunaux français peuvent juger Facebook*, http://www.lemonde.fr/pixels/article/2016/02/12/la-justice-francaise-est-competente-pour-juger-facebook_4864381_4408996.html, 15. 10. 2017.

402 Regen Embuscado, *French Court Rules Against Facebook in Gustave Courbet Lawsuit*, <https://news.artnet.com/art-world/french-art-lovers-sue-facebook-426308>, 15. 10. 2017.

S obzirom da je u pitanju samoinicijativno blokiranje od strane Fejsbuka, a ne reagovanje po prijavi ostalih korisnika Fejsbuka, može se pretpostaviti i to da je sporna fotografija uočena na Fejsbuku uz pomoć softvera za procenu sadržaja. Softver je verovatno primetio na osnovu algoritma da se radi o golotinji, ali nije shvatio niti je to moguće da shvati da se radi o slici kao umetničkom delu. Isto tako se moglo raditi i o skulpturi ili o nekom drugom obliku umetničkog izražavanja. Softver nije u mogućnosti da proceni duhovni aspekt izražavanja, niti šta je neko sa izražavanjem mogao da misli.

Fejsbuk će tek trebati da se suoči sa sadržajem tužbe francuskog profesora Be-soa, pošto je sudska nadležnost ustanovljena. Francuski sud će imati težak zadatak da reši konflikt između ljudskih prava pojedinca iz EU sa jedne strane i Fejsbuka po osnovima načela ugovornog prava sa druge strane.

Ukoliko se uzme komponenta ljudskih prava čl. 10 Evropske konvencije o ljudskim pravima i osnovnim slobodama kojime se štiti sloboda izražavanja profesora u ovom slučaju, predviđa mogućnost da se cenzura može uvesti iz razloga zaštite morala. Neophodno je da cenzura bude u skladu sa zakonom, da je neophodna u demokratskom društvu a radi zaštite osnovnih vrednosti tog društva.⁴⁰³ Pritom će se po osnovu ljudskih prava postaviti pitanje pretežnijeg interesa?

Ukoliko se uzme komponenta ugovornog prava, može se postaviti pitanje: da li se korisnik Fejsbuka odrekao svog prava na slobodu izražavanja pristupanjem Fejsbuku ili se pak saglasio sa globalnim ponašanjem i standardom Fejsbuka? Drugim rečima: Da li je moguće odreći se prava na slobodu izražavanja ugovorom? Bez perjudiciranja rešenja ovoga spora, sigurno će poznata problematika svesnosti Fejsbuk korisnika o odricanju ovog prava biti problematična. Ukoliko bi se pravno na slobodu izražavanja tretiralo kao jedno od ugovornih načela u smislu dobrih običaja, standarda prakse itd., pitanje je čiji bi se običaji tada primenjivali? Dobri poslovni običaji Fejsbuka?

Odgovore na ova pitanja u ovom sporu daće odredbe francuskog prava.

5.8. Zaplena Fejsbuk profila

Početak 2012. godine u nemačkoj pokrajini Baden Vitenberg je jedan dvadesetogodišnjak optužen zbog saučesništva u krađi, pošto je svom prijatelju objasnio kako da provali u jednu kuću. Iako uobičajen slučaj u krivičnom pravu, od velikog značaja za pravnu praksu u pogledu Fejsbuka je odluka nadležnog sudije koji je vodio postupak. On je posegao za do sada neuobičajenom praksom. Pošto istraga nije donela odgovarajuće rezultate, jer je optuženi obrisao podatke iz telefona i na taj način sprečio istražne organe da se domognu korisnih podataka koji bi pomogli u istrazi, sudija je odlučio da zapleni Fejsbuk profil optuženog.

Ovom odlukom su obuhvaćene poruke, čet protokola, liste prijatelja, beleške, slike optuženog. Ono što je u ovom slučaju bitno napomenuti, je da optuženi i pored toga što je od javnosti hteo da sakrije ove podatke, nije imao u vidu da su ovi

⁴⁰³ Miloš Stojković, *Fejsbuk i pornografija: sloboda izražavanja ili globalna cenzura*, <http://pravoikt.org/fejsbuk-i-pornografija-sloboda-izrazavanja-ili-globalna-cenzura/>, 15. 10. 2017.

podaci snimljeni na Fejsbuk serverima. Sudija je svoju odluku opravdao i time da je zaplena poruka i ovog načina komunikacije uporediva sa poštom i telegramima. Takva zaplena je dozvoljena shodno članu 99 nemačkog Zakona o krivično procesnom pravu.

Ipak ova odluka sudije ostala je samo pokušaj, pošto je izostalo njeno sprovođenje u praksi. Sprovođenje je izostalo zbog problema vezanog za sudsku pomoć i činjenicu, gde se Fejsbuk serveri i podaci nalaze. Nemačka filijala Fejsbuka je ovaj zahtev suda uputila svom predstavništvu u Irskoj, zbog toga što nije imala direktan pristup podacima. Irsko predstavništvo je odbilo da isporuči podatke, tvrdeći da se podaci nalaze u SAD.

U međuvremenu se spor završio osudom. Ono što je ovaj slučaj pokazao je da Fejsbuk nije najspremniji na saradnju i pružanje pravne pomoći. Osim toga predstavlja i presedan u postupanju suda, koji bi se mogao primeniti i na ostale društvene mreže, čiji se podaci nalaze u EU.⁴⁰⁴

5.9. Fejsbuk kao sredstvo za istražne radnje

Slučaj 1:

Otkrivanje ubice, priznanje, ranije pretnje, pretpostavka nevinosti

Fejsbuk se sve češće koristi za istražne radnje kako u krivičnom tako i u predkrivičnom postupku. Tako se u Srbiji dogodio slučaj, koji će pored svireposti izvršenja krivičnog dela, ostati upamćen po tome što je policija iskoristila Fejsbuk, kao sredstvo za ponalaženje izvršioca krivičnog dela.

Iako je ime Darijan Musić poznato široj javnosti u Srbiji, ovaj slučaj je sa pravnog stanovišta izuzetno interesantan. Izvršilac krivičnog dela je zverski i na svirep način ubio svoju devojkicu. Ne ulazeći u detalje ovog monstruoznog čina, koncentrišaćemo se na način otkivanja krivičnog dela i pravne aspekte vezane za zaštitu izvršioca krivičnog dela.

Sam Darijan je priznao krivično delo putem Fejsbuka, ali ne samo to, otkrio je i lokaciju gde se nalazi tako što se ulogovao na svoj Fejsbuk profil, te je time omogućio policiji da mu uđe u trag i uhapsi ga. Predhodni slučajevi u međunarodnoj sudskoj praksi su pokazali da ovakav vid priznanja može biti učinjen u afektu, kao što je i samo krivično delo učinjeno iz ljubomore. Ne opravdavajući monstruošan čin izvršenja samog dela, oslanjajući se na sudsku praksu inostranih sudova, moguće je da se ovakav vid priznanja ne uzme kao relevantan. Ipak, sudska odluka u ovom sporu će pokazati i značaj priznanja ubistva putem Fejsbuka, kakvu ono težinu ima u realnom svetu.

Opuženi, da li i osuđeni već, ali u svakom slučaju obeleženi od stane okoline, je ubistvo i najavio, pošto je preko Fejsbuka napisao „da ga je devojkica varala dok je bio u zatvoru i da je treba ubiti i to više puta“.⁴⁰⁵

404 Georg Dreier, *Beschlagnahme 2.0.*, output online, <http://www.output.at/making-it-legal/beschlagnahme-2-0>, 15. 10. 2017.

405 *Mislim da je treba ubiti više puta!*, alo.rs, <http://www.alo.rs/vesti/aktuelno/mislim-da-je-treba-ubiti-vise-puta/4270>, 22. 8. 2013.

U ovom pogledu se pojavljuju novi pravni problemi kao što su pretpostavka nevinosti kao i ozbiljnost pretnje putem Fejsbuka i kada zapravo policija treba da reaguje?

Fejsbuk i pored svih svojih propusta nije platforma/država koja je dužna da štiti interese zaštite ljudskih života, iako ima sve elemente za to, kao i u standardnom shvatanju pojma državnosti — neograničenu teritorijalnu primenu, internet kao globalnu mrežu (teritorija), korisnike (stanovništvo), kao i mogućnost da reguliše da se određeni sadržaj objavi, obriše ili sakrije (vlast).⁴⁰⁶ Stoga proizlazi da je država imala dve mogućnosti: Ili da sazna od Fejsbuka za krivično delo, ako joj Fejsbuk pruži pravnu pomoć, ili da na drugi način preko internet provajdera u Srbiji dođe do podataka sa profila optuženog. Da li je država znala ili nije, pa nije intervenisala, pravo je hipotetičko pitanje! U Nemačkoj već postoje neka rešenja, ali i u svemu ovome treba pažljivo postupiti, jer može biti ugroženo pravo privatnosti pojedinaca. Tako su u gradu Hanoveru i u pokrajinama Donjoj Saksoniji i Hesenu napravljene stranice na Fejsbuku na kojima građani mogu prijaviti kriminalce ili potencijalne učinioce krivičnih dela.⁴⁰⁷ Međutim, ukoliko se bez osnovane sumnje kontroliše čitav Fejsbukov protok podatka u svrhu zaštite od krivičnih dela, to bi svakako predstavljalo kršenje prava privatnosti. Ali ukoliko se već nadziru elektronske komunikacije, što je u Srbiji i u nekim zemljama EU zakonski regulisano, postavlja se pitanje svrhe prikupljanja ovakvih podataka, ukoliko se krivično pravna preventivna funkcija izgubi.⁴⁰⁸ Osim toga optuženi je navedenu poruku pretnje poslao iz zatvora.

Ono što je sigurno je da pretpostavka nevinosti mora važiti sve do osude i u tome su glavni propusti medija, ali pre svega policije u ovom slučaju. Nesumljivo je da se radi o slučaju, koji sam po načinu izvršenja izaziva veliku pažnju javnosti. Međutim, ako se uzme u obzir da policija nije zaštitila i pravo optuženog na njegovu privatnost. Naime, da bi se dočarao i detaljnije opisao izvršilac krivičnog dela u medijima se može pročitati celokupan život Darijana Musića. Postavlja se i pitanje, ako ovo nije ranije bilo poznato policiji, zašto niko nije reagovao? Gde su granice prava javnosti da zna i privatnosti pojedinca? Da li javnost mora svaki detalj života optuženog da zna? Svakako da je za vid istrage zanimljivo da je Darijan ubijao i mučio životinje, voleo da puca, otvarao vrata motornom testerom, bio problematičan, učestvovao u tučama i bio nezadovoljan svojim životom, ali to su ipak stvari koje treba da se tiču istrage i ocene dokaza u sudskom postupku, a ne i šire javnosti.

406 O ovome govori i nedavna kampanja Marka Cakerberga i akcija za povezivanje na Fejsbuk što većeg broja korisnika. Trenutni cilj je postavljen na 5 milijardi korisnika, koji trenutno uopšte ne koriste internet. Sve je ovo naravno ispraćeno željom da se ljudi povežu. Video kampanja je dostupna na linku: http://www.youtube.com/watch?feature=player_embedded&v=NdWaZk vAJfMZuckerbergwillInternetzugangvereinfachen, dpa, futurzone.at, <http://futurezone.at/digital life/17818-zuckerberg-will-internetzugang-vereinfachen.php>, 22. 8. 2013.

407 Andreas Wilkens, *Schaar: Skepsis gegenüber Facebook-Fahndung*, heiseOnline, <http://www.heise.de/newsticker/meldung/Schaar-Skepsis-gegenueber-Facebook-Fahndung-1751005.html>, 23. 9. 2013.

408 O ovome će biti više reči u narednim poglavljima.

Slučaj 2:
Pretnje ubistvom i intervencija policije

Za razliku od predhodnog slučaja, u inostranoj praksi je policija zbog pretnji ubistvom putem Fejsbuka preventivno intervenisala. U ovom slučaju se radi o pretnji ubistvom devetorici momaka bivše devojke od strane jednog devetnaestogodišnjaka iz Boicenburga u Nemačkoj. Mladić je želeo da ubije svu devetoricu a potom izvrši samoubistvo. Da bi ga ozbiljno shvatili, na svom profilu postavio je sliku, na kojoj se nalazi sa oružjem u ruci.

Kada je policija došla na lice mesta, mladić se u svom stanu zatvorio i pojavljivao se povremeno na prozoru sa oružjem. Policiji je pretio putem poziva za hitne intervencije da će zgradu dići u vazduh, ukoliko se ne razidu. Više od sat vremena je trajalo ubeđivanje sa policijom i mladić je na kraju uhapšen. Pištolj koji je on koristio bio je lažan, a uz sve to bio je i pod uticajem droge. Protiv mladića je pokrenut krivični postupak zbog remećenja javnog reda i mira i pretnji ubistvom.⁴⁰⁹

409 *Facebook-Morddrohung löst Polizeieinsatz aus*, apa/dpa, <http://futurezone.at/digitallife/11221-facebook-morddrohung-loest-polizeieinsatz-aus.php>, 22. 8. 2013.

