

SVEUČILIŠTE U ZAGREBU

FILOZOFSKI FAKULTET

ODSJEK ZA FILOZOFIJU

Maja Vejić

PROBLEM SUBJEKTA U CYBER-RATOVANJU

Diplomski rad

Mentor: nasl. doc. dr. sc. Goran Sunajko

Zagreb, rujan, 2018.

Sadržaj

1. Uvod.....	1
2. Ideja subjekta u filozofiji.....	4
2.1. Platonova spilja.....	4
2.2. Aristotel: formiranje subjekta.....	6
2.3. Descartes: formiranje novovjekovnog subjekta.....	7
2.4. Hobbes: subjektivnost i suverenost.....	9
2.5. Kant: <i>Sapere aude!</i>	13
2.6. Husserl: pojava i realnost.....	15
2.7. Jonas: odgovornost subjekta.....	19
3. Problem subjekta u cyber-sferi.....	23
3.1. Kako postojati online?.....	23
3.2. Realni vs. virtualni subjekt.....	26
3.3. Hiperindividualizacijom prema nestanku: gdje je nestao subjekt?.....	33
4. Pravne implikacije cyber-ratovanja.....	38
4.1. Pravni problemi: što je napad u cyber-sferi?	38
4.2. Subjekt u cyber-ratovanju.....	43
4.3 Cyber-subjekt vs. cyber-civil.....	48
5. Zaključak: subjekt na kušnji.....	52
Popis literature.....	55

Problem subjekta u cyber ratovanju

Sažetak

Pitanje subjektivnosti jedno je od primarnih pitanja u povijesti filozofije. Cilj ovog rada je preispitati pojam subjekta, s posebnim osvrtom na problematiku subjektivnosti unutar cyber-sfere i cyber-ratovanja. Prva cjelina bavi se razvojem ideje subjektivnosti i formiranja subjekta kroz filozofsku misao, od Platona i Aristotela, preko Descartesa, Hobbesa i Kanta, sve do Husserla i Jonasa. U tom dijelu obrađeni su neki ključni elementi teorija subjektivnosti, ideja suvereniteta, te neke etičke dileme nužne za raspravu o subjektu. Druga cjelina bavi se upravo pitanjima načina egzistencije individue u cyber-sferi i mogućnosti postojanja online iz konteksta prethodne rasprave o subjektivnosti, mogućnosti razdvajanja subjekta realnog svijeta i subjekta cyber-sfere, kako u personalnom, tako možda i u pravnom smislu i fenomenom sve intenzivnijeg pokušaja brisanja subjektivnosti iz cyber-sfere. Treća cjelina finalizira problematiku raspravom o ratnom kontekstu djelovanja u cyber-sferi, pokušajima redefiniranja osnovnih ratnih pojmova, lociranjima točki odgovornosti i postavljanjima pitanja civila kao dodatne pod-kategorije rasprave o subjektu. Zaključnim se poglavljem, „Subjekt na kušnji“, pokušava sintetizirati sva tri dijela i još jednom ukazati na važnost kontinuirane rasprave o subjektivnosti u današnjim uvjetima i okolnostima.

Ključne riječi: subjekt, subjektivnost, etika, cyber-sfera, cyber-rat, suverenitet, odgovornost, civil, cyber-operacije

The Problem of Subject in Cyber-War

Abstract

The question of subjectivity is one of the elementary questions in the history of philosophy. The goal of this paper is to once again question the term subject, especially concerning the problem of subjectivity in the cyber-sphere and cyber-war. The first part analyses the development of the idea of subjectivity in the history of philosophy, from Plato and Aristotle, through Descartes, Hobbes and Kant, over to Husserl and Jonas. Some key aspects of the subjectivity theories, ideas of sovereignty and some ethical dilemmas necessary for thinking about subject are discussed in this part. The second part focuses on the ways the individual exists in the cyber-sphere, and the possibility of existing online, in the context of the earlier discussion about subjectivity, the possibility of separating the subject of the real world from the subject in the cyber-sphere, both in private and legal sense, and the phenomenon of more and more intense attempts of deleting the subject from the cyber-sphere. The third part finalizes the problem with the discussion about wartime cyber-operations, attempting to redefine the main war terminology, locating the key points of responsibility in cyber warfare and furthermore questioning the idea of the civilians as a part of the discussion about the subject. The final chapter, “The trial of subject”, aims to bring the previous three parts together and once more point out the importance of a continuous discussion about the subjectivity in the modern day and circumstances.

Key words: subject, subjectivity, ethics, cyber-sphere, cyber-war, sovereignty, responsibility, civilian, cyber-operations

1. Uvod

Pitanje subjekta zaokuplja filozofe još od samih početaka filozofije. Subjekt je enigma koja je sigurno preokupirala misli ljudima i znatno prije Antike, jer je to pitanje koje je tako prirodno ljudima – što je osoba, kako je razumijemo i shvaćamo, tko je taj subjekt i koja je njegova funkcija, uloga, poanta. Što subjekt uopće čini subjektom?

Pitanje nije stalo na filozofiji, već unutar filozofije postoje brojne teorije o subjektu, fokusiraju se na različite aspekte i proučavaju subjekt iz različitih perspektiva. No i izvan je filozofije to pitanje itekako važno, pa se njim bave i pravnici, psiholozi, sociolozi, liječnici i razni drugi stručnjaci različitih disciplina, ne bi li subjekt napokon bio finalno smješten na svoje mjesto u svijetu, shvaćen i objašnjen do kraja. Definicije su bliske, ali ne i identične, i toliko pune detalja i različitih točki koje se uzimaju kao središnja karakteristika, da je vrlo diskutabilno hoće li se struke, pa i pojedinci unutar struka ikada usuglasiti oko jedne kompletne definicije.