6. FEJSBUK I NEUTRALNOST INTERNET MREŽE

6.1. Ljudska prava

Temelji demokratskog društva postavljeni su na dve premise slobodi i jednakosti. Treba imati u vidu da se sloboda od sedamnaestog veka meri slobodom pojedinca. U ovom kontekstu sloboda prestaje tamo gde počinje sfera javne, državne vlasti. Upravo su neki autori to objasnili na sledeći način „Tamo gde svako neposredno učestvuje u procesu donošenja kolektivnih odluka, pojedinac biva podređen autoritetu celine i gubi svoju slobodu kao privatna osoba, a upravo je privatna sloboda ono što građanin zahteva od javne vlasti“.⁴¹⁰

Jednakost se vezuje pre svega za jednakost šansi, dok se jednakost u skladu sa liberalističkim učenjem poistovećuje sa jednakošću u slobodi. To znači da svako može uživati onoliko slobode koliko je to spojivo sa slobodom drugih i može činiti šta mu je volja, sve dotle dok to ne ugrožava slobodu drugih. Ove garancije su zajemčene u modernim ustavima. Tako da su od osamnaestog veka svi moderni ustavi sadržali spisak ljudskih prava. U tom pogledu su se najpre razvila tzv. negativna prava (npr. prava na život, kretanje, privatnost, svojinu, sloboda savesti, govora, veroispovesti, štampe itd.), koja su jamčila slobodu pojedinca od državne vlasti. Potom je došlo do kategorije tzv. aktivnih prava (npr. pravo na socijalnu i zdravstvenu zaštitu i osiguranje, pravo na ograničeni radni dan i sedmicu, pravo na štrajk, pravo na rad, pravo na jednaku naknadu za rad i na naknadu u slučaju nezaposlenosti, pravo na obrazovanje) i obaveze države da aktivno učestvuje i brani slobodu pojedinca. Sa razvitkom svesti o zaštiti životne okoline i ovo pravo postaje važan element u katalogu pobrojanih prava.⁴¹¹

Upravo svest je možda i ključna reč, koja se povezuje i sa pojmom neutralnosti internet mreže i značajem interneta u digitalnom svetu. Ljudi mogu uživati sopstvena prava i slobode samo onda ako znaju da im ona pripadaju, ako su kadri da prepoznaju kada su im prava ugrožena ili uskraćena i najzad, ako su spremni da se pravnim putem bore za zaštitu sopstvenih prava. Sveopštu slobodu čoveka ponajviše ugrožava odsustvo spremnosti da se ustane u odbranu vlastitog prava.⁴¹²

410 Miodrag A. Jovanović, *Temelji demokratije*, Pravni fakultet u Beogradu, strana 3, <https://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCkQFjAA&url=https://www.ius.bg.ac.rs%2Fprof%2FMaterijali%2Fjovmio%2Fpredavanja%25202012%2FTemelji%2520demokratije.doc&ei=40JRUq6UJIrm4wTOYHAAw&usq=AFQjCNENPjPp0IpcxvVMwFHK3aTkUlnDKA>, 6. 10. 2013.

411 Ibidem, str. 2, 3, 4, 7 i 8.

412 Rudolf Jering u svom čuvenom delu *Borba za pravo* kaže: „Pokaže li se pojedinčevo pravno osećanje slabim, gnjilim, klonulim, i ne uzmogne li pojedinac da savlada prepreke koje mu na put stavljaju nepravični zakoni i rdave ustanove, bez čega ne može da se slobodno i snažno razvije; počnu li da ga gone, umesto da ga brane i potpomažu; navikne li pojedinac da zbog toga trpi nepravdu i da je smatra nečim što ne može da se izmeni — ko će onda još i da

Neutralnost internet mreže gledano sa pravnog stanovišta postavlja mnogo pitanja tzv. predhodnih pitanja, da bi se dao nedvosmislen odgovor na pitanje samog pojma, ali i značaja na globalnom planu. Zbog preširokog određivanja ovog pojma i značenja na globalnom planu, pokušaćemo da objasnimo pravne aspekte ovog problema u kontekstu sa Fejsbukom.

Potrebno je uočiti 5 aspekata:

1. *Internet kao globalna mreža* je napravljena tako da se na njemu mogu slobodno širiti i primati informacije. On je i više od toga, baza u kojoj se nalazi pregršt informacija i koja omogućava komunikaciju između ljudi, daje nam moć da izrazimo svoje mišljenje, da stvaramo, da učimo i delimo informacije. Danas je više od dve milijarde ljudi onlajn, što čini skoro trećinu planete. Osim toga internet je i pokretačka snaga ekonomije u 21. veku, pre svega zbog poslova koji se sklapaju putem ove mreže. Metaforično bi se internet mogao definisati i kao most koji spaja komunikaciju između ljudi.

Mnogi prilikom definisanja neutralnosti internet mreže ukazuju na to da internet treba da bude otvoren, slobodan i bez diskriminacije. To znači da bi korisnici trebalo da imaju *identičnu brzinu protoka podataka* bilo da šalju mejl, gledaju Jutjub video ili pričaju preko Skajpa. Upotreba bržeg i sporijeg protoka podataka, bi shodno ovom principu bila nedozvoljena.

Jedna od najvažnijih karakteristika današnjeg interneta, je to da je internet odlična platforma za inovacije. Danas svako od nas može da kreira, objavi novi servis ili novi sadržaj na internetu, bez prethodnog odobrenja ili testiranja i za to je samo neophodan pristup internetu. Neutralnost internet mreže je takođe jedan od instrumenata fer tržišne utakmice, kojim se garantuje malim i srednjim preduzećima od starta jednakost šansi u svom prodoru na tržište.⁴¹³ Ovim principom se omogućava i osigurava da i inovatori mogu da počnu od malog i da sanjaju o tome da postanu u budućnosti novi Fejsbuk ili Gugl, a da ne budu već u startu onemogućeni u tome i da njihove ideje i inovacije budu blokirane. Ukoliko internet mreža ne bi bila neutralna, početnici bi bili potisnuti sa tržišta od strane velikih kompanija, koje bi plaćale za svoje vodeće mesto na internetu. Između ostalog važno je uspostaviti ravnotežu između otvorenosti i neutralnost internet mreže, na jednoj strani, i na drugoj strani slobode u pogledu dizajna inovacija u najširem smislu.⁴¹⁴

Pobornici ideje o neutralnosti internet mreže ističu i da bi ukidanje neutralnosti internet mreže značilo pored nejednakosti u sadržini / transportu podataka i nejednakost ljudi.

pomisli da tako ugušeno, pritisnuto, slomljeno pravno osećanje, može da plane živim osećajem i energičnim otporom tamo gde pravna povreda nije nanosena jednoj individui, već celom narodu? Ko nije naviknut da muški brani svoje rođeno pravo, kako će moći oduševljeno da se žrtvuje za pravo celine?". Miodrag A. Jovanović, *Temelji demokratije*, Pravni fakultet u Beogradu, Strana 17, <https://www.google.at/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCkQFjAA&url=http%3A%2F%2Fwww.ius.bg.ac.rs%2Fprof%2FMaterijali%2Fjovmio%2Fpredavanja%25202012%2FTemelji%2520demokratije.doc&ei=40JRUq6UJlrm4wTORyHA Aw&usq=AFQjCNENPjPp0IpcxvVMwFHk3aTkUlnDKA>, 6. 10. 2013.

413 Barbara Wimmer, Aktivisten fordern Gesetz für Netzneutralität, futurezone.at, <http://futurezone.at/netzpolitik/aktivisten-fordern-gesetz-fuer-netzneutralitaet/24.586.035>, 24. 10. 2013.

414 Dragan Prlja, Andrej Diligenski, *Pravni aspekti neutralnosti internet mreže*, Strani pravni život, br. 3, 2011, Institut za uporedno pravo, Beograd, <http://www.comparativelaw.info/spz> 20113.pdf, strana 127.

Protivnici ideje o neutralnosti internet mreže smatraju da uvođenje klasnog interneta zapravo odgovara stanju u društvu, te da su i pojedinci u državama podjeljeni po klasama.

2. Da bi se internet mreža koristila i bila na nivou optimalnom za korišćenje, potrebno je konstantno investirati u opremu i kapacitete internet mreže. Te troškove snose *internet servis provajderi (ISP)* koji korisnicima nude infrastrukturu, odnosno mogućnost komunikacije između korisnika.⁴¹⁵ U tom pogledu postoji ogromna mogućnost zloupotrebe odnosno kontrole transfera podataka, brzine transfera podataka od strane internet provajdera.⁴¹⁶ Oni mogu odlučivati, pošto poseduju infrastrukturu, ko će je koristiti, a ko ne i tu postoji glavna opasnost po neutralnost internet mreže.⁴¹⁷ Pošto se internet saobraćaj poslednjih godina drastično uvećao, internet provajderi su u mogućnosti da kreiraju brze i spore protoke podataka. Ko može da plati brzi protok podataka, moći će da koristi sve mogućnosti interneta, dok ostali koji nemaju materijalnih mogućnosti to neće moći sebi da priušte.⁴¹⁸ Pozadina toga svega je dogovor internet provajdera sa velikim kompanijama na tržištu, koje bi internet provajderima plaćale nadokadu za prioriteto mesto na tržištu.⁴¹⁹

Ukoliko bi se uzeo za primer korišćenje Skajpa za telefoniranje, tada bismo mogli da govorimo o povredi principa neutralnosti internet mreže, ako bi telefoni-

415 Dobar primer za ovo je snabdevanje električnom energijom. Niko se ne pita da li je za priključak struje, koji korisnici imaju u domaćinstvu, korišćen sony ili samsung televizor, već da li je omogućeno snabdevanje strujom. Kao pandan ovom primeru treba i internet da bude slobodan, otvoren za sve.

416 Postoji mišljenje stručnjaka da stanje na tržištu nekih zemalja i nije toliko alarmantno. Konkurencija i razvijeno tržište telekomunikacija dovode to toga da se mogućnosti ISP u pogledu kontrole sadržaja i pristupa internetu smanjuju kao i da se automatski uklanjaju. Stefan Krempel, *Bundesnetzagentur: Probleme mit der Netzneutralität „nicht alarmierend“*, heise.de, <http://www.heise.de/newsticker/meldung/Bundesnetzagentur-Probleme-mit-der-Netzneutralitaet-nicht-alarmierend-1743842.html>, 27. 10. 2013.

417 Barbara Wimmer, *Aktivisten fordern Gesetz für Netzneutralität*, futurezone.at, <http://futurezone.at/netzpolitik/aktivisten-fordern-gesetz-fuer-netzneutralitaet/24.586.035>, 24. 10. 2013.

418 Nova iskušenja za neutralnost internet mreže ogledaju se i u investicije ISP u razvoj mreže. Pre svega se ističu da neutralnost internet mreže uništavaju i zahtevi tržišta, kao npr. video on demand. Da bi se dobila HD video slika, neophodno je konstantno pratiti tehnološki razvoj na tržištu. Ovaj razvoj omogućuju nove LTE tehnologije i prenos podataka brzinom svetlosti putem staklenih vlakna. Telekom provajderi koji žele da naprave ovakvu strukturu mreže moraju u ovakve projekte da investiraju milijarde. Poređenja radi trenutno je na nivou EU prosečna brzina protoka interneta oko 50 megabita u sekundi. U Nemačkoj postoje Backbone mreže, koje poseduju brzinu protoka od 400 gigabita u sekundi, a prenosom podataka brzinom svetlosti putem staklenih vlakna, brzina interneta će biti izražena u terabitima u sekundi. To znači da određene usluge, korisnici interneta neće moći da koriste, koje zahtevaju ovako naprednu tehnologiju ili da će protok usluga u najmanju ruku biti usporen. ISP stoga neće prodavati samo pristup internetu, nego i internet sa prioritentnim uslugama u ovom slučaju sa video sadržajem (video streaming), čiji će protok biti izuzetno brz. Stefan Krempel, *Breitband killt Netzneutralität*, heise.de, <http://www.heise.de/newsticker/meldung/Breitband-killt-Netzneutralitaet-1705805.html>, 27.10.2013. Barbara Wimmer, *Aktivisten fordern Gesetz für Netzneutralität*, futurezone.at, <http://futurezone.at/netzpolitik/aktivisten-fordern-gesetz-fuer-netzneutralitaet/24.586.035>, 27. 10. 2013.

419 Nicolas Fennen, „*The Internet Must Go*“: *Weshalb die Abschaffung der Netzneutralität keine gute Idee ist*, Netzpolitik.org, <https://netzpolitik.org/2013/the-internet-must-go-warum-die-abschaffung-der-netzneutralitaet-keine-gute-idee-ist/>, 13. 9. 2013.

ranje bilo onemogućeno ili na bilo koji način blokirano uz zahtev da se naknadom može ubrzati protok i bolji kvalitet veze. Može se zaključiti da su cenzura sadržaja i blokada transfera podataka od suštinskog značaja da bi internet mreža ostala neutralna.

3. *Država* se postavlja kao regulator svih ovih odnosa i ona je ta, koja bi trebalo da omogući fer utakmicu na tržištu. Osim toga država se postavlja bar u evropskim pravnim sistemima kao garant ljudskih prava, a pre svega prava privatnosti i tajnosti elektronske komunikacije. Države mogu lako da prate kretanje mobilnih telefona, identifikuju sve osobe sa mobilnim telefonima u određenoj oblasti i presreću pozive i tekstualne poruke. Takođe su u mogućnosti da krše osnovna ljudska prava i putem pristupa sačuvanom sadržaju e-mejllova i poruka pojedinaca, koje mogu dobiti od internet servis provajdera. Uz pomoć postavljanja dodataka na optičke kablove, preko kojih se obavlja protok digitalnih informacija, i primenom tehnike prepoznavanja reči, glasa i govora, države mogu ostvariti skoro potpunu kontrolu nad telekomunikacijama i internet saobraćajem.⁴²⁰ Sofisticiranim metodama i naglim tehnološkim razvojem došlo je do naglog povećanja opasnosti od digitalnog nadzora i cenzure sadržaja na internetu.

Pored ovoga u ovom kontekstu države moraju obratiti pažnju na *pravo privatnosti pojedinaca*. Ako se naredi internet provajderima da nadziru npr. celokupan protok informacija na Fejsbuku, dolazi do mešanja države u pravo pojedinaca na privatnost i mešanje države u privatni sektor uopšte. Opravdanost nadziranja komunikacija odnosno ugrožavanja prava privatnosti pojedinaca je dozvoljen samo ako postoji pretežniji interes države ili pojedinaca. Opravdanje se naravno odnosi i kreće uvek u pravcu bezbednosti države i pojedinaca. Na nivou EU je ova mogućnost već bila zakonski regulisana donošenjem Direktive o zadržavanju podataka. I dalje je moguće da neke države članice EU, koje su usvojile slične zakone kao npr. Nemačka prikupljene podatke na ovakav način iskoriste. Za to je potrebno da postoji određeno zakonom propisano krivično delo. Neke države članice EU dakle nadziru celokupan mobilni, telefonski i internet saobraćaj, zbog mogućeg izvršenja teških krivičnih dela i veće bezbednosti građana. U ovom kontekstu treba naglasiti reč mogućeg izvršenja teških krivičnih dela, jer to znači da smo svi mi potencijalni teroristi. Povod za ovakvu vrstu pravne regulative zvanično nije bio Fejsbuk, nego teroristički napadi u Njujorku, Londonu i Madridu, koji su inicirali donošenjem Direktive o zadržavanju podataka. Veliki broj država se opredelio za nadzor interneta a pre svega društvenih mreža kao i trajno ili privremeno blokiranje pristupa društvenim mrežama.

Ipak treba imati u vidu da se ovom prilikom pored privatnosti radi i o eroziji demokratskog društva u celini i osnovnih principa na kojima je ovo društvo zasnovano. To se pre svega odnosi na slobodu medija, slobodu mišljenja i izražavanja, tajnost pisama i komunikacije i konačno pretpostavku nevinosti.⁴²¹ Upravo

420 *State communication surveillance undermines freedom of expression, warns UN expert*, United Nations Human Rights, Office of the High Commissioner for Human Rights, <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13400&LangID=E%20>, 30. 9. 2013.

421 *Stellungnahme der AntragstellerInnen des Ausgangsverfahrens im Vorabentscheidungsverfahren gemäß Artikel 267 AEUV*, Scheucher Rechtsanwalt GmbH, Gerichtshof der Europäischen Union, Luxemburg, 29. 3. 2013, strana 5.

predpostavka nevinosti je prekršena kod nadzora elektronskih komunikacija odnosno špijuniranja, pošto se radi o osnovnoj zaštitnoj poziciji svakog građanina pred državom, da se prilikom osnovane sumnje za postojanje krivičnog dela, može sprovesti istraga protiv određenog lica. Ukoliko su svi građani špijunirani ili nadzirani, dolazimo do toga da su svi potencijalni teroristi, što se fundamentalno kosi sa ovim principom. Preneseno na tajnost komunikacije i pisma to bi značilo da bi ubuduće trebalo ispitati i dokumentovati svako pismo ili pošiljka, koje bi možda sadržale u sebi relevantne informacije koje bi opravdale špijuniranje. Pored toga narušava se i princip jednakosti, pošto su svi osumnjičeni, jer se građani koji su nevinu poistovećuju sa učiniocima krivičnih dela.⁴²²

4. *Pojedinci* su naredni važan element ovog odnosa, kojima država teba da omogući slobodno širenje i primanje informacija. Ovo pravo je garantovano pojedincima u vidu *prava na slobodno mišljenje i izražavanje*, a koje spada u jedno od temeljnih ljudskih prava i sloboda. Ono je regulisano članom 10 Evropske konvencije o zaštiti ljudskih prava kao i članom 11 Povelje o osnovnim ljudskim pravima EU. Međutim ono je zasnovano i na tome, što pojedinci ulažu takođe svojim novcem kroz plate i poreze u infrastrukturu mreže.⁴²³ Stoga su države dužne da transparentno obaveštavaju građane, šta se dešava sa njihovim novcem u ovom smislu.

Ukoliko bi ISP prekršili neutralnost internet mreže i blokirali izvesne internet servise, bila bi to u osnovi povreda prava na slobodu mišljenja i izražavanja. Tu naime ne bi postojao slobodan pristup mreži. Kada je reč o internet sadržaju usporavanje ili davanje prednosti određenim podacima ili paketima, diskutabilno je, da li postoji tada povreda prava na slobodu mišljenja i izražavanja. Ukoliko bi se radilo o brzini protoka podataka, a ne o generalno pristupu mreži, to bi bilo dopušteno ugovoriti. Pošto nije ugrožen sam pristup internet mreži. Sa druge strane davanje prednosti određenim podacima u internet saobraćaju bi takođe predstavljalo povredu ovog osnovnog ljudskog prava, pošto se radi direktno o samom pristupu internet mreži. Sve ove garancije se odnose na garanciju država pojedincima. Privatni sektor nije ovim obuhvaćen i ostavljeno mu je da svoje odnose sa pojedincima reguliše putem ugovornog prava.⁴²⁴

Pošto je segment ljudskih prava u ovom pogledu regulisan, a privatni sektor između internet provajdera i korisnika još uvek nije regulisan (ostavljen ugovornom regulisanju), postavlja se pitanje, da li neutralnost internet mreže treba regulisati zakonski ili ga ostaviti bez regulacije? Države ovu garanciju mogu ispuniti samo na teritoriji matične države i u tome su mogućnost i potreba regulacije ove oblasti limitirane, pošto je internet globalna mreža, pa se postavlja i pitanje svrhe regulacije u tom kontekstu.⁴²⁵

422 Ibidem, str. 7, 8, 9.

423 Tako je u Austriji izdvajanje na godišnjem nivou 30 milijardi evra, koje građani uplaćuju iz svojih plata. Barbara Wimmer, *Aktivisten fordern Gesetz für Netzneutralität*, futurezone.at, <http://futurezone.at/netzpolitik/aktivisten-fordern-gesetz-fuer-netzneutralitaet/24.586.035>, 27. 10. 2013.

424 Dragan Prlja, Andrej Diligenski, *Pravni aspekti neutralnosti internet mreže*, Strani pravni život, br. 3, 2011, Institut za uporedno pravo, Beograd, <http://www.comparativelaw.info/spz> 20113. pdf, str. 132, 6. 10. 2013.

425 Tako imamo primer predloga da se internet saobraćaj u EU reguliše kao šengenski prostor. Na taj način bi se po pobornicima ovog predloga zaštitili evropski građani pre svega od špijuniranja,

Ukoliko je regulacija ograničena i ako uzmemo za primer Nemačku, ona je u stanju da reguliše celokupan internet sadržaj u Nemačkoj i u slučaju potrebe države nadzire komunikaciju npr. na Fejsbuku. Ovakav nadzor komunikacije moguć je samo u pogledu protoka informacija koje nemački internet provajderi mogu da presretnu. Na taj način nije moguće uticati na Fejsbuk pa se kao jedino rešenje javlja mogućnost otvaranja predstavništva u Nemačkoj i tako se pravnim vezivanjem za određenu teritoriju omogućava kontrola Fejsbuka u ovom pogledu. Koliko je to pravno ostvarivo, videli smo u sudskim odlukama i praksi.

Treba imati u vidu da je uopšte uzev regulisanje neutralnosti internet mreže potpuno izlišno, pošto je pristup mreži i blokiranje sadržaja informacija kao osnovno ljudsko pravo u ovom pogledu već regulisano ustavima kao deo prava na primanje informacije u okviru prava na slobodu mišljenja i izražavanja. Ipak i pored toga neke zemlje su već regulisale ovu oblast zakonima (Slovenija, Holandija), a neke to planiraju uredbama kao npr. Nemačka.

U nacrtu nemačke uredbe neutralnost internet mreže je garantovana na sledeći način:

- a) U otvorenom, odnosno slobodnom internetu podaci se prenose, tako da svi paketi podataka imaju jednak tretman, nezavisno od sadržaja, usluge, aplikacije, porekla ili cilja prenosa i kojima treba omogućiti korišćenje svih usluga, sadržaja i aplikacija putem interneta.
- b) Pristup otvorenom internetu i njegovim sadržajima, uslugama i aplikacijama kao i odvojenim mrežama, koji se korisnicima posebno šalju u ponudama uz naknadu, treba da bude za sve korisnike i internet provajdere bez diskriminacije, transparentan i javan.
- c) Klase prenosa podataka u otvorenom internetu kao i pristup otvorenom internetu opisan u tački b) ne smeju onemogućiti osnovni princip regulisan pod tačkom a).⁴²⁶

Ovako opisana garancija neutralnosti internet mreže već na prvi pogled ostavlja puno mogućnosti pre svega internet provajderima za slobodno tumačenje i manipulaciju. Ukoliko internet provajderi javno i transparentno kažu korisnicima da će za pristupanje određenom sadržaju biti neophodno da uplate dalje pakete i za to traže naknadu (što proizlazi iz tačke b), oni time zapravo u osnovi krše temeljni princip nediskriminacije i neutralnosti internet mreže postavljen u tački a).

U Velikoj Britaniji je od strane apelacionog suda potvrđeno da je pristup internetu jedna vrsta ljudskog prava. Danas je nerazumno, da se nekom zabrani pristup internetu od kuće, ustanovio je sud.

pošto bi se moglo kontrolisati ko ulazi u evropski internet saobraćaj. Međutim šengenski sporazum je postavljen na drugačijim temeljima (odbrana od krijumčarenja, lažnih alizanata, trgovine drogom itd.) i kosi se sa principom neutralnosti internet mreže, ukoliko bi se primenio. Inače ovaj predlog je prvi put potekao još 2010 godine u okviru Protokola radne grupe EU za gonjenje učinioca krivičnih dela. *Wieder da: Der Vergleich des Internet mit dem Schengener Abkommen*, Netzpolitik.org, Matthias Monroy, <https://netzpolitik.org/2013/wieder-da-der-vergleich-des-internet-mit-dem-schengener-abkommen/>, 21. 9. 2013.

426 Markus Beckedahl, *Der aktuelle Stand der Netzneutralität auf Bundes- und EU-Ebene*, Netzpolitik.org, <https://netzpolitik.org/2013/der-aktuelle-stand-der-netzneutralitaet-auf-bundes-und-eu-ebene/>, 12. 9. 2013.

Povod za ovu odluku je bila presuda protiv jednog voajera, koji je osuđen jer je fotografisao pomoću mobilnog telefona 14-godišnju devojčicu dok se tuširala. Telefon je ubacio u flašicu od šampona, ali se igrom slučaja prilikom fotografisanja uključio blic, pa je devojčica uspela da otkrije telefon. Ubrzo nakon toga policija je pretresla stan osuđenog i pronašla u njegovom kompjuteru na stotine slika dečije pornografije. Ovaj čovek je osuđen na 3 godine društveno korisnog rada, a pritom je uz kaznu trebalo da bude podvrgnut i programu prevencije za izvršenje seksualnih delikata. Na osnovu tog programa je njemu bilo zabranjeno da poseduje kompjuter, da koristi kameru u javnosti i da u svom poslu ima kontakt sa decom. Policiji je dato pravo da u bilo koje vreme pretraži njegov stan. Ova zabrana je trebala da važi tokom čitavog njegovog života.

Osuđeni je uložio žalbu, pošto je smatrao da bi on ovom sudskom odlukom bio odsečen od ostatka sveta. Sudija u žalbenom postupku je uvažio njegovu žalbu i istakao da je u osudi u prvostepenom postupku preterana želja sudija da ovakva vrsta kazne važi za ceo život. Osim toga istaknuto je da se nikome od kuće ne može zabraniti pristup internetu. Njegova kazna je preinačena i policiji dato pravo da svakog trenutka može imati uvid u surfovanje na internetu osuđenog. Ova presuda može imati uticaja i na buduće presude prema hakerima i sajber kriminalcima, prema kojima se najčešće određuju privremene mere zabrane korišćenja interneta.⁴²⁷

5. *Fejsbuk* se u ovom kontekstu javlja kao platforma, odnosno posrednik ili bolje rečeno regulator koji omogućava olakšano i ubrzano primanje i slanje informacija na internet mreži i komunikaciju između pojedinaca (korisnika). Sa svojih preko dve milijarde korisnika, predstavlja jedan od bitnijih faktora na tržištu za zagušenje interneta i povećanje investicija internet servis provajdera u infrastrukturu internet mreže. Pre svega kada se ima u vidu koliko se dnevno putem ove društvene mreže objavi tzv. postova (video i muzičkih klipova, slika itd.), što nesumnjivo guši internet saobraćaj i zahteva konstantno ulaganje u kapacitete internet mreže. Sa druge strane postoji potreba korisnika za brzom i nesmetanom razmenom informacija i podataka. Stoga i ne čudi zalaganje Fejsbuka za princip neutralnosti internet mreže.

Kao što je već napomenuto *Fejsbuk ima attribute državnosti*. Ono što Fejsbuku nedostaje je potpuna infrastruktura, a to je internet mreža. Za razliku od država poseduje servere na osnovu kojih je u jačoj poziciji od država, pošto se postavlja kao neprikosnoveni arbitar da li će nešto biti objavljeno ili ne. Na tim serverima ima više informacija od bilo koje tajne službe. Državama kao jedino sredstvo zaštite od Fejsbuka ostaju internet provajderi, koji spadaju, u većini evropskih zemalja, u privatni sektor (ali se finansiraju iz državnog budžeta takođe) i koji bi jedini bili u mogućnosti da kontrolišu, koji se podaci putem ove društvene mreže razmenjuju. Treba imati u vidu, da je regulacija te oblasti trenutno moguća samo po teritorijalnom principu, kao što je već objašnjeno.⁴²⁸

Sam Fejsbuk je takođe pribegao merama nadzora sadržaja sopstvenih korisnika, pa je tako aktivirao servise za pronalaženje samoubica, organizatore trgovine

427 Florian Rötzer, *Internet als Menschenrecht: Kein Verbot in UK für Internetzugang*, heise.de, <http://www.heise.de/newsticker/meldung/Internet-als-Menschenrecht-Kein-Verbot-in-UK-fuer-Internetzugang-1749442.html>, 27. 10. 2013.