Moderno je doba otežalo tu raspravu rađanjem virtualnog svijeta. Cyber-sfera otvorila je vrata pojavi nekog novog subjekta, subjekta 1.2, koji je zbog svoje virtualne prirode još veći misterij i problem nego realni subjekt u stvarnom svijetu. O cyber-subjektu se govori iako je upitno postoji li takvo nešto uopće i, ako postoji, kako postoji. Postojanje cyber-subjekta vezano je uz sferu koja nam je također poprilično strana i nerazumljiva iako smo je sami stvorili i kolektivnim djelovanjem svakodnevno pospješujemo njen eksponencijalan rast. Cyber-sfera je nedefinirana, rasprostranjena virtualnim svijetom suviše apstraktnim za standardne odrednice prostora, a naša je angažiranost unutar njega sve veća. Virtualni i stvarni svijet su zahvaljujući našem postojanju *online* sve isprepleteniji, a da mi pritom nismo uopće još sigurni kakvo je to naše postojanje *online*, i je li neki dio nas uistinu postao to nešto što bismo mogli zvati cyber-subjekt.

Moderno je doba je sve turbulentnije i sve brže, također zahvaljujući širokoj dostupnosti Interneta. Informacije nikada nisu bile više nadohvat ruke u svakom trenutku, izvještaje s drugog kraja planeta dobivamo izravno u trenucima događanja zahvaljujući *live-streamingu*, komuniciranje je među ljudima postalo toliko jednostavno i efikasno da je na neki način gotovo izbrisalo fizičku udaljenost među sudionicima i jednako nam je lako kontaktirati susjedu na našem katu kao i prijatelja na drugom kontinentu. Sve te pozitivne strane brze informiranosti i olakšane komunikacije naravno imaju i „drugu stranu medalje“. Informacije koje su se donedavno „kuhale“ u novinskim redakcijama i po čitav dan prije nego

odu u tisak za sljedeći dan, tada su imale vremena dobiti sve sastojke, ili barem dobar dio. Informacija koju bismo sutra dobili u novinama bila bi provjerena, sastavljena od onoliko detalja koliko ih se uspjelo stići skupiti, i svejedno doživljena kao preliminarna – u slučaju ičeg ozbiljnijeg i potencijalno opasnijeg čekale su se konferencije za novinare, i tek bi nam onda novinar dao kompletnu sliku s maksimumom dostupnih detalja.

Danas taj posao „radi“ bilo tko tko ima pametni telefon i pristup internetu, a to je na dobrom dijelu planeta – svatko. Rezultat je toga preplavljenost medija fragmentima izvučenima iz konteksta. Kraljevsko vjenčanje ili doček nogometne reprezentacije toliko opterete mreže, da telefoni postanu nefunkcionalni jer svatko ima potrebu dati svoj osobni doprinos izvještavanju s mjesta događaja. O pucnjavi u srednjoj školi doznajemo prije nego napadač uopće bude zaustavljen jer prepadnuti učenici sakriveni u ormarije manično *tweetaju*, šalju poruke obitelji, uploadaju svoj pogled na situaciju na Instagram i Facebook u strahu da neće više imati priliku vidjeti obitelj i prijatelje. Za teroristički napad doznajemo putem videa koje je slučajno snimio neki turist i koji je, shvativši što se događa, brže-bolje informaciju objavio na sve mreže.

S jedne strane to omogućuje hitnu intervenciju i nerijetko osigurava vrlo koristan dokazni materijal. S druge strane, te su informacije fragmentirane, viđene iz vrlo subjektivne perspektive, nedovršene i neobrađene, te kao takve, u moru jednako nefunkcionalnih komadića, predstavljaju rizik ne samo prelaska u dezinformaciju, nego u opasnu lavinu krivih informacija koja može uroditi masovnom histerijom i kaosom. Ti komadići informacija također su podložni manipulaciji, pa iako smo kao korisnici uvjereni da gledamo upravo ono što se uistinu događa, i prema tome formiramo svoj osobni sud, to ne mora uopće biti istina, i šira slika uz kontekst može drastično promijeniti informaciju koju dobijamo. Korisnicima je sve teže snaći se u tom brzom metežu virtualnog svijeta, i filtriranje kroz komadiće puzzlea da bi se složila što je moguće točnija slika sve je teži zadatak.

Jedna je od posljedica toga manipulacija strahom, vrlo primjetna na Zapadu od početka ovog stoljeća.. Terorizam je postao rak-rana, jer iako je kontroliranje ljudi strahom i prijetnjama oduvijek poznato, zahvaljujući brzom protoku informacija i lakom manipuliranju perspektivama, kontroliranje populacije strahom je postalo vrlo jednostavan i vrlo efikasan mehanizam. Terorističko je djelovanje zbog svoje kaotične prirode i načina rada i inače pravno-politička noćna mora, a preseljeno u cyber-sferu, čini se gotovo nerješivo. Terorizam uz sebe vuče još jedan paradoks – čini se da je on jedino kriminalno djelovanje u kojem

određena skupina pokušava preuzeti svu odgovornost, pa čak i tamo gdje je očigledno da je nema, dok pravni sustav uporno negira ta „priznanja“ i traži individualne krivce.

Odnos je terorističkih grupa prema ideji o subjektu u cyber-sferi tako vrlo zanimljiv fenomen i terorističko djelovanje putem Interneta, čak i kad ima vrlo realne i vrlo krvave rezultate u stvarnom svijetu, još jednom otvara pitanje subjekta uopće, a naročito načina postojanja subjekta *online*. No nije terorizam jedini konfliktni fenomen koji se preselio u cyber-sferu. Samo moderno ratovanje preselilo je jednim dijelom u virtualni svijet. Kad su u pitanju međunarodni konflikti u virtualnom svijetu, mijenjaju se definicije mnogih dosad utemeljenih pravnih pojmova, poput . napada, obrane, granice, teritorija, civila, odgovornosti, pa i same države. A ta se potreba za redefiniranjem ponovno vraća na pitanje samog subjekta, odnosno na pitanje može li u kontekstu cyber-ratovanja, pa i cyber-sfere uopće, postojati nešto toliko kompleksno i specifično kao što je subjekt.

Cilj ovog rada nije dati odgovore na ova pitanja niti regulirati pravne i političke sustave cyber-sfere. Taj izrazito kompleksan zadatak ipak će biti prepušten pravnicima, politici i vojsci. Umjesto pokušaja davanja odgovora na mnoga nemoguća pitanja, cilj je radije postaviti neka preciznija pitanja, čiji su odgovori možda i dalje nemogući, i pokušati promisliti problematiku subjekta u cyber-sferi iz filozofijske perspektive. To naravno ne znači isključivanje perspektiva drugih disciplina.. Prikupivši te perspektive, i promotrivši širu sliku iz perspektive filozofskog „koraka unatrag“, ideja je uočiti neke nove detalje i ukazati na njih, te postaviti nova pitanja koja bi možda mogla predstavljati barem korak unaprijed u pokušaju otkrivanja subjekta u cyber sferi, a naročito u kontekstu konflikta i ratnog stanja.

2. Ideja subjekta u filozofiji

2.1. Platonova spilja

Započeti raspravu o subjektivnosti nije jednostavan zadatak. Kroz povijest filozofije pojavile su se mnoge teorije o tome što subjekt uopće jest, po kojim ga kriterijima definirati i koja je njegova uloga u društvu. To, dakako, nije novo pitanje, jer su se antički filozofi itekako već bavili tom problematikom. Stoga ćemo pokušaj razumijevanja subjekta, kako onog stvarnog, tako u jednom trenutku i onog virtualnog, započeti upravo u antici, i to u metaforici Platonove spilje.

Platonova je spilja jedna od najslavnijih metafora koje u djelu „Država“¹ koristi. Platon opisuje spilju u kojoj žive ljudi od rođenja vezani. Do njih ne dopire svjetlo dana, tek svjetlo vatre koja gori iza njih, bacajući sjene na zidove pred njima. Njihovo razumijevanje svijeta temeljeno je samo na tim sjenama – svoj okoliš i predmete iz njega vide kao sjene, i za njih su sjene predmeti, a ne tek odrazi. Spriječeni od drugih oblika interakcije sa svijetom, njihovo je iskustvo, kao i oni sami, vezano samo uz spilju i sjene koje do njih dopiru².

Iako sjene nisu realnost, tim ljudima one to jesu, jer nemaju drugog iskustva. U tom prizoru već imamo koncept fenomena – kako raščlanjujemo jedan fenomen od drugog, kako ih prepoznajemo, koncipiramo i razumijemo, možemo li uopće vjerovati svom razumijevanju nekog fenomena? Čovjeku iz spilje nije nerazumljiva sjena, nego u trenutku kad se oslobodi iz nje izađe, nerazumljiv mu je onaj predmet čiju sjenu tako dobro poznaje³. Tek s vremenom provedenim u drukčijim iskustvima od onih na koja je navikao, čovjek iz spilje može raspoznati predmet u realnom svijetu kao pravi, i razumjeti da sjena nije bila realnost, nego samo privid, štoviše iskrivljeni privid. Na tom primjeru dobro vidimo da ono što mi shvaćamo kao realnost ne mora nužno biti utemeljeno u zbilji, no ipak, dok god ne otkrijemo i ne shvatimo širu sliku, ta će nam naša iskrivljena realnost biti jedina realnost koju imamo, jednako kao što čovjeku iz spilje nisu predmeti bili realna stvar, nego im je sjena predmeta bila realnost.⁴

¹ Usp. Platon, *Država*, Zagreb, 2009., Sedma Knjiga

² Usp. Santas, Gerasimos (ur.), *The Blackwell Guide to Plato's Republic*, Blackwell Publishing Ltd, 2006., Lear, Jonathan, „Allegory and Myth in Plato's Republic“

³ Usp. Ferrari, G. R. F.(ur.), *The Cambridge Companion to Plato's Republic*, Cambridge University Press, 2007., Denyer, Nicholas, „Sun and Line - The Role of the Good“

⁴ Usp. Jure Zovko, *Klasici Metafizike*, Zadar, 2008., Uvod, str.23-24

U pogledu odnosa realnog i virtualnog svijeta mi smo trenutno dobrim dijelom još u stadiju gledanja sjena u spilji. Teško nam je odvojiti ideju virtualnog svijeta od ideje onog realnog, jednim dijelom zato jer još nismo u potpunosti izašli iz jednog i ušli u drugi, a dijelom zato što su toliko isprepleteni da se uistinu čini da je jedan preslika drugog. No pitanje je koliko je virtualni svijet preslika realnog, a koliko mu je sjena, i to izdužena, deformirana sjena koja zapravo i ne nalikuje na svoj predmet.

Platon nas ovim prizorom uvodi, kako smo već rekli, u fenomenologiju, prikazujući način na koji ljudi shvaćaju fenomene oko sebe, kako stvaramo sliku o onom što je realno, i koliko ta slika zapravo može biti krhka i podložna utjecaju okolnosti iskustva. Realnost može biti samo privid, ali i dalje shvaćena i prihvaćena kao realnost. Isto se u tom kontekstu događa i sa samom subjektivnošću – ono što shvaćamo kao subjekt može biti samo sjena, a ono što opisujemo kao subjektivitet ništa drugo do privid.

Čak i pod novim svjetlom izvan spilje, upitno je možemo li nešto toliko apstraktno kao što je subjektivitet uistinu vidjeti jasnije od sjene. Sama količina teorija o subjektu koje su nastale nakon Platona, i koje nastaju i dalje, upućuje na to da nam subjektivitet možda i ne može biti jasniji od tek privida, te da su okolnosti naših različitih realnosti ono što određenim prividima daje težinu istine. To se naročito čini kao u slučaju s virtualnim svijetom i subjektivitetom u cyber-sferi. Moguće je da je u takvim okolnostima subjekt uistinu samo ono što se kontekstualno čini istinitim, a subjektivitet tek područje onog komadića sjene koji uspijevamo percipirati. Vrlo je diskutabilno može li virtualni subjekt ikad uistinu biti realni predmet koji je „izvan spilje“, ili je njegov domet ipak samo to da bude sjena na zidu.