428 Zanimljivo je da primer Fejsbuka i otvaranja predstavništva u Irskoj sledio i Jahu, koji je svoju filijalu preselio iz Švajcarske u Dablin. *Jabu odlazi iz Švajcarske*, Tanjug, Blic.rs, <http://www.blic.rs/IT/402167/Jahu-odlazi-iz-Svajcarske>, 29. 9. 2013.

ljudima kao i sprečavanje pedofilije. Kontrolu poruka korisnika Fejsbuka potvrdio je i Džo Salivan, zadužen za održavanje bezbednosti ove društvene mreže, koji je istakao: „da je pretraga za sumnjivim porukama usmerena samo i isključivo na određene vrste slučajeva, da bi se, pre svega sprečile sve češće akcije pedofila i organizacija koje se bave zloupotrebom ljudi“.⁴²⁹ Osim ove aktivnosti ova platforma je priznala da nadzire i korespondenciju preko četa.⁴³⁰ Veliko je pitanje, da li se u ovoj prevelikoj brizi Fejsbuk zadržava isključivo na pomenutom sadržaju. Način na koji to ova društvena mreža sprovodi, nije objavljen. Svakako je jasno, da ako je Fejsbuk u stanju da sve ove aktivnosti korisnika filtrira, logično se postavlja kao pitanje, šta Fejsbuk ne može da proceni i otkrije?!⁴³¹

Još više zabrinjava činjenica da su čelnici Fejsbuka priznali da se sve vrste komunikacija putem ove društvene mreže strogo nadziru i prate. Prati se svaka vrsta komunikacije preko statusa, priče, četa uz pomoć automatizovanih softvera, na osnovu kojih je moguće utvrditi i značenje fraza u nekom jeziku. Uvid u ovu vrstu podataka Fejsbuk omogućava i tajnim službama SAD. Naročito sumnjive razgovore odnosno komunikaciju Fejsbuk prosleđuje tajnim službama, koje ove navode proveravaju. Ovi podaci se šalju na osnovu „ugrožene sigurnosti“.

Na primeru Srbije ispostavilo se da podatke koje MUP želi da pribavi od Fejsbuka, mora predhodno da zatraži na osnovu zahteva i to putem međunarodne pravne pomoći. Ukoliko Fejsbuk iz Amerike izda odobrenje, moguće je pristupiti podacima korisnika.⁴³² Ipak postoje i druge indicije na osnovu kojih MUP može slobodno pristupiti podacima bilo kog korisnika u Srbiji. Na osnovu Zakona o elektronskim komunikacijama, omogućeno je praćenje komunikacije na osnovu sudske odluke. Iako se, kao i u slučaju Fejsbuka u SAD, podaci korisnika mogu uzimati samo kada postoji ugrožena bezbednost, odnosno konkretna pretnja po sigurnost i bezbednost države i građana, stiče se utisak da su mogućnosti zloupotrebe otvorene. Upravo pitanje koga to još policija i tajne službe mogu da kontrolišu i prate predstavlja misteriju u ovom pravu države na očuvanje javnog poredka.⁴³³

Fejsbuk je zaključio sporazum sa vladom Pakistana, na osnovu koga je dužan da blokira, ukloni neželjene sadržaje, na koje im ukaže pakistanska vlada. Treba imati u vidu da ova platforma u jednom periodu uopšte nije bila dostupna u ovoj državi, pre svega zbog prikazivanja bogohulnih karikatura proroka Muhameda.⁴³⁴

429 *Facebook sprečava akcije pedofila*, MONDO — agencije, <http://www.mondo.rs/a252910/Mob-IT/Vesti/Facebook-sprecava-akcije-pedofila.html>, 6.10.2013.

430 *Facebook verstößt gegen heimisches Gesetz*, oe24.at, <http://www.oe24.at/digital/Facebook-verstoess-gegen-heimisches-Gesetz/73393089>, 6. 10. 2013.

431 *Facebook sprečava akcije pedofila*, mondo.rs, <http://www.mondo.rs/a252910/Mob-IT/Vesti/Facebook-sprecava-akcije-pedofila.html>, 21. 10. 2013.

432 *Veliki Brat ne spava, Svaka reč na Fejsbuku se snima!*, D. Tadić, sajt Kurira, <http://www.kurir-info.rs/svaka-rec-na-fejsbuku-se-snima-clanak-319901>, 2. 8. 2012.

433 *Veliki Brat u Srbiji: Fejsbuk daje policiji naše privatne informacije!*, 16. 4. 2012. godine (preuzeto sa: www.telegraf.rs), <http://www.sigurnodijete.ba/index.php/bs/bezlinka/aktuelne-vijesti/311-veliki-brat-u-srbiji-fejsbuk-daje-policiji-nashe-privatne-informacije>, 2. 8. 2012.

434 Jan-Peter Kleinhans, *Facebook zensiert Inhalte in Pakistan*, netzpolitik.org, <https://netzpolitik.org/2013/facebook-zensiert-inhalte-in-pakistan-aber-ist-mitglied-der-global-network-initiative/>, 27. 10. 2013.

6.2. Edvard Snouden i afera „PRIZMA“

Proseđivanjem podatka američkog obaveštajca Edvarda Snouodena, koje je „Vašington post“ objavio početkom juna 2013. godine, ustanovljeno je da je američka Nacionalna agencija za bezbednost (NSA) šest godina sprovodi program „PRIZMA“, kojim su praćeni svi podaci i komunikacije miliona ljudi na društvenim internet mrežama. Vlada SAD je preko servera velikih internet kompanija imala potpuni pristup ogromnoj količini podataka i mogućnost praćenja stotine miliona ljudi na internetu u celom svetu, i to sve u realnom vremenu. Tako je Majkrosoft prosleđivao NSA službi sve što on nudi na internetu od 2007. godine, Jahu i AOL od 2008., Gugl i Fejsbuk od 2009., Jutjub od 2010., i Epl od 2013. godine. Poražavajuće je saznanje da je celokupna korespondencija u Gugl mejlu, poruke razmenjene na Fesjbuku, objave na Tviteru, bila dostupna sveznajućem „velikom bratu“ u SAD.

„Vašington post“ između ostalog piše i o tome da je program „PRIZMA“ odobrio američki federalni sud, i da su bili upoznati članovi Komiteta za obaveštajne poslove Kongresa, koji su bili obavezani čuvanjem državne tajne.

Da je ono što je „Vašington post“ objavio tačno, potvrdio je Džejms Klaper (James Clapper) direktor Nacionalne obaveštajne službe. Pored toga je istaknuto da „Obelodanjivanje dokumenta koji nosi oznaku najveće tajnosti preti da dovede do dugotrajnih i neotklonjivih posledica za identifikaciju i odgovor na mnogobrojne pretnje sa kojima se američka nacija suočava“.⁴³⁵

Portparol Bele kuće Džoš Erners je u svom obraćanju novinarima istakao da je nadgledanje „odlučujuće oruđe u zaštiti nacije od terorističkih pretnji“ i da „omogućava službama da otkriju da li su neke osobe u SAD uključene u terorističke aktivnosti sa ljudima koji se nalaze van Amerike“.⁴³⁶

„Vol Strit džornal“ je objavio da je NSA preko programa „PRIZMA“ pratila i sve transakcije ostvarene putem kreditnih kartica. Svoje nezadovoljstvo programom američke vlade izneli su brojni aktivisti za ljudska prava i nevladine organizacije, koje su bile šokirane saznanjem za postojanje ovakvog programa. „Potvrđeni su naši najgori strahovi. Ako država može da prati koga mi zovemo, naše pravo na privatnost nije samo ugroženo, ono više ne postoji“, rekao je advokat američke Unije za građanske slobode Aleksander Abdo.⁴³⁷

Pobornici ovakvih metoda nadzora elektronskih komunikacija ističu da su u pitanju tzv. metapodaci, koji u suštini ništa ne govore. Otkrivanje detalja o telefonskim pozivima, bez ulaženja u sadržinu komunikacije, ne treba da predstavlja razloge za zabrinutost građana. Tako je i već pomenuti direktor Nacionalne obaveštajne službe Džejms Klaper istakao da: „program „PRIZMA“ ne dozvoljava vladi da prisluškuje telefonske razgovore. Informacije koje se dobijaju ne uključuju sadržaj bilo kojih komunikacija ili identitet pretplatnika“.⁴³⁸

435 *Kontrola društvenih mreža, novi skandal za Obamu*, Tanjug, portal Zaštita podataka o ličnosti, <http://partners-serbia.org/privatnost/aktuelno/2402/>, 30. 9. 2013.

436 *Ibidem*.

437 *Ibidem*.

438 Kurt Opsahl, *Why Metadata Matters*, Electronic Frontier Foundation, <https://www EFF.org/deeplinks/2013/06/why-metadata-matters>, 29. 11. 2017.

Priznanjem američke administracije da su prikupljeni metapodaci, postavlja se pitanje o kakvoj vrsti podataka se zapravo radi.

Metapodaci između ostalog govore o tome:

- Da li su korisnici pozvali telefonske seks usluge u 2:24 posle ponoći i pričali 18 minuta (radi se o *vremenu trajanja komunikacije* i osnovnim podacima — br telefona, adresa, ip adresa), ali nije poznato o čemu su pričali.
- Da li su korisnici pozvali telefonske linije za sprečavanje samoubistva sa mosta Golden Gejt (radi se o *lokaciji sa koje je objavljena komunikacija* i osnovnim podacima — br telefona, adresa, ip adresa), dok tema razgovora ostaje tajna.
- Da li su korisnici razgovarali sa službom za testiranje na HIV, sa lekarima i zdravstvenim osiguranjem (radi se o *ustanovama, koje su pozivane i osnovnim podacima* — br telefona, adresa, IP-adresa), ali nije poznato o čemu su razgovarali.
- Da li su korisnici razgovarali sa ginekologom, razgovarali pola sata, a kasnije tog dana pozvali lokalni broj službe za planiranje roditeljstva (ustanove koje su pozivane i vreme i osnovni podacima — br telefona, adresa, IP-adresa). Takođe nije poznato šta su razgovarali.

Ipak se iz prikazanog može zaključiti podaci o telefonskim pozivima građana tzv. metapodaci mogu da otkriju mnogo više o sadržaju poziva od onoga što američka vlada tvrdi. Metapodaci omogućavaju da se saznaju najintimniji detalji iz života građana. Osim toga ovi podaci se povezuju sa drugim informacijama — generisani od strane korisničkih smart telefona, personalnih računara i tableta. Oni mogu da otkriju vreme i trajanje komunikacije, konkretne uređaje koji se koriste, e-mail adrese ili brojeve koji su kontaktirani, ali i lokacije na kojima se korisnici nalaze. Pošto praktično svaki uređaj ima jedinstveni identifikacioni broj (ID, MAC adresu), sve vrste komunikacije i internet aktivnosti mogu biti povezane i identifikovane na relativno lak način.⁴³⁹

Digitalne tragove ostavljamo svakodnevno, a oni mogu da otkriju mnogo o pojedincu kao npr. informacije o tome gde neka osoba živi, šta radi, koje je veroispovesti, političke pripadnosti, gde putuje, šta kupuje onlajn, pa čak i u koje vreme ide na spavanje i napušta kuću. Pored toga je moguće jasno doći i do zaključaka o socijalnom životu pojedinca. Ipak, treba se zapitati šta je intimnije, slušanje razgovara telefonom, ili mogućnost da se prikažu aktivnosti i odnosi, iz dana u dan, prilično detaljno, u bilo koje vreme? Ove podatke prikupljaju i čuvaju društvene mreže između ostalih i Fejsbuk ali i na osnovu zakona telekom i internet servis provajderi, za različite vremenske periode. Razlika je samo u motivima prikljupljanja podataka od strane društvenih mreža i telekom i ISP.⁴⁴⁰

⁴³⁹ *Ibidem.*

⁴⁴⁰ Ann Cavoukian, *Metapodaci — Odvajanje činjenica od fikcije*, portal Zaštita podataka o ličnosti, <http://partners-serbia.org/privatnost/aktuelno/ann-cavoukian-metapodaci-odvajanje-cinjenica-od-fikcije/>, 1. 10. 2013.

Državama ostaje izuzetno težak zadatak da obezbede i sigurnost i privatnost pojedinaca. Sigurnost i privatnost pojedinaca se moraju sačuvati i od terorizma, ali i od tiranije. Stoga države koje prikupljaju metapodatke treba u startu da obezbede visok nivo pravnih, tehničkih i organizacionih garancija. Pristup ovim podacima treba da bude ograničen, a svrha kao suštinski element, nedvosmisleno određena. Kontrola pristupa ovim podacima treba biti dodeljena sudijama, ili nezavisnim regulatornim telima. Nekadašnji Poverenik za zaštitu podataka Savezne Republike Nemačke Peter Šar smatra da bi kontrolu podataka i tajnih službi trebalo staviti pod kontrolu parlamenta.⁴⁴¹

Na nivou EU i dalje je sporna, a npr. u Srbiji je na snazi i implementirana je u domaća zakonodavstva tzv. Data Retention Directive (2006/24/EU), na osnovu koje su ISP dužni da snimaju podatke u trajanju minimalno 6 meseci do 2 godine.⁴⁴² Podaci koji se snimaju su: imena i prezimena kao i adrese korisnika (osnovni podaci), ko je, sa kim i kada telefonirao (pristupni podaci), gde se u tom trenutku nalazio (podaci o lokaciji), i koja je IP-adresa korištena.⁴⁴³ Može se prostim poređenjem snimljenih podataka, koje snimaju države članice EU i podataka koje snima NSA utvrditi da se radi o identičnom stepenu nadzora.⁴⁴⁴

Mi želimo sigurnost rekli bi zvaničnici država. Time bi svaka vrsta iznanađenja predstavljala opasnost. Iz potreba da se sve unapred zna i kontroliše dolazimo do sveobuhvatne kontrole. Građani postaju prepoznatljivi, predvidljivi, podložni manipulaciji, postaju objekti državnih intitucija. Iz toga svega dalje proizlazi da svako od nas postaje od čoveka fajl ili algoritam. Ukoliko se neko nalazi duže nego što je uobičajeno na stanici, odmah shodno algoritmu postaje sumnjiv, ko se prebrzo kreće biva ubijen, ili ako se neko uopšte nalazi na pogrešnom mestu u pogrešno

441 BDSB: Kontrolle von Nachrichtendiensten notwendig, Das Datenschutzportal unwatched.org, http://www.unwatched.org/20131119_BDSB_Kontrolle_von_Nachrichtendiensten_notwendig, 13. 12. 2013.