Platon ipak svoje ljude iz spilje ne ostavlja zavezane da gledaju u sjene, nego ih oslobađa i pušta na svjetlo dana. Izlazak nije jednostavan – čovjek je prvo u potpunosti zaslijepljen intenzivnim svjetlom na koje nije naviknut. Postupnim navikavanjem lagano razaznaje obrise, povezuje ih sa sjenama koje su mu poznate, i malo po malo dolazi do zaključka da je njegova dotadašnja ideja o realnosti bila kriva. Također, otkrivši nove istine teško mu je ostaviti ostale u neznanju spilje, pa se vraća podijeliti nova otkrića. No ostalima u spilji njegove priče djeluju nemoguće i kao sanjarije, ismijavaju ga i ne vjeruju mu, jer ne žele izaći iz sigurnosti svog vlastitog svijeta i riskirati otkriće da njihova realnost ipak nije istinita. Vidjet ćemo poslije i kod Kanta sličan argument o tome kako je ljudima lakše i prirodnije ostati u sigurnosti naučenog, nego preispitivati realnost i prilagođavati se nekim novim uvjetima. Ipak, iako i Platon i Kant pokazuju razumijevanje za ljudski poriv za

ostajanjem u sigurnoj zoni privida (odnosno kod Kanta, samoskrivljene nepunoljetnosti, ali o tom više poslije), i kod jednog i kod drugog ipak je ključno odvažiti se na taj korak, da bismo uopće bili u mogućnosti biti aktivan dio realnog svijeta – odnosno da bismo uistinu postali subjekt.

2.2. Aristotel: formiranje subjekta

Dok se Platon kroz alegorije bavi čovjekom i njegovim odnosom s prirodom, Aristotel svijet opisuje na prilično sistematiziran način, koji uvelike podsjeća upravo na način na koji to rade egzaktne znanosti. U djelu „Fizika“ tematiku prirode, bića, a time i čovjeka, obrađuje gotovo enciklopedijski, počevši od objašnjavanja odnosa dijela i cjeline, preko bića kao međusobno različitih djelova cjeline, preko pitanja o bitku, do razmišljanja o naravi, kretanju i počelima i pokretalima uopće.

Prvenstveno odvaja pojmove bitka i bića, jer bitak razumije kao nešto što nema veličinu, te je stoga nedjeljivo, dok su bića ograničena i kao mnoga dio cjeline. Bića su spoznatljiva upravo zbog svoje ograničenosti, dok je ono što je neograničeno prema Aristotelu nespoznatljivo. Pojam koji je kod Aristotela značajan za razumijevanje bića je *promjena*⁵. Iako bića raspoznavamo svako kao zasebnu cjelinu, pa ih tako u kontekstu njih samih vidimo kao isto, također su određena kontinuiranom promjenom. Promjena je tako i značajka čovjeka, Aristotel na čovjeka gleda kroz prizmu *postajanja*, a njega vidi kao kontinuirani proces kojim iz jednostavnog bića dolazimo do složenog. Jednostavni element možemo razumjeti kao temelj i onu glavnu karakteristiku po kojoj jedno biće raspoznavamo od drugog, a postajanjem, odnosno promjenom, na taj se temelj nadograđuju sve druge karakteristike, koje su u principu sekundarne odrednice, i mogu, ali i ne moraju, biti trajne. Kao primjer Aristotel navodi neobrazovanog čovjeka:

„Kažem to ovako: Čovjek može postati 'obrazovan', ili 'neobrazovan čovjek' može postati 'obrazovan čovjek'. Jednostavnim dakle nazivam nastalo 'čovjek' i 'neobrazovano' – te i što svako od tih postaje – 'obrazovano' – isto tako jednostavnim. A složenim i ono što postaje i koje postaje, kad kažemo da 'neobrazovan čovjek postaje obrazovan čovjek'. A o tima ne kažemo samo kako štogod postaje 'ovo', nego i 'iz ovoga', kao 'iz neobrazovana' 'obrazovan', ali tako se ne kaže o svima. Jer ne govori se 'iz čovjeka je postao obrazovan'. Od

⁵ Usp. Barnes, Jonathan (ur.), *The Cambridge Companion to Aristotle*, Cambridge University Press, 1995.

stvari koje postaju – a o kojima kažemo da postaju kao jednostavne – jedno koje postaje preostaje dok drugo ne preostaje. Jer čovjek preostaje i biva i kad postaje 'obrazovan čovjek', dok 'neobrazovano' i 'ono koje je bez obrazovanog' ne preostaje ni jednostavno ni kao složeno.“⁶

Aristotel dalje o bićima razmišlja promišljajući prvo pitanje uzroka bića uopće, jer svaka kretanja prouzročena je nekim pokretačem, pa i svako biće kojem je glavna karakteristika upravo kretanje mora imati nekakvog pokretača. Pod pojmom *kretanje* ne misli se pritom samo na fizičku promjenu mjesta, nego na bilo kakvu promjenu neke karakteristike bića. Samo postojanje je dakle kretanje, jer se odvija u vremenu i protok vremena je već promjena, odnosno kretanje. U kontekstu kretanja Aristotel se bavi i samim pitanjima vremena i mjesta (odnosno prostora).

Dok je Platon u *Državi* proučavao čovjeka više u psihološkom i sociološkom smislu (njegov razvoj, suodnos s drugima i mjesto u društvu), Aristotel se u *Fizici* bavi sasvim drukčijim pogledom – formira čovjeka kao biće u vremenu i prostoru, i bavi se temeljnim odredbama tog bića. Ideja o kontinuiranoj kretnji, ali i dalje razumijevanju čovjeka, odnosno bilo kojeg bića, kao jedne koherentne cjeline koja je raspoznatljiva kao takva unatoč svojoj kontinuiranoj promjeni, značajna je i danas za razumijevanje čovjeka kao subjekta u kontekstu virtualne realnosti. Vidjet ćemo poslije koliko ta ideja kontinuirane promjene, ali i negiranja jednog aspekta bića promjenom u drugi (npr. promjena neobrazovan/obrazovan) može biti presudna za razumijevanje virtualnog identiteta u odnosu na stvarnog čovjeka u realnom svijetu.

2.3. Descartes: formiranje novovjekovnog subjekta

Razgovarati o teorijama subjektivnosti bez da se spomene René Descartes svakako ne bi imalo smisla. Njegov *cogito ergo sum* jedan je od najslavnijih zaključaka povijesti filozofije, i dio opće kulture i izvan granica filozofije, što je dodatan pokazatelj koliki je značaj Descartesa u razmišljanju o subjektu. Njegova filozofska sumnja i finalni dokaz o vlastitom postojanju kroz razmišljanje toliko su jako odjeknuli, da većina ljudi „van struke“ filozofije kad se spomene problematika subjektivnosti automatski pomisle na Descartesa i njegovo „Mislim dakle jesam.“

⁶ Aristotel, *Fizika*, Zagreb, 1987., str. 20

Descartes je poznat i kao otac moderne filozofije. Rano je iz vlastitog iskustva⁷ shvatio da unaprijed dane istine, koje naučimo iz druge ruke, ne moraju uopće biti istinite. Teze koje učimo u školi kao apsolutno točne nekad budu naknadno opovrgnute, ono što nam je razumljivo kao „istina“ unutar jedne kulture u nekoj drugoj kulturi može djelovati sasvim apsurdno. Ljudi s vremenom dolaze do novih spoznaja koja nerijetko rezultiraju potpunim preslagivanjem sustava istinitosti. Descartes je svega toga svjesan i zaključuje kako je naša individualna dužnost ne prihvaćati „istine“ , dok ih vlastitim razumom ne preispitamo.⁸

Takav egzaktno znanstveni pristup je ono po čemu Descartes pripada modernitetu. Također, taj je princip karakterističan i za periode velikih promjena. U kontekstu značajnih novih okolnosti, najbolji mogući način za razumijevanje svijeta u tom novom kontekstu i usustavljivanje novih paradigmi i načina funkcioniranja upravo je preispitati sve dotadašnje pretpostavke, staviti ih pod novo svjetlo, krenuti od negacije svake od dotad prihvaćenih „istina“, i jednu po jednu pokušati postaviti u novi sustav. Pojava interneta i razvoj virtualnog svijeta jedna je takva velika promjena okolnosti i sustava, u kojoj je za razumijevanje novog svijeta Descartesova metoda sumnje i preispitivanja možda i najpouzdanija, jer je definitivno jasno da u virtualnom svijetu opće prihvaćene društvene konvencije realnog, razumijevanje međuljudskih odnosa, pa čak i pitanja realnosti i psihologije jednostavno više ne vrijede.

Za definiranje subjekta u cyber-sferi, Descartes opet postaje relevantan. U njegovoj filozofiji pitanje o „ja“ je jedno od ključnih točki preispitivanja, i nova polazišna točka nakon stadija sumnje. Isto pitanje se postavlja i u pitanju cyber-sfere. Tko je tamo „ja“ i kako možemo biti sigurni u to „ja“ *online*? Descartesov model sumnje polazi od tog da sve što vjerujemo da je istinito može zapravo biti nekakva varka. Zavaravati nas može sve, od vanjskog svijeta do vlastitih osjetila. Svima se barem jednom dogodilo da zaspu na jednoj ruci i probude se bez osjeta u njoj – no to što je privremeno ne osjećamo, ne znači da nemamo više ruku, štoviše, neugodan osjećaj naglog naviranja krvi u nju kad se vratimo u prirodan položaj, vrlo brzo će nam izrazito intenzivno ponovo dokazati da je ipak imamo. No Descartes je svjesan da je naša procjena vrlo podložna raznim utjecajima koji nas mogu navesti na krive zaključke, pa počinje od preispitivanja svega onog što smatra istinitim, i pokušava sigurnijim metodama preispitati istinitost. Na taj način postupno dolazi do tog da je jedino što može sa sigurnošću ustvrditi je da on u tom trenutku misli, a s obzirom da

⁷ Usp. Rodis-Lewis, Geneviève, *Descartes' life and the development of his philosophy* u: Cottingham, John (ur.), *The Cambridge Companion to Descartes*, Cambridge University Press, 1992.

⁸ Usp. Descartes, *Discours de la méthode*, Éditions Gallimard, 2009.

djelatnost mišljenja zahtijeva nekakav subjekt mislitelja, onda on i postoji – *mislim, dakle postojim*⁹.

Descartesu je subjekt tako primarno prostor samosvijesti i mentalnog djelovanja. To je za analizu subjekta u kontekstu virtualnog, a ne realnog svijeta vrlo značajna točka, jer u prostoru virtualnog svijeta ne možemo se fokusirati na to da subjekt pokušamo vezati uz određeno tijelo kao jedinicu djelovanja, nego moramo pronaći neki drugi temelj formiranju. Zapravo, odnos virtualno-realno neodoljivo vuče natrag prema Descartesovom dualizmu duše i tijela. Descartes u svojoj analizi u *Discours de la méthode* konstatira da su duša i tijelo međusobno odvojeni entiteti. Temelji to na činjenici da ono što danas poznajemo kao autonomni dio ljudskog organizma funkcionira u potpunosti neovisno o našoj svijesti. Neovisno o čemu razmišljamo, naše srce i dalje pumpa krv u krvotok, naša pluća i dalje cirkuliraju kisik. Dapače, čak i kad bismo se mislima fokusirali na rad nekog od tih organa, ne bismo mogli puno toga promijeniti. Ne možemo mentalno natjerati srce da prestane s radom ili da promijeni ritam, kao što i disati možemo prestati samo na kratko, prije nego nas tijelo refleksom natjera da ponovo prodišemo, neovisno o volji tijela. Dakle, duša i tijelo su kod Descartesa povezani, ali ne jedno. Ista se teza može prenijeti i na cyber-sferu, odnosno na odnos virtualnog i realnog subjekta – virtualna osoba i realna osoba su povezane, ali ne nužno jedna jedinstvena osoba, i jedna može postojati neovisno o drugoj, o čemu više riječi poslije.