442 Ovom direktivom nije predviđeno da se nadziru komunikacije u svrhu zaštite autorskih prava, već se nadzor elektronskih komunikacija vrši isključivo kao prevencija u odnosu tzv. teška krivična dela. Na taj način se u praksi dolazi do velikih problema, jer se prikupljeni podaci ne mogu koristiti za otkrivanje krađa autorskih dela, plagijata i gonjenje učinioca ovih krivičnih dela. Poseban problem je i taj što autori moraju na ovakve prestupe delovati po privatnoj tužbi, a korišćenje ogromne količine prikupljenih podataka eto i u ovom kontekstu ostaje potpuno besmisleno. *Parlamentarische Enquete zum Urheberrecht (Berichte 2)*, youtube.com, <http://www.youtube.com/watch?v=tvbo6DUyMKU>, 28. 10. 2013.

443 Dragan Prlja, Andrej Diligenski, *Pravni aspekti neutralnosti internet mreže*, Strani pravni život, br. 3, 2011, Institut za uporedno pravo, Beograd, <http://www.comparativelaw.info/spz> 20113. pdf, str. 135.

444 Rezultati iz austrijske prakse su pokazali na osnovu konkretnih podataka, u koju svrhu se najčešće koristili snimljeni podaci. U periodu između aprila 2012. i marta 2013. godine bilo je 326 zahteva upućenih državnom tužilaštvu Austrije. Odgovoreno je na 312 zahteva. U 161 završenih postupaka, zadržavanje podataka je trebalo u 71 slučaju da doprinese istrazi. Većina zahteva upućenih se nije odnosila na izvršenje teških krivičnih dela kao što su terorizam, ubistva, već na krađu (106 zahteva) i stalking (termin za uznemiravanje osoba). Snimljeni podaci doprineli su istrazi u 16 slučajeva krađe, 12 slučajeva vezanih za prevenciju od droge, 12 slučajeva stalkinga i 7 slučajeva prevara. Barbara Wimmer/Patrick Dax, EU-Generalanwalt: Vorratsdatenspeicherung rechtswidrig, futurezone.at, <http://futurezone.at/netzpolitik/vorratsdatenspeicherung-widerspricht-eu-recht/40.501.074>, 13. 12. 2013.

vreme.⁴⁴⁵ Ipak se ovde ne radi samo o zaštiti podataka, informacija, tajnosti komunikacije, nego i o pravu na individualnost svakog od nas.⁴⁴⁶

Pogrešni su argumenti kojim se opravdava vršenje nadzora. Pristalice nadzora ističu da ako građani nemaju šta da kriju, ne moraju da se plaše za svoju privatnost. Istina je da privatnost nije u skrivanju — ne radi se o tajnosti. Privatnost podrazumeva kontrolu — *ličnu kontrolu i slobodu izbora*. U slobodnom društvu, pojedinci moraju biti slobodni da donose informisane odluke o sopstvenom životu, uključujući i kada i u kojoj meri žele da otkriju lične detalje iz svog života!

Upravo u koncentraciji znanja i delovanjem tajnih službi ugroženi su temelji demokratskog društva. Ukoliko jedna država postane sveznajuća, povećava se mogućnost zloupotrebe ovog znanja. Ono što je sigurno je da države moraju da prihvate, da je cena slobode u jednoj izvesnoj nesigurnosti. Da li je cena masovnog špijuniranja i internet nadzora u tome, što bi se možda sprečili teroristički napadi?⁴⁴⁷ Koliko je to moguće i opravdano ukazala je i Elfride Jelenek austrijska dobitnica nobelove nagrade za književnost „Rat protiv terorizma se ne može dobiti, dok se rat protiv slobode može dobiti u izvesnoj meri“.⁴⁴⁸ U novije vreme često se terorizam i špijuniranje nazivaju bratom i sestrom.⁴⁴⁹ Izgleda da je za neke države glavna vrednost to, da postanu špijuni sopstvenih građana. U takvom odnosu treba imati u vidu da onaj ko planira savršeno špijuniranje i kontrolu građana, mora tom

445 Ovi oblici kontrole ljudi se već finansiraju od strane EU od 2009. godine i to pozamašnom svotom novca od 11 miliona evra u okviru projekta INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment). Ovim projektom treba da se detaljno razrade metode za predviđanje masovnih panika, ali i zločina. U okviru ovoga nadzora će se koristiti video-nadzor i biometrijski metodi raspoznavanja lica, a možda i bespilotne robotirane letilice. Prema Dojče Veleu pomoću ovih tehnoloških naprava, javni prostor bi mogao da se nadgleda sa ciljem da se pronađu uočljivi obrasci ponašanja koji nisu bliže definisani. Sumnjive osobe bi tako mogle lakše da se uoče, a podaci o njima, ako postoje, mogli bi da se provere u bazi podataka. Tako bi policija proveravala koja su to nenormalna ponašanja kao npr. da li neko trči, više ili glasno priča, da li neko sedi na podu u železničkoj stanici, da li je neko zaboravio prtljag i slično. Sva ova obeležja bi bila sumnjiva i potencijalno opasna. Kompjuterka procena i programiranje na ovakav način sumnjivih ponašanja i povezivanje sa određenim licima, dovelo bi do toga da svako ponašanje može biti potencijalno sumnjivo ili nenormalno. Sve ove aktivnosti koristile bi se u svrhu podrške državnim organima bezbednosti. *ACTA je pala, sledi borba protiv INDECT-a*, TANJUG, sajt b92.net, http://www.b92.net/tehnopolis/vesti.php?yyyy=2012&mm=08&nav_id=631935, 6. 10. 2013. Barbara Wimmer, *Überwachungsprojekt: Wie gefährlich ist INDECT?*, futurezone.at, <http://futurezone.at/netzpolitik/ueberwachungsprojekt-wie-gefaehrlich-ist-indect/24.583.564>, 27. 10. 2013.

446 Hans G. Zeger, *Literaturhinweis! Mensch. Nummer. Datensatz, Arge Daten* — Österreichische Gesellschaft für Datenschutz, http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&cs=85080cyv, 6. 10. 2013.

447 Phil Zimmermann, *Verschlüsselungs-Pionier: Geheimdienste bedrohen Demokratie*, derStandard.at, <http://derstandard.at/1379292203311/Verschlusselungs-Pionier-Geheimdienste-bedrohen-Demokratie>, 1. 10. 2013.

448 Citat na nemačkom jeziku glasi: Ein Krieg gegen den Terror ist nicht zu gewinnen, ein Krieg gegen die Freiheit aber in gewissem Maß schon.

449 Tako je 2001. godine neposredno posle napada u Njujorku dodeljena švajcarka prestižna nagrada BIG Brother Award sa ovim naslovom. <http://www.bigbrotherawards.ch/2001/presse/pressemitteilungen/BBA-Info-3d.pdf>, 5. 10. 2013.

prilikom dozvoliti i minimum transparentnosti u svom radu.⁴⁵⁰ Sve se čini da se vraćamo u 17. i 18. vek i u francusku i američku revolucionarnu borbu za temeljna ljudska prava? Pa ipak radi se o moći! Aristotel nije imao mnogo nedoumica kada se radi o moći. On kaže: „Zahtevati da vlada zakon znači zahtevati da vlada Bog i zakoni, a zahtevati da vlada čovek znači dopustiti i životinji da vlada, jer požuda je nešto životinjsko, a strast kvari i najbolje ljude kada su na vlasti“.⁴⁵¹

Pored špijuniranja građana, od strane NSA službe, špijunirane su i države (kao npr. Brazil, Francuska, Italija, Nemačka, Španija, Meksiko). Na taj način su američke tajne službe povredile i suverenitet špijuniranih država. Tom prilikom interesantan je odnos između tadašnjeg američkog predsednika Obame i francuskog Olanda, nakon razotkrivanja špijuniranja od strane saveznika. Obama je pokušao da umiri francuskog kolegu, sa time da se radi o iskrivljenoj slici iz medija. Oland je istakao da je to nedopustivo među prijateljima i saveznicima i zatražio je objašnjenje situacije. Prema navodima francuskih medija u ovoj akciji američkih službi bili su obuhvaćeni i francuski privrednici, administracija i političari.⁴⁵²

Slično je postupila i nemačka kancelarka Angela Merkel, čiji je telefon prema navodima nemačke vlade direktno bio prisluškivan. Prisluškivanje je obavljeno iz ambasade SAD u Berlinu, koja se nalazi na manje od kilometar od kancelarije šefice nemačke vlade.⁴⁵³ Od kolege Obame, Merkelova je zatražila objašnjenje. Identično kao i u slučaju sa Francuskom, istaknuto je prijateljstvo, partnerstvo između dve zemlje i neprihvatljivost takvog ponašanja i posledice, koje takvo ponašanje sa sobom nosi. Naravno iz krugova vlade SAD je stiglo saopštenje, da špijuniranja nije bilo i rečeno da je to potvrđeno i nemačkim kolegama.⁴⁵⁴ Interesantno je da je nemačka kancelarka samo nekoliko meseci pre ovog saznanja izjavila da ne postoji razlog da se se ne veruje američkim prijateljima, da su oni poštovali nemačke zakone. Osim toga je i zvaničnik vlade u istom periodu ovu stvar proglasio kao završenu i istakao da su im američke kolege pismeno potvrdile, da špijuniranja nije bilo.⁴⁵⁵ Ipak se čini, da je cela priča oko špijuniranja daleko od toga da je završena.

450 Barbara Wimmer, *Überwachungsprojekt: Wie gefährlich ist INDECT?*, futurezone.at, <http://futurezone.at/netzpolitik/ueberwachungsprojekt-wie-gefaehrlich-ist-indect/>, 24. 10. 2013.

451 Miodrag A. Jovanović, *Temelji demokratije*, Pravni fakultet u Beogradu, Strana 16. <https://www.google.at/url?sa=t&rcrt=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CCkQFjAA&url=http%3A%2F%2Fwww.ius.bg.ac.rs%2Fprof%2FMaterijali%2Fjovmio%2Fpredavanja%25202012%2FTemelji%2520demokratije.doc&ei=40JRUq6UJrm4wTOYHAAw&usg=AFQjCnENPjPp0IpcxvVMwFHk3aTkUlnDKA>, 6. 10. 2013.

452 Martin Holland, *NSA-Affäre: Obama beschwichtigt Frankreichs Präsidenten Hollande*, heise.de, <http://www.heise.de/newsticker/meldung/NSA-Affaere-Obama-beschwichtigt-Frankreichs-Praesidenten-Hollande-1983149.html>, 22. 10. 2013.

453 *SAD prisluškivale telefon Merkelove iz ambasade u Berlinu?*, novosti.rs, tanjug, <http://www.novosti.rs/vesti/planeta.299.html:460584-SAD-prisluškivale-telefon-Merkelove-iz-ambasade-u-Berlinu>, 25. 10. 2013.

454 Martin Holland, *NSA-Affäre: Angela Merkel wurde wohl abgehört und beschwert sich*, heise.de, <http://www.heise.de/newsticker/meldung/NSA-Affaere-Angela-Merkel-wurde-wohl-abgehoeert-und-beschwert-sich-1984739.html>, 24. 10. 2013.

455 *Wie man NSA-Affären aufklärt und beendet*, netzpolitik.org, Kilian Froitzhuber, <https://netzpolitik.org/2013/wie-man-nsa-ffaeren-aufklaert-und-beendet/>, 25. 10. 2013.

Sada se predlaže u Nemačkoj stvaranje nemačkog interneta, kome američke tajne službe ne bi mogle da pristupe. Tom prilikom trebalo bi uvesti i kodiranje mejlova. Za početak ovaj nemački intranet bi obuhvatao samo nemačke servere, a u planu bi bilo širenje i na šengenski prostor. Međutim osnovno je pitanje, da li bi takav intranet uopšte povećao bezbednost i da li bi time bilo prekinuto špijuniranje?! Sa druge strane potpuno kontrolisani, nacionalni internet podrazumeva i to da će državi biti poznato ko šalje podatke, koji se podaci i gde šalju.⁴⁵⁶

U objavljenoj studiji od strane Odbora za građanske slobode, pravosuđe i unutrašnje poslove evropskog parlamenta (LIBE) pod nazivom „Nacionalni program za masovni nadzor podataka o ličnosti u državama članicama EU i kompatibilnost sa pravom EU“ istraženo je učesće u masovnom nadzoru komunikacija.⁴⁵⁷ Ovim istraživanjem su obuhvaćene države članice EU kao što su Nemačka, Francuska, Velika Britanija, Švedska i Holandija. U izveštaju se navodi da se rezultati istraživanja odnose ne samo na zaštitu podataka, već i na vezu sa građanskim slobodama i demokratijom uopšte. Rezultati su pokazali da se prisluškivanje, presecanje, nadziranje elektronskih komunikacija odvija od strane tajnih službi u svim pomenutim zemljama, osim u Holandiji. Takođe je ustanovljeno da su tajne službe Nemačke, Francuske i Švedske inferiorne u poređenju sa američkim i britanskim, ali da to pomenute države nije sprečilo da sarađuju međusobno sa američkim kolegama.⁴⁵⁸

Sa javnim istupanjem Edvarda Snoudena i otvaranjem očiju javnosti o špijuniranju i povredi prava pojedinaca na privatnost i tajnost komunikacije, više ništa nije kao pre.⁴⁵⁹ O tome govori i podatak da je Fejsbuk izgubio 11 miliona korisnika, pre svega zbog nepoverenja u ovu društvenu mrežu zbog prosleđivanja podataka američkim tajnim službama.⁴⁶⁰ Svakako još jedan od povoda za ovakav rezultat je bilo i nedavno objavljivanje Fejsbuka kojim državama su prosleđivani podaci i na koliko zahteva je tom prilikom odgovoreno. Na taj način je ova društvena mreža i sama priznala da daje podatke o svojim korisnicima.⁴⁶¹

Ogorčenje zbog ovakvih posledica koje je prozorio Snouden po Fejsbuk, izrazio je i lično Mark Zakerberg, koji je pozvao američku administraciju da obe-

456 Dženifer Fraček, Darko Janjević, *Nemci prave „nacionalni Internet“*, b92.net, izvor: dw.de, http://www.b92.net/tehnopolis/vesti.php?yyyy=2013&mm=10&nav_id=770142, 27. 10. 2013.