2.4. Hobbes: subjektivnost i suverenost

Thomas Hobbes pojavljuje se u povijesti filozofije kao značajno ime u sferi filozofije politike. No ni u svom slavnom „Levijatanu“ Hobbes ne uskače odmah u društvene odnose i političku problematiku, nego se prva cjelina bavi upravo razumijevanjem čovjeka kao jedinke. Ta analiza počinje promišljanjem prvenstveno o osjetu, da bi putem analize predodžbi, jezika, osnova voljnih kretanja i ciljeva došao do pitanja moći, vrijednosti i dostojanstva, te onoga što on naziva prirodno stanje. Prirodno stanje vidi kao rat svih protiv svih – svaki pojedinac potencijalna je opasnost drugom pojedincu jer njim vladaju prirodni nagoni i egoizam. Na svakom je stoga da se osobno osigura ili nametne svoju volju, bilo

⁹ Usp. Markie, Peter, *The Cogito and its importance*, u: Cottingham, John (ur.), *The Cambridge Companion to Descartes*, Cambridge University Press, 1992.

putem fizičke sile, bilo nekakvom lukavštinom. Prirodno stanje¹⁰ je stanje kontinuiranog straha za vlastitu egzistenciju, i kao takvo izrazito nepogodno za život, pa je ljudima u cilju naći nekakvo alternativno rješenje.

Iz tog je vidljivo da Hobbes svoju filozofiju politike temelji na razumijevanju individue, da bi tu osobu polako smjestio u odnos s drugima putem društvenog ugovora, te na tim međusobnim odnosima utemeljio državu kao veću cjelinu, ali jedinstvenu. Hobbes u duhu svog vremena čovjeka gleda mehanicistički, i analizira ga kao mehanizam, koji shvaćen samostalno (u prirodnom stanju) ima svoje principe akcije i reakcije, a ulaskom u društvo postaje dio većeg mehanizma. Odnosno, „pod utjecajem Descartesa, svijet je shvaćen mehanicistički, stoga i Hobbes promatra čovjeka kao mehanizam koji agira i reagira“.¹¹

U kontekstu današnjeg vremena i promišljanja o odnosu osoba unutar cyber-sfere, Hobbseovo uspostavljanje države kao jedne jedinstvene cjeline nije nimalo zastarjelo. Naprotiv, pitanje se odnosa pojedinac – država i prijenosa odgovornosti s pojedinaca na jedno jedinstveno tijelo suverena ponovo otvara, samo ovaj put u virtualnom području. Cyber-sfera relativno je mlado područje, ali eksponencijalno raste i nije geografski ograničeno. Sve je napućenija, a „pravila ponašanja“ još uvijek nisu jasna. Virtualni stanovnici cyber-sfere trenutno se nalaze upravo u Hobbsevom trenutku rata svih protiv svih, čeka se virtualni društveni ugovor.

Hobbes trenutak rađanja države vidi u trenutku kada strah pojedinca spram svakog drugog pojedinca eskalira u potrebu za univerzalnom zaštitom efikasnijom od puke samoobrane. Anksioznost zbog budućnosti, pa čak i one najbliže (npr. čovjek koji bere jabuke sad, jer zna da će poslije biti gladan, u stanju je anksioznosti već zbog tog što mora osigurati te jabuke, da mu ih netko drugi ne ukrade¹²) vodi do tog da ljudi počinju težiti nekom dugotrajnijem i stabilnijem rješenju. To rješenje Hobbes vidi u obliku homogeniziranog straha – veliki strah „od mača“ (odnosno strah od kazne) zamijenio bi sve manje individualne strahove pojedinaca prema svim drugim pojedincima koji ga okružuju i predstavljaju potencijalnu opasnost. No da bi to moglo funkcionirati, pretpostavka je da će na takav sustav kazne pristati svi pripadnici društva, bez iznimke. Pripadanje zajednici uz sve

¹⁰ Više o prirodnom stanju usp. Hoekstra, Kinch, Hobbes on the Natural Condition of Mankind, u: Springborg, Patricia (ur.), *The Cambridge Companion to Hobbes's Leviathan*, Cambridge University Press, 2007.

¹¹ Goran Sunajko, *Metafizika i suverenost*, HFD, Zagreb 2015., str. 225.

¹² Usp. Ryan, Alan, Hobbes's political philosophy, u: Sorell, Tom (ur.), *The Cambridge Companion to Hobbes*, Cambridge University Press, 1996., str. 219.

prednosti i osiguranje koje s tim idu, svaki pojedinac plaća odustajanjem od svoje autonomije i potpunim prepuštanjem odgovornosti jednoj osobi¹³. Taj čin ujedinjenja mnoštva u jednu osobu Hobbes smatra rođenjem države, odnosno Levijatana. Levijatana i državu Hobbes ovako definira: „Jer preko te ovlasti, koju mu je dao svaki pojedinačni čovjek u državi, on ima na raspolaganju toliko moći i snage da tim zastrašivanjem bude u stanju uskladiti volje svih njih prema miru kod kuće i prema uzajamnom pomaganju protiv neprijatelja izvana. U njemu se sastoji bit države; ona je (da je definiramo) osoba, a tvorac njezinih radnji postao je velik broj pojedinaca, i to posredništvom uzajamnih sporazuma, s ciljem da koriste snagu i sredstva svih, onako kako to budu smatrali za mir i zajedničku obranu.“¹⁴

Iz tog je citata vidljivo da Hobbesa ne brine samo odnos individua unutar jednog teritorija, nego i opasnost „izvana“, njegova država definirana je, između ostalog, i teritorijalno, granicama.

Kako to preseliti u virtualni svijet, u kojem geografske granice očito ne mogu postojati? Suverenitet država u realnom svijetu uključuje i nepovredivost granica, a te su granice fizičke i jasne. Nasilno prodiranje kroz njih ili negiranje njihovog postojanja smatra se povredom suvereniteta i razlogom za legitimnu samoobranu države. Suverenitet u cyber-sferi nije jasno definiran, i vrlo je teško odrediti granice unutar virtualnog svijeta. Serveri web-stranica mogu se nalaziti bilo gdje, i domena s koje se nekakav napad dogodio ne bi trebao nužno značiti odgovornost države u kojoj se server fizički nalazi. Kako bi se države onda trebale postaviti u kontekstu „cyber-suvereniteta“, i mogu li se državni zakoni prenijeti na virtualni svijet? Kolika prava i ovlasti nad internetom može imati vladar realnog svijeta, i na koji način?

Hobbesova država kroz vladara postaje jedna osoba. Država, odnosno vladar, nosi odgovornost odlučivanja o zakonima i kaznama, obrazovanju, prihvatljivim i neprihvatljivim ponašanjima. Također je odgovoran za odlučivanje u ratu i međunarodnim odnosima. Suprotstavljanje odluci vladara nije dozvoljeno, jer su ljudi ulaskom u društvo pristali na tu

¹³ više o Hobbesovom usustavljanju odnosa osoba i predstavnika Skinner, Quentin, *Hobbes on Persons, Authors and Representatives*, u: Springborg, Patricia (ur.), *The Cambridge Companion to Hobbes's Leviathan*, Cambridge University Press, 2007.

¹⁴ Thomas Hobbes, *Levijatan*, Zagreb, 2013., str. 122-123.

predaju moći. Dakle vadar je taj koji ima finalnu riječ u upravljanju državom, i u smislu unutarnjeg uređenja, i u smislu međunarodnih odnosa¹⁵.

Ukoliko taj princip prenesemo na cyber-sferu, prvo pitanje koje se postavlja je što bi značio suverenitet online. Na koji način nešto što je u realnom svijetu primarno određeno povijesno-geografskim elementima preslikati u virtualni svijet, u kojem ta određenja ne moraju nužno imati jednaku vrijednost? Također, pripadaju li cyber-subjekti istoj državi kojoj pripadaju i odgovarajući subjekti u realnom svijetu?

Hobbesov idealan vladar je apsolutist, to ga čini i nositeljem odgovornosti u državi. Sve institucije, svako djelovanje je pod njegovim nadzorom. Pojedinci imaju osobnu odgovornost jedino u smislu poštivanja sustava i adekvatnog djelovanja, no ukoliko oni tu odgovornost ne ispune, vladar je taj koji odlučuje o kazni, dakle preuzima odgovornost za ispravljanje pogreške u sustavu i osiguranje da sustav, odnosno država, i dalje funkcionira prema ugovoru, odnosno zakonu. Pojedinaac koji nije spreman na taj način predati odgovornost riskira to da ultimativno bude isključen iz sustava, odnosno društva.

Cyber-sfera područje je izrazite individualizacije i prostor za svojevrsno potpuno oslobađanje i anarhiju. Na neki način, ona je povratak u prirodno stanje. Prenosjenje Hobbesovog sustava u cyber-sferu značilo bi kraj tog potpunog individualizma *online* i prihvaćanje prepuštanja kontrole nekom nadležnom. I dok većini ljudi koncept države kao finalne instance odgovornosti u realnom svijetu nije nimalo problematičan, u cyber-sferi vidimo upravo suprotnu tendenciju, i negodovanje nad pokušajima državne regulacije *online* djelovanja. S druge strane, u kontekstu konfliktnih situacija ili oružanih sukoba među državama, kontrola nad cyber-sferom i cyber-operacijama uistinu više liči na Hobbesov apsolutistički sustav, nego na demokraciju. U cyber-ratovanju upravo je država ta koja preuzima odgovornost za svako online-djelovanje, ali preuzima i potpunu kontrolu nad čitavim sustavom. Autonomija samih civila u cyber-sferi u kontekstu cyber-ratovanja vrlo je upitna, ali o tome više riječi poslije.

¹⁵ Za detaljniji uvid u problematiku autoriteta, usp. Simon, Robert L. (ur.), *The Blackwell Guide to Social and Political Philosophy*, Blackwell Publishers Ltd, 2002., Simmons, A. John, "Political Obligation and Authority"

2.5. Kant: *Sapere aude!*

Prikazavši dosad nekoliko filozofskih teorija koje bi nam mogle pomoći u razmatranjima o subjektu i subjektivitetu u cyber-sferi, dolazimo do još jedne ključne odrednice, a to je definiranje subjekta preko njegovih činova i razumskog djelovanja koje je u pozadini tog djelovanja. Uzimanjem te dimenzije subjekta u obzir ulazimo više u polje etike, gdje nam svakako može pomoći Immanuel Kant.

U svom tekstu „Što je prosvjetiteljstvo?“¹⁶, Kant iznosi nekoliko teza koje su i dalje relevantne i u realnom svijetu, ali mogu biti posebno relevantne u kontekstu naših prvih koraka u razumijevanju i stvaranju društva u online-sferi. Prva od tih teza je da je ljudima vrlo zgodno biti nezreli (odnosno kako Kant kaže – nepunoljetni). Nezrelost čini mjehurić opuštenosti, mira i sigurnosti (makar lažne sigurnosti) u kojem se čovjeku lako sakriti od odgovornosti i problema stvanog svijeta. Kant objašnjava kako je jasno da je ljudima najlakše prepustiti čak i brigu o sebi drugim ljudima oko sebe, npr. liječnicima, raznim savjetnicima, pomagačima itd., nego se sami time zamarati. Zbog toga je izglednije da će iz takvog stanja izaći društvo u cijelosti, nego pojedinac kojem su takve navike ugodne. No kao što i u Platonovoj spilji sjene nisu stvarnost, nego tek odraz stvarnosti, tako ni plutanje u mjehuriću nezrelosti nije pravi, svjestan život, nego infantilno puzanje kroz život. Da bi osoba mogla uistinu svojim djelovanjem biti individualna, samosvjesna osoba, treba preuzeti odgovornost za sebe i djelovati¹⁷.

Prelazak čitavog društva iz stanja lagodnog, nesvjesnog plutanja u svjesno i odgovorno djelovanje naravno nije pitanje jednog trenutka osvještavanja, nego proces koji zahtijeva vrijeme i kolektivnu osviještenost. Prosvjetiteljstvo Kant vidi kao čovjekov izlazak iz samo-skrivljene nepunoljetnosti, odnosno kao proces osvještavanja nužnosti vlastitog odgovornog djelovanja. Princip se odgovornosti¹⁸ u Kanta temelji na volji i to onoj koja omogućuje kategorički imperativ: „djeluj tako da možeš htjeti da maksima tvoje volje može vrijediti kao princip općeg zakonodavstva“. Ovaj moralni iskaz zapravo znači princip odgovornosti prema kojemu subjekt ne bi trebao djelovati u suprotnost s vlastitim načelima koje je postavio i koja se u konačnici primjenjuju na njega. Iako je obrazovanje društva vrlo

¹⁶ Kant, Immanuel, *Pravno-politički spisi*, Zagreb, 2000.