457 National programmes for mass surveillance of personal data in EU Member States and the compatibility with EU law.

458 Tekst studije i zaključci se mogu pronaći na sledećoj stranici [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET\(2013\)493032_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf). Anna Biselli, *EU-Studie über Massenüberwachung in den Mitgliedsstaaten*, netzpolitik.org, <https://netzpolitik.org/2013/eu-studie-ueber-massenueberwachung-in-den-mitgliedsstaaten/>, 29. 10. 2013.

459 Interesantan je komentar nemačke kancelarke Angele Merkel, koja je rekla da je internet za sve nas nova zemlja ili novookrivena teritorija. Braneći je od ove nepromišljene izjave, njene pristalice su istakle da se internet toliko brzo razvija, da se skoro svakog dana praktično stupa na novu zemlju. Volker Briegleb, *Twitterregung nach Merckels „Neuland“ – Bemerkung*, heise.de, <http://www.heise.de/newsticker/meldung/Twitterregung-nach-Merckels-Neuland-Bemerkung-1892876.html>, 22. 10. 2013.

460 *Fejsbuk izgubio 11 miliona korisnika*, press Online, <http://www.pressonline.rs/plus/tehnol/286533/fejsbuk-izgubio-11-miliona-korisnika.html>, 21. 9. 2013.

461 Nevena Cukućan, *Fejsbuk udovoljava zahtevima 74 država sveta*, Deutschewelle, <http://www.dw.de/fejsbuk-udovoljava-zahtevima-74-dr%C5%BEava-sveta/a-17052038>, 21. 9. 2013.

lodani učesče u aktivnostima špijunaže i objasni građanima aktivnosti u ovom projektu.⁴⁶² Fejsbuk je odlučio da u ovom velikom skandalu putem suda ostvari pravo građana da saznaju više o celokupnoj aferi. Veliki giganti poput Jahua, Majkrosofta i Gugla odlučili da se u ovom sporu priključe i zajedničkim snagama istupe protiv državne administracije. Ovaj zahtev je predat američkom sudu za spoljni obaveštajni nadzor FISC (Foreign Intelligence Surveillance Court).⁴⁶³ ⁴⁶⁴ Ovaj sud je zbog pritiska javnosti ponovo potvrdio dozvolu za prikupljanje i obradu metapodataka i na taj način legalizovao program PRIZMA. Tom prilikom je šef NSA službe istakao da ukoliko oni ne bi znali, da postoje pretnje, ne bi mogli ni da ih speče, te da ova kva vrsta nadzora služi za prevenciju od terorističkih akcija.⁴⁶⁵

Pomenuti giganti (izuzev Majkrosofta) su inače polovinom 2012. godine osnovali lobi udruženje za očuvanje otvorenog, inovativnog i slobodnog interneta. Sedište udruženja je u Vašingtonu, a predsedavajući je bivši kongresmen Mihael Bakerman (Michael Beckerman). Prema njemu cilj udruženja je da se ukaže političarima u Vašingtonu na značaj interneta i ovih kompanija na tržištu rada, za privredni razvoj i slobodu uopšte.⁴⁶⁶

Pored afere PRIZMA i špijuniranja od strane američke vlade, ustanovljeno je da je i britanska vlada u okviru programa Tempora od strane tajne službe GCHQ (Government Communications Headquarters) na sličan način špijunirala građane. Ovaj slučaj špijuniranja građana, otkrio je takođe britanski dnevni list Gardijan, a na osnovnu dokumenata Edvarda Snoudena.⁴⁶⁷ U dokumentima se navodi da su države i građani špijunirani na osnovu optičkih podmorskih kablova. Tom prilikom

462 Martin Holland, *Zuckerberg: Wegen NSA-Affäre schwindet Vertrauen in Facebook*, heiseOnline, <http://www.heise.de/newsticker/meldung/Zuckerberg-Wegen-NSA-Affaere-schwindet-Vertrauen-in-Facebook-1962107.html>, 29. 9. 2013.

463 Sličan zahtev uputio je i Odbor za pravosuđe američkog Senata. U tom zahtevu generalni inspektor treba da izvrši sveobuhvatnu kontrolu NSA programa, kako bi se utvrdilo na koji način su prikupljeni podaci. *Senat traži kontrolu NSA*, Novosadske novine, Beta, <http://novinenovosadske.rs/senat-trazi-kontrolu-nsa/>, 29. 9. 2013.

464 Martin Holland, *NSA-Affäre: Facebook verlangt ebenfalls mehr Transparenz*, heiseOnline, <http://www.heise.de/newsticker/meldung/NSA-Affaere-Facebook-verlangt-ebenfalls-mehr-Transparenz-1953314.html>, 29. 9. 2013.

465 *Geheimgericht: USA dürfen weiter Telefondaten überwachen*, AFP, <http://futurezone.at/geheimgericht-usa-duerfen-weiter-telefondaten-ueberwachen/> 30.805.025, 19. 10. 2013.

466 *Google, Facebook und Ebay gründen Internetlobby*, APA/AFP, futurezone.at/netzpolitik/google-facebook-und-ebay-gruenden-internetlobby/24.583.626, 6. 10. 2013.

467 Nedavno je podneta još jedna tužba ali ovoga puta protiv vlade SAD. Tužbu je podnelo udruženje za zaštitu prava građana ACLU, da bi nateralo vladu da objavi učesče NSA službe u aktivnostima špijuniranja. Cilj je između ostalog i da se otkrije kako vlada opravdava da se optuženi drže u neizvesnosti za optužbe, kao i koje se podignute optužbe prema njima zasnivaju na špijunskim aktivnostima NSA. Pravni osnov za podnošenje tužbe je Zakon o slobodi informacija (Freedom of Information Act), koji svakom građaninu SAD daje pravo na uvid u dokumenta vlade. Ako se optuženima ne bi saopštilo, da su oni špijunirani od strane NSA bez sudskog naloga, time bi vlada SAD sprečila sudsku vlast da ispita program špijuniranja građana, saopštili su iz organizacije ACLU. Takođe ističu da u 5 godina, od kako je ovaj zakon stupio na snagu, niti jedan od osumnjičenih nije obavešten o tome da je procesuiran putem vladinog programa za špijuniranje PRIZMA. Ova organizacija je uzaludno pokušavala do sada da dođe do takvih informacija. *Details zu US-Spionage gegen Terrorverdächtige gefordert*, APA,

špijuniran je internet saobraćaj, a podaci su prosleđivani američkoj NSA. Prema navodima Snoudena, nisu samo Britanci učestvovali u špijuniranju celokupnog internet saobraćaja, već to rade i Kanada, Novi Zeland i Australija. U pogledu podataka prikupljeni su podaci o mejlovima, objavama na društvenim mrežama, telefonskim razgovorima, posetama veb stranicama. Program Tempora je prema Snoudenu u Britaniji započet polovinom 2012. godine.⁴⁶⁸

Ono što je za ovaj slučaj specifično, a ne može se primeniti u slučaju PRIZMA je tužba protiv Velike Britanije pred Evropskim sudom za ljudska prava u Strazburu zbog ovog programa špijuniranja. Tužbu je podnelo udruženje za zaštitu prava građana iz Velike Britanije.⁴⁶⁹ Razlog za ne pokretanje tužbe u slučaju PRIZMA je što SAD nisu članice Evropske konvencije o zaštiti ljudskih prava i osnovnih sloboda iz 1953. godine, dok Velika Britanija to jeste. U Velikoj Britaniji su se sudovi po ovom pitanju proglasili nenadležnima, a parlament nije poveo istragu u pomenutom slučaju, te je stoga kao jedino pravno sredstvo za zaštitu ljudskih prava ostala tužba Evropskom sudu za ljudska prava u Strazburu.⁴⁷⁰

Koliko je ovaj slučaj uzdrmao britansku javnost govori i to da je u međuvremenu otvorena i parlamentarna debata, međutim sa ciljem ovog puta istraživanja protiv nedeljnika Gardijan. Ovu istragu je potvrdio i tadašnji britanski premijer Dejvid Kameron. Cilj je da se ustanovi da li je ovaj list svojim pisanjem prekršio neki zakon ili uopšte ugrozio nacionalnu bezbednost Velike Britanije. Bivši premijer je ubeđen da je urednik bio svestan, da će svojim pisanjem i objavljivanjem tekstova izazvati opasnost za nacionalnu bezbednost.⁴⁷¹ Na ovaj način se država umešala u slobodu štampe, kao i pravo na slobodu mišljenja i izražavanja, koji su granatovani Konvencijom o zaštiti ljudskih prava i sloboda u članu 10. Ostaje da se vidi, da li će parlament ovom prilikom uspeti da ostvari pravo na osnovu nekog britanskog zakona i na taj način zbog problema bezbednosti, sankcioniše Gardijan.⁴⁷²

futurezone.at, <http://futurezone.at/netzpolitik/details-zu-us-spionage-gegen-terrorverdaechtige-gefordert/31.540.479>, 19. 10. 2013.

468 Oliver Diedrich, *Bericht: Briten schnüffeln Internet noch massiver aus als die USA*, heise.de, <http://www.heise.de/newsticker/meldung/Bericht-Briten-schnueffeln-Internet-noch-massiver-aus-als-die-USA-1894852.html>, 19. 10. 2013.

469 Martin Holland, *GCHQ-Überwachung: Bürgerrechtler klagen in Straßburg*, heise.de, <http://www.heise.de/newsticker/meldung/GCHQ-Ueberwachung-Buergerrechtler-klagen-in-Strassburg-1972227.html>, 19. 10. 2013.

470 Stefan Krempf, *Rechtsexperten im EU-Parlament: NSA und GCHQ verletzen Menschenrechte und Souveränität*, heise.de, <http://www.heise.de/newsticker/meldung/Rechtsexperten-im-EU-Parlament-NSA-und-GCHQ-verletzen-Menschenrechte-und-Souveraenitaet-1979088.html>, 19. 10. 2013.

471 *Snowden-Enthüllungen: Ausschuss soll Untersuchungen gegen Guardian einleiten*, unwatched.org, http://www.unwatched.org/20131017_Snowden-Enthuellungen_Ausschuss_soll_Untersuchungen_gegen_Guardian_einleiten, 19. 10. 2013.

472 U članu 10 stav 2 kaže se: „Pošto korišćenje ovih sloboda (slobode mišljenja i izražavanja) povlači za sobom dužnosti i odgovornosti, ono se može podvrgnuti formalnostima, uslovima, ograničenjima ili kaznama propisanim zakonom i neophodnim u demokratskom društvu u interesu nacionalne bezbednosti, teritorijalnog integriteta ili javne bezbednosti, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili morala, zaštite ugleda ili prava drugih, sprečavanja otkrivanja obaveštenja dobijenih u poverenju, ili radi očuvanja autoriteta i nepristrasnosti

6.3. Ostali aspekti mešanja država u neutralnost internet mreže

Pored već navedenog fenomena digitalnog nadzora interneta i uopšte telekomunikacija u svrhu borbe protiv terorizma, trgovine ljudima i opšte bezbednosti, države kao opravdanje za špijuniranje građana navode i ugrožavanje autorskih prava ali i zaštite dece u borbi protiv dečije pornografije i zloupotrebe dece. Tim povodom mnoge države su pribegle nadzoru interneta i elektronskih komunikacija, da bi uspele navodno da spreče ove pojave. Sa tim u vezi je zanimljivo kakve mere se preduzimaju u praksi.

Vlasti Velike Britanije nadziru komunikaciju Britanaca preko Fejsbuka i Tvitera, još pre afere Tempora. Ove informacije proizlaze iz parlamentarnog izveštaja iz Februara 2013. godine. Nadziranje treba da omogući celokupnu kontrolu internet saobraćaja preko poziva obavljenih putem Skajpa do pristupa pornografskim sadržajima. Metod koji koriste vlasti je tzv. „*Deep Packet Inspection*“, koji omogućava nadzor detaljnim pretraživanjem sadržaja.⁴⁷³

Tako se zbog borbe protiv dečije pornografije u Velikoj Britaniji uvode od 2014. godine tzv. filteri, pomoću kojih će internet provajderi moći da blokiraju stranice na internetu, koje imaju ovakve sadržaje. Uбудućе će, oni koji budu hteli da gledaju pornografski sadržaj, morati da dokažu svoje godine, da bi im internet provajderi dozvolili pristup sadržaju. Osim ove mogućnosti, internet servis provajderi će moći da je koriste i za igre na sreću, kako bi blokirali pristup. Za implementaciju britanskog modela se zalažu i neke partije u Austriji, koje ovakav vid kontrole interneta, ne posmatraju kao cenzuru, već kao legitiman oblik borbe za zaštitu prava dece. Međutim, udruženja internet servis provajdera su drugačijeg mišljenja te ističu „da čim postoji infrastruktura za blokiranje veb stranica, ona se može vrlo lako zloupotребiti u druge svrhe. Prema njihovom mišljenju ova tematika je stvar obrazovanja i vaspitanja u širem smislu reči, a ne problem interneta i njegove kontrole. Osim toga sve ovo vodi do stigmatizacije, a šta je sve moguće sa takvom kontrolom postići pokazao je slučaj programa PRIZMA.“⁴⁷⁴

U Kini, zemlji koja ima 500 miliona korisnika interneta, možda postoji i najveća cenzura na svetu. Pored velikog broja korisnika interneta, nisu sve usluge ove mreže dostupne. Tako su npr. društvene mreže poput Fejsbuka, Tvitera totalno cenzurisane i nije im moguće pristupiti. Opravdanje za cenzuru sadržaja je nacionalna bezbednost! To svakako ne znači da u Kini nema društvenih mreža, ali se one nalaze isključivo u ovoj zemlji i pod kontrolom su domaćih vlasti.^{475 476}

sudstva“. Na taj način je shodno Konvenciji dato pravo državama, da pronađu niži pravni akt ili argument da sankcionišu slobodu mišljenja i izražavanja.

473 *Engleska: Vlada špijunira društvene mreže?*, b92.net, http://www.b92.net/tehnopolis/vesti.php?yyyy=2013&mm=02&nav_id=684054, 27. 10. 2013.

474 *Porno-Filter für ÖVP denkbar*, futurezone.at, die Presse,<http://futurezone.at/netzpolitik/porno-filter-fuer-oevp-denkbar/24.600.514>, 21. 10. 2013.

475 Najpoznatije su Sina Weibo, Renren, Youku.

476 *Kineska internet cenzura i društvene mreže*, b92.net, http://www.b92.rs/tehnopolis/vesti.php?yyyy=2011&mm=12&nav_id=562320, 21. 10. 2013.

Za razliku od Kine u Indiji je Fejsbuk dostupan, ali su vlasti tražile strožu kontrolu korisnika i mogućnost da nadgledaju i uklone ili blokiraju uvredljiv sadržaj sa Fejsbuka. Povod za ovakvu reakciju vlasti je to što se na Fejsbuku često vredi kultura i osećanja Indijaca. Iz Fejsbuka su tom prilikom saopštili da oni i inače uklanjaju uvredljiv i pornografski sadržaj.⁴⁷⁷ Pored toga je Fejsbuk u sudskom postupku obavezan da uspostavi sistem i mehanizme, koji bi omogućili uklanjanje uvredljivih i bogohulnih poruka.⁴⁷⁸ U Indiji je takođe na snazi zakon, kojim se omogućava internet korisnicima da reaguju na onlajn sadržaje u roku od 36 sati od objavljivanja. Po pritužbi korisnika, operateri veb sajtova su dužni da uvredljive ili neprigladne sadržaje uklone.⁴⁷⁹

Takođe u Iranu je Fejsbuk dostupan, iako je u ovoj zemlji posećivanje bilo koje internet stranice „koja širi nemoral i može oslabiti veru zabranjeno i predstavlja protivislamsku aktivnost“. Fejsbuk je jedna od ovih internet stranica, te je greh biti njen član prema mišljenju iranskog ajatolaha Lotfolah Safi-Golpajganija. Ovakve ocene pojava u društvu ajatolaha predstavljaju uredbe o ponašanju u ovoj islamskoj republici. I pored mnogobrojnih blokada veb sajtova, Iranci uspevaju da pronalaze zaobilazna rešenja i pristupaju željenim sadržajima. Blokade i cenzura sadržaja se opravdavaju borbom protiv zapadne kulture.⁴⁸⁰ Osim toga u Iranu postoji i policija, koja se bavi nadzorom interneta, a u planu je i stvaranje iranskog interneta.⁴⁸¹ Za Fejsbuk i ostale društvene mreže je irancima dozvoljen pristup, međutim uz pomoć jednog softvera, kojim se filtrira sadržaj.⁴⁸² Zvaničnici ove države smatraju da je bolje imati jednu inteligentnu kontrolu društvenih mreža, nego ih kompletno zabraniti ili blokirati. Fejsbuk je posebno nadziran prilikom ponovnog izbora predsednika Mahmuda Ahmadinedžada, pošto su Fejsbuk i Tviter imali ključnu ulogu prilikom organizacije protesta u islamskim zemljama.⁴⁸³

U Tadžikistanu je pristup Fejsbuku zabranjen zakonom, kao odgovor na pritužbe građana zbog laži i uvreda vlade. Putem ove društvene mreže je bilo previše uvreda na račun predsednika države i članova vlade, osim toga poznate ličnosti su

477 *Indija traži nadgledanje internet*, b92.net, http://www.b92.rs/tehnopolis/vesti.php?yyyy=2011&mm=12&nav_id=563450, 21. 10. 2013.

478 *Indija: Google i Facebook prihvatili cenzuru*, tanjug, novosti.rs, <http://www.novosti.rs/vesti/naslovna/aktuelno.236.html:365397-Indija-Google-i-Facebook-prihvatili-cenzuru>, 21. 10. 2013.

479 Indija je zemlja koja ima najveći potencijal za povećanje korisnika interneta. Sa svojih 1,2 milijarde stanovnika, trenutno ima svega 10% stanovništva pristup internetu. Očekuje se da će se taj broj u naredne tri godine utrostručiti i na taj način će Indija postati treća zemlja po broju internet korisnika posle SAD i Kine. *Google und Facebook müssen Inhalte löschen*, futurezone.at, <http://futurezone.at/netzpolitik/google-und-facebook-muessen-inhalte-loeschen/24.576.461>, 25. 10. 2013.

480 *Fejsbuk antiislamska mreža*, Tanjug, kurir.rs, <http://www.kurir-info.rs/fejsbuk-antiislamska-mreza-clanak-132186>, 21. 10. 2013.

481 Još jedan od razloga za stvaranje iranskog internet je i odbrana odnosno zaštita od sajber napada. Inače je Iran samo u 2012. godini blokirao 5 miliona veb stranica. Axel Kannenberg, *Iran plant wohl doch die Abkopplung vom Internet*, heise.de, <http://www.heise.de/newsticker/meldung/Iran-plant-wohl-doch-die-Abkopplung-vom-Internet-1664898.html>, 21. 10. 2013.

482 *Iran želi kontrolu društvenih mreža*, b92.net, Tanjug, http://www.b92.net/tehnopolis/vesti.php?yyyy=2013&mm=01&nav_id=675021, 27. 10. 2013.

483 *Iran plant kontrollierten Zugang zu Facebook*, portal futurezone.at, APA/AFP, <http://futurezone.at/netzpolitik/iran-plant-kontrollierten-zugang-zu-facebook/24.590.855>, 27. 10. 2013.

bile uznemiravane i klevetane od nepoznatih, anonimnih korisnika, navodi se u odluci vlade.⁴⁸⁴

Inače je Evropski sud doneo odluku u kojoj se društvenim mrežama i internet provajderima zabranjuje da uvedu „filtre“, koji će korisnicima onemogućiti da razmenjuju sadržaje zaštićene autorskim pravima. Povod za ovu odluku suda je bio zahtev belgijske agencije za zaštitu autorskih prava SABAM, koja je tužila društvenu mrežu Netlog, zahtevajući da se njenim korisnicima zabrani razmena filmskih, muzičkih i drugih sadržaja preko interneta. Sud je u presudi utvrdio da se zahtevom agencije SABAM i potencijalnom ugradnjom filtera od strane društvene mreže Netlog, kojima bi se korisnici sprečavali da razmenjuju sadržaje koji su zaštićeni autorskim pravima, krše principi slobodne trgovine i slobode izražavanja ali i pravo privatnosti korisnika interneta.⁴⁸⁵ Pored toga u odluci suda je navedeno da bi filtriranjem internet saobraćaja bili praćeni svi korisnici elektronskih komunikacija provajdera Skarlet i na taj način bi bila narušena njihova prava ali i prava EU. Sud je istakao da bi tom prilikom trebalo uspostaviti „pravedan balans“ između prava na intelektualnu svojinu, s jedne strane, i prava na zaštitu podataka ličnog karaktera i slobodu razmene informacija, s druge strane.⁴⁸⁶

Veoma je upečatljiva izjava bivšeg austrijskog šefa službe za zaštitu ustavnosti i borbu protiv terorizma Gert-René Polli povodom afere PRIZMA, koji tvrdi da su ciljevi NSA usmereni na potpunu kontrolu nad svetskim tokovima novca i sakupljanje svih relevantnih informacija tim povodom. Osim toga za ekonomiju SAD je centralna tema tzv. industrijska špijunaža, za čije praćenje su prikupljane informacije od vlada stranih država, avio kompanija, kompanija koje se bave snabdevanjem električnom energijom i finansijskih organizacija. Kao primer za svoju tvrdnju Polli je naveo podatke vezano za kreditne transakcije. Naime na osnovu SWIFT sporazuma između EU i SAD i američkog Patriot Act-a, omogućeno je lako prikupljanje informacija o aktivnostima kompanija, pošto američke tajne službe u skladu sa ovim propisima imaju pristup navedenim podacima. „Borba protiv terorizma je samo jedan sporedan efekat i predstavlja argument, da bi se proširila ovlašćenja tajnih službi, kao i da bi i druge zemlje ušle u saradnju sa SAD“, tvrdi ovaj stručnjak. Možda i najvažnija izjava ovog stručnjaka povodom celokupnog programa špijuniranja je da je „špijunaža verovatno drugi najstariji zanat na svetu. Ovaj bi bilo teže verovatno ukinuti, nego da se ukine najstariji“. Na ovaj način je reagovao na takozvane pokušaje sklapanja sporazuma o ne špijuniranju između EU i SAD, i izrazio svoje mišljenje o tome koliko bi oni bili politički naivni.⁴⁸⁷

484 *Tadžikistan zabranio Facebook*, b92.net, Tanjug, http://www.b92.net/tehnopolis/vesti.php?yyyy=2012&mm=11&nav_id=663922, 27. 10. 2013.

485 *Bez filtriranja na društvenim mrežama*, tanjug, b92.net, http://www.b92.rs/tehnopolis/vesti.php?yyyy=2012&mm=02&nav_id=583335, 21. 10. 2013.

486 *Evropski sud: Društvene mreže bez „filtera“*, Beta/AFP, blic.rs, <http://www.blic.rs/IT/307429/Evropski-sud-Društvene-mreze-bez-filtera>. 21. 10. 2013.

487 Florian Christof, *Kampf gegen den Terrorismus ist nur ein Nebeneffekt*, futurezone.at, <http://futurezone.at/netzpolitik/kampf-gegen-den-terrorismus-ist-nur-ein-nebeneffekt/30.407.666>, 24. 10. 2013.

7. ZAKLJUČAK

Fejsbuk svakodnevno koristi više od dve milijarde ljudi. Osim toga ova društvena mreža svakodnevno prikuplja neverovatne količine svih vrsta podataka, daleko veće nego što mogu da prikupi tajne službe bilo koje države. Fejsbuk prati internet surfovanje odnosno saobraćaj i na taj način pravi detaljno profilisanje internet korisnika. Kada su korisnici prijavljeni (ulogovani), Fejsbuk uzima podatke sa profila korisnika, ime, e-mail adresu, listu prijatelja i stvari koje su lajkovane, ali i IP-adresu, podatke o rezoluciji ekrana, operativnom sistemu i browseru koji je korišćen. Vreme, datum i URL svakoga ko koristi Fejsbukov društveni dodatak „Social Plug-in“. Podaci se prate, bez obzira da li je korisnik pristao i bez ikakve najave da će to biti urađeno.

Korisnici nemaju dovoljno informacija u politici o privatnosti Fejsbuka, ne postoji konkretan, nedvosmislen i izričit pristanak korisnika na prepoznavanje lica, kao ni informacija o tome. Funkcija se automatski aktivira i biometrijski podaci sakupljaju bez unapred date saglasnosti korisnika. Prikupljanje biometrijskih podataka od preko dve milijarde korisnika predstavlja prekomerno sredstvo u odnosu na svrhu koja se postiže. Time je povećan rizik mogućnost zloupotrebe kao i rizik čuvanja ovolikog broja podataka.

Fejsbuk je do sada uspeo da prikupi količinu podataka o pojedincima koju nije uspela da prikupi ni jedna vlada na svetu. Pored ovoga korisnici Fejsbuka su u stalnoj opasnosti, zbog lakog pristupa osetljivim informacijama koje se o njima čuvaju.

Većina korisnika nije uopšte svesna, da ako njihov prijatelj na Fejsbuku instalira neku aplikaciju, aplikacija može automatski dovesti do transfera podataka i pristupa profilu, slikama, imenima i ostalnim podacima prijatelja.

Još više zabrinjava činjenica da su čelnici Fejsbuka priznali da se sva vrsta komunikacije putem ove društvene mreže strogo nadzire i prati. Prati se svaka vrsta komunikacije preko statusa, priče, četa uz pomoć automatizovanih softvera, na osnovu kojih je moguće utvrditi i značenje frazi u nekom jeziku. Uvid u ovu vrstu podataka Fejsbuk omogućava i tajnim službama SAD.

Fejsbuk ima skoro sve *prerogative države* (osim vlasti nad internet mrežom), pošto je u stanju da odobrava međunarodnu pravnu pomoć, ima ogroman broj korisnika širom sveta, postavlja se kao arbitar u proceni globalnog morala, dobrih običaja i kao sudija da li će određeni sadržaji biti objavljeni, obrisani ili blokirani. Te stoga i ne čudi što države potpisuju sporazume sa Fejsbukom poput Indije, Pakistana itd.

Korisnici Fejsbuka nemaju pravo na „digitalni zaborav“. Deaktivacija znači privremeno ukidanje profila, ali ne i trajno. Naime ukoliko korisnik deaktivira svoj nalog, Fejsbuk će i dalje držati njegove podatke, za slučaj da se vrati. Upravo ovakav način zadržavanja podataka je suprotan modernim propisima o zaštiti podataka. Obrada i način korišćenja podataka korisnika predstavlja najveću nedoumicu. I da-

lje nije poznato šta zapravo Fejsbuk radi sa podacima korisnika. Svi podaci koje korisnici postavljaju na Fejsbuk pripadaju i postaju vlasništvo Fejsbuka, što je potpuno neprihvatljivo. Naime, oni postaju umesto ličnog prava pojedinca, svojina Fejsbuka. Kao što je Maks Šrems istakao radi se o potpunoj „*eksproprijaciji podataka*“ korisnika Fejsbuka.

Ohrabruje donošenje Opšte uredbe o zaštiti podataka na nivou EU, kao i jednoobraznost u primeni prava. Fejsbuk će morati da promeni ponašanje u obradi podataka svojih korisnika i prilagodi se odredbama uredbe, inače mu prethodi *kazna do skoro milijardu evra*.

Problematika sudske nadležnosti je u slučaju Fejsbuka veoma kompleksna, pošto dolazi do preplitanja više pravnih grana i mnoštva pravnih sistema. Fejsbuk u svojim opštim uslovima poslovanja, na koje naravno pristaju svi korisnici interneta, navodi isključivu nadležnost suda SAD i time je svaki korisnik obavezan da svoju sudsku zaštitu ostvari u SAD, sa izuzetkom ukoliko se radi o korisnicima, koji dolaze izvan SAD i Kanade, a u slučaju eventualnih sporova za njih je predviđena isključiva nadležnost sudova u Irskoj. Upravo Opšta uredba o zaštiti podataka je konačno rešila problematiku sudske nadležnosti, tako da korisnici Fejsbuka mogu ovu društvenu mrežu da tuže i u državi članici EU iz koje potiču.

Sporazumom Privacy Shield između EU i SAD su utvrđeni dodatni mehanizmi zaštite podataka građana EU od špijuniranja američkih tajnih službi na koje se i Fejsbuk obavezao. Čini se da je ipak ova vrsta garancije i od strane SAD i od strane Fejsbuka, kao što je konstatovao Jan Albrecht „*blanko ček bez adekvatne zaštite podataka*“ za korisnike Fejsbuka.

Sudska praksa je pokazala tendenciju zaštite podataka i zaštite potrošača. Stoga se mogu očekivati ubuduće drakonske kazne po Fejsbuk. Osim toga u praksi je pokazano i to da jedan klik na Fejsbuku može imati za posledicu sudski spor i kaznu od više stotina hiljada evra (npr. pozivi na žurke), a nekoliko reči objavljenih putem Fejsbuka mogu rezultirati otkazom na poslu, krivičnim delima ili zatvorskim kaznama.

Po svemu sudeći *politika i pravo su u velikom zaostatku za tehnologijom*, ali i osnovni principi na kojima su napravljene moderne države više nisu u stanju da isprate razvoj interneta i protok informacija. Čini se da će se ipak posle svih navedenih okolnosti i u slučaju Fejsbuka u krajnjoj liniji desiti narod. Pošto „*kada pravo postane nepravo i nepravda, otpor postaje obaveza!*“, rekao je Bertold Brecht poznati nemački pesnik i dramaturg.

Nalazimo se u vremenu, u kojem je istupanje američkog obaveštajca Edvarda Snoudena, jasno pokazalo sliku i obim neslobode pojedinca u modernom demokratskom društvu. Ideja totalnog internet nadzora od strane država i uloga Fejsbuka u ovom lancu, još jednom je potvrdila izreku da je znanje moć!

Poražavajuće u svemu tome je, što se posledice ne osećaju direktno i neposredno u našim životima. Informacije su danas postale u tom segmentu važne kao i zaštita životne sredine. One su kao radijacija — zbog gomilanja podataka, samo je pitanje vremena kada će procureti. Istovremeno smo se već na puno toga navikli, pa i na svakodnevno korišćenje Fejsbuka, ali da li smo uopšte svesni, na koji način funkcioniše Fejsbuk? Upravo to neznanje nas čini robovima modernog doba i giga-

nata poput Fejsbuka. Društvene mreže su nam omogućile da se tako lako spajamo sa ljudima širom sveta, ali ne i da sa njima raskinemo!⁴⁸⁸ Treba imati u vidu i da nas Fejsbuk, kao uostalom i komunikacija putem interneta spaja sa ljudima koji su daleko od nas, ali nas razdvaja od onih koji su pored nas.

Ono što se zapravo dešava u modenoj komunikaciji putem interneta je istorijski gledano jedan drastičan prelazi iz stanja totalne neobaveštenosti u stanje sveobuhvatne informisanosti. Iako ljudi generalno ne bi voleli da se o njima sve zna, danas je moguće o svima sve saznati. Glavni uzrok ovoga su digitalna nepismenost i kontrola od strane moćnika poput Fejsbuka.

Neutralnost internet mreže svakako ne postoji iz svega priloženog, ali da li ono predstavlja i eroziju društva u celini (pošto se radi o temeljnim ljudskim pravima) i koje će posledice svega biti, ostaje da se vidi. Ne bi bilo nemoguće i da se celokupna priča oko Fejsbuka i špijuniranja preko društvenih mreža i od strane država završi jednom internet revolucijom, pa da umesto već viđenog arapskog proleća dobijemo Snoudenovu revoluciju ili neku sajber revoluciju. Da li je i koliko globalne moćnike u ovom lancu ovo saznanje uzdrimalo, da li je u svesti građana došlo do tačke usijanja, pokazaćće vreme.

„Status hominum naturalis antequam in societatem coiretur Bellum fuerit; neque hoc simpliciter, sed bellum omnium in omnes“!

Prirodno stanje ljudi, pre nego što su ušli u društvo/zajednicu bio je rat; i to nije jednostavan, *već rat svakog čoveka protiv svih ljudi*.⁴⁸⁹ Tomas Hobs (u delu *Sloboda „Libertas“*, poglavlje 1, deo 12).

488 S. Đurić, Za raskid na Fejsu potrebno uputstvo?, sajt novosti.rs, http://www.novosti.rs/vesti/zivot_+303.html:463379-Za-raskid-na-Fejsu-potrebno-uputstvo, 13. 12. 2013.

489 U nekim izvorima se kaže i „Bellum omnium contra omnes“ Rat sviju protiv svih! Misli se na život i borbu između ljudi.

8. LITERATURA

- Aplin Tanya, *Copyright Law in the Digital Society: The Challenges of Multimedia*, 2005.
- Bainbridge David, *Introduction to Computer Law*, Longman, 2000.
- Banović Božidar, *Elektronski dokazi*, Revija za kriminologiju i krivično pravo, br. 3/2006.
- Diligenski Andrej, *Obaveza navođenja pravog imena na Fejsbuku*, portal Zaštita podataka o ličnosti, <http://partners-serbia.org/privatnost/blog/obaveza-navodenja-pravog-imena-na-fejsbuku/>, 8.8.2013.
- Dimitrijević Predrag, *Pravo informacione tehnologije*, SVEN, Niš, 2010.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L* 281, 23/11/1995.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *Official Journal L* 201, 31/07/2002.
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *Official Journal L* 105, 13/04/2006.
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, *Official Journal L* 337, 18/12/2009.
- Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, *Official Journal L* 337, 18/12/2009.
- Drakulić Mirjana i Drakulić Ratimir, *Pravna regulacija e-poslovanja*, Internet adresa: <http://www.e-trgovina.co.yu/pravo/regulacija1.html>, 17. 8. 2009.
- Drozdova Ekatarina A, *Civil Liberties and Security in Cyberspace*, u: Abraham D.Sofaer, Seymour E.Goodman (ed.), *The Transnational Dimension of Cyber Crime and Terrorism*, Hoover Press, 2001.
- Dworkin Gerald, *Judicial Control of Copyright on Public Policy Grounds*, in: *Intellectual Property and Information Law*, Kluwer, 1998.

- Efroni Zohar, *Access — Right: The Future Of Copyright Law*, Oxford University Press, 2011.
- Fejsbuk, *Opšti uslovi poslovanja Fejsbuka*, <http://www.facebook.com/legal/terms>, 2013.
- Fink Simon, *Datenschutz zwischen Staat und Markt (Die „Safe Harbor“-Lösung als Ergebnis einer strategischen Interaktion zwischen der EU, den USA und der IT-Industrie)*, UNIVERSITÄT KONSTANZ, 2002, Magisterarbeit.
- Hoeren Thomas, *Facebook und Co: Es ist nicht alles Gold, was glänzt, Risiken für Unternehmen und Privatnutzer*, Wissen+Karriere časopis, broj Ausgabe 06/2011 September/Oktober
- Jehoram Tobias Cohen, *Copyright in Non-Original Writings Past — Present — Future ?*, in: *Intellectual Property and Information Law*, Kluwer, 1998.
- Jelić Ivan, *Zajednica u savremenom informatičkom društvu*, 2006, Internet adresa: <http://www.bos.rs/cepit/idrustvo2/tema14/zajednica.pdf>.
- Kabel Jan, *Intellectual Property and Information Law*, Kluwer, 1998.
- Koumantas Georges, *Reflections on the Concept of Intellectual Property*, in: *Intellectual Property and Information Law*, Kluwer, 1998.
- Krebs Brian, *Year of Computing Dangerously*, Washington Post, 22. 12. 2006, <http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122200367.html>.
- Litman Jessica, *Digital copyright: protecting intellectual property on the Internet*, Prometheus Books, 2001.
- Maisl Herbert, *Etat de la Legislation Française et Tendences de la Jurisprudence Relatives à la Protection des donnees Personnelles*, Revue Internationale de Droit Comparé, No. 3, 1987.
- Mezrih Ben, *Slučajni milijarderi: nastajanje Fejsbuka*, Beograd: Evro-Giunti, 2010.
- National Research Council (US), *The digital dilemma: intellectual property in the information age*, National Academic, 2000.
- Overbeck Wayne, Genelle Belmas, *Major principles of media law*, Stamford: Cengage Learning, 2011.
- Prlja Dragan, Andrej Diligenski, *Pravni aspekti neutralnosti internet mreže*, Strani pravni život, br. 3, 2011.
- Prlja Dragan, Ivanović Zvonimir, Reljanović Mario, *Krivična dela visokotehnološkog kriminala*, Institut za uporedno pravo, Beograd, 2011.
- Prlja Dragan, Reljanović Mario, *Pravna informatika*, Beograd, Službeni glasnik, 2010.
- Prlja Dragan, Reljanović Mario, *Visokotehnološki kriminal — uporedna iskustva*, Strani pravni život 3/2009.
- Regulation 2016/679 of the European Parliament and of the Council of 7 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88.
- Reljanović Mario, *Odnos prava na privatnost i pojedinih aspekata visokotehnološkog kriminala*, u: Komlen-Nikolić Lidija et alia, *Suzbijanje visokotehnološkog kriminala*, Beograd, 2010.

- Savet Evrope, *Konvencija o zaštiti ljudskih prava i osnovnih sloboda*, Rim, 1950, http://www.echr.coe.int/NR/rdonlyres/EA13181C-D74A-47F9-A4E5-8A3AF5092938/0/Convention_BOS.pdf, 4. 3. 2013.
- Schafer Arthur, *Privacy — A Philosophical Overview, Aspects of Privacy Law*, Edited by Dale Gibson, Toronto, 1980.
- Stamotoudi Irini, *Copyright Enforcement and the Internet*, Kluwer, 2010.
- Stokes Simon, *Digital Copyright: Law and Practice*, 2005.
- Vaidhyathan Siva, *Copyrights and copywrongs: the rise of intellectual property and how it threatens*, NYU Press, 2003.
- Warren Samuel, Brandais Louis, *The Right to be Left Alone*, Harvard Law Review, 1890.
- Wilkens Andreas, *Facebook: „Likes“ stehen unter dem Schutz der US-Verfassung*, heise-Online, <http://www.heise.de/newsticker/meldung/Facebook-Likes-stehen-unter-dem-Schutz-der-US-Verfassung-1662776.html>, 22. 8. 2013.



Andrej Diligenski

Andrej Diligenski rođen je u Beogradu 1984. godine, gde je diplomirao na Pravnom fakultetu Univerziteta u Beogradu na međunarodnom pravnom smeru. Specijalističke master studije je završio u Beču u oblasti informatičkog prava i prava informacionih tehnologija na temu „Implementacija elektronske uprave — poređenje Austrije i Srbije“ („Umsetzung von E-Government“ — Ein Vergleich zwischen Österreich und Serbien). Trenutno radi na odbrani doktorske disertacije na Pravnom fakultetu u Beču na temu „Zaštita podataka u telekomunikacionom pravu Crne Gore“ (Datenschutz im Telekommunikationsrecht Montenegros).

Sertifikovan je od austrijskog sertifikacionog tela ARGE DATEN i austrijskog univerziteta Donau Uni Krems kao poverenik za zaštitu podataka. Pored toga je i sertifikovan menadžer za informacionu sigurnost (information security manager) po svetskom standardu ISO 27001 od austrijskog sertifikacionog tela CIS.

Zaposlen je kao menadžer za zaštitu podataka firme Grant Thornton Unitreu Advisory GmbH u Beču.

Spoljni saradnik je Instituta za uporedno pravo u Beogradu. Objavio je više naučnih radova i blogova između ostalih „Zaštita autorskih prava u digitalnom svetu“, „Pravni aspekti neutralnosti internet mreže“, „Organizovani kriminal i digitalna forenzika“, „Zaštita podataka kod mergers & acquisitions“, „Religija, politika i pravo u sajber svetu“, itd.

E-mail: andrej84_4@hotmail.com



Dragan Prlja

Dragan Prlja rođen je u Ostojićevu 1959. godine, a diplomirao je, magistrirao i doktorirao na Pravnom fakultetu Univerziteta u Beogradu na međunarodno-pravnom smeru.

Zaposlen je kao naučni saradnik u Institutu za uporedno pravo u Beogradu.

Predavač je na više fakulteta na predmetima vezanim za upotrebu informacionih tehnologija u oblasti prava.

Objavio je 27 knjiga i preko 100 naučnih radova iz oblasti visokotehnološkog kriminala, elektronske trgovine, elektronske uprave, zaštite podataka, i autorskih prava.

E-mail: d.prlja@iup.rs

CIP — Каталогизација у публикацији
Народна библиотека Србије, Београд

342.738
316.472.4

ДИЛИГЕНСКИ, Андреј, 1984–

Fejsbuk, zaštita podataka i sudska praksa / Andrej
Diligenski, Dragan Prlja. – Beograd : Institut za uporedno pravo,
2018 (Beograd : Dosije studio). – 145 str. : slike autora ; 24 cm
Tiraž 500. – Beleške o autorima: str. [146–147]. – Napomene i
bibliografske reference uz tekst. – Bibliografija: str. 143–145.

ISBN 978-86-80186-28-3

1. Прља, Драган, 1959– [аутор]

а) Фејсбук (компанија ; Менио Парк) – Правни аспект

б) Право на заштиту података о личности

с) Друштвене мреже – Правни аспект

COBISS.SR-ID 257526028

ISBN 978-86-80186-28-3