¹⁷ Usp. Schneewind, J.B., *Autonomy, obligation, and virtue: An overview of Kant's moral philosophy*, u: Guyer, Paul (ur.), *The Cambridge Companion to Kant*, Cambridge University Press, 1992.

¹⁸ Više o Kantovom kategoričkom imperativu u: Hill, Thomas E. Jr (ur.), *The Blackwell Guide to Kant's Ethics*, Blackwell Publishing Ltd., 2009.

značajno da bi proces „osamostaljivanja“ bio moguć, Kant upozorava i na opasnost stjecanja predrasuda, i važnost samostalnog kritičkog razmišljanja. To ne znači apsolutnu slobodu djelovanja. Restrikcije su naravno nužne, i nisu sve restrikcije automatski loše, dapače, da bi društvo moglo funkcionirati, moraju postojati, uostalom do racionalnosti i važnosti pojedinih restrikcija vrlo lako dolazimo upravo kritičkim razmišljanjem. Kant to i dodatno pojašnjava tezom da je najlakši način za testiranje prihvatljivosti neke društvene mjere upravo taj da si postavimo pitanje bismo li si, kao društvo, i sami postavili takav zakon.

Kantova etika poznata je po tom da u centar postavlja samosvijest i odgovornost i spram sebe i spram okoline. Polazišno pitanje tako ne smije biti želimo li nešto učiniti, nego bismo li mogli prihvatiti kad bi i drugi to činili. Takvim pristupom tjeramo se na objektivnost u procjeni, i otežavamo si izmišljanje izlika i prebacivanje odgovornosti negdje drugdje. Dužnost nam je biti svjesni svog djelovanja i utjecaja tog djelovanja na okolinu. Prihvatanjem takvog etičkog pristupa, društvo se u cijelosti pomalo dovodi u „stanje punoljetnosti“, odnosno postaje odgovorno, razumno društvo.

U kontekstu online-sfere moglo bi se reći da smo ponovo u tom stanju samouzrokovane nepunoljetnosti iz kojeg se tek trebamo usuditi izaći. Tek nas čeka ponovno učenje i razumijevanje sustava, tek smo u stadiju prilagođavanja na nove uvjete i principe. Kantov kategorički imperativ u kontekstu cyber-sfere može se učiniti manje relevantnim, jer se na prvi pogled čini da posljedice online-djelovanja ne mogu biti baš toliko problematične da bismo se zamarali preispitivanjem. No kad se uzme u obzir da online-djelovanje, a naročito cyber-operacije u kontekstu oružanih sukoba, imaju itekako velik utjecaj na stvarni svijet (od pojedinca, preko društva u cijelosti, pa čak i na prirodu), kategorički imperativ ne samo da ostaje, nego je više no ikad važno da ga se shvati i prihvati upravo kao *imperativ*.

2.6. Husserl: pojava i realnost

Dosad smo prikazali nekoliko pogleda i teorija o tome što je osoba, što je biće uopće, koja bića smatramo subjektima i koje je njihovo mjesto u svijetu. No za raspravu o subjektu u kontekstu nekog svijeta izvan ovog realnog, materijalnog, nužno se zapitati o realnom svijetu uopće, i još jednom staviti realnost bića i načine postojanja pod upitnik. S obzirom da se Edmund Husserl u djelu *Ideje za čistu fenomenologiju i fenomenologijsku filozofiju* između ostalog bavi i upravo tim pitanjima, njegovo razmišljanje o realnosti (Životnom svijetu) i našim percepcijama realnosti svakako je neizostavno za ovu raspravu. Sam Husserl već u uvodu kaže „Najradije bih izbacio i vrlo opterećenu riječ realno samo kada bih imao neku odgovarajuću zamjenu.“¹⁹ Već iz te je rečenice jasno koliko je pojam realnosti problematičan, a Husserl čak nije ni imao problem virtualne realnosti i paralelne egzistencije ljudi u realnom i virtualnom svijetu kao dodatnu komplikaciju. Unatoč tome, njegovo preispitivanje realnosti dobra je uvertira za daljnje pokušaje objašnjavanja realnosti cyber-sfere.

Husserl se prvenstveno želi osloboditi ograde empiricizma i egzaktnih znanosti. Iako ne negira njihovu relevantnost u odgovarajućim jasno odvojenim domenama (u smislu deskripcije iskustveno dostupne prirode), smatra da je problematično prihvatiti da iskustvo preuzme funkciju objašnjenja. Naime, iskustvo je podložno raznim vanjskim čimbenicima, i ne mora nužno biti dostatno za razumijevanje neke pojave. Dapače, iskustvo neke pojave može biti samo jedan manji element cjeline određene pojave, ili čak može biti u potpunosti pogrešna interpretacija. Prirodni nam se svijet daje kroz prizmu onoga što naziva kontinuirana mnogostrukost, a to znači na način da stvari spoznajemo s obzirom na heterogenost naših osjetila koja su promjenljiva, stoga je cilj dospjeti do tla apodiktičke izvjesnosti invarijantne biti predmeta koja ostaje nepromijenljiva.

Još jedan značajan element za daljnju raspravu je i razdvajanje samostalnog od nesamostalnog predmeta. Samostalne biti Husserl naziva konkretum, a nesamostalne apstraktum. Također uvodi i pojam individuum, koji definira kao „ovo-tu, čija je stvarna bit neki konkretum.“²⁰ Ti će odnosi biti važni kasnije za razdvajanje virtualnog (fenomen) od realnog (pojava) subjekta, o čemu više poslije. Još jedna važna distinkcija upravo u tom kontekstu bit će i distinkcija materijalne stvari i duše, gdje Husserl objašnjava da je duša

¹⁹ Edmund Husserl, *Ideje za čistu fenomenologiju i fenomenologijsku filozofiju*, Breza, Zagreb, 2007., str. 8

²⁰ Ibid., str. 36

fundirana u materijalnoj stvari, iako su te dvije „varijante“ zapravo različite regije bitka, i primjer su preplitanja, pa i djelomičnog preklapanja različitih fenomena.

No vratimo se trenutno na probleme empirizma kao metode razumijevanja realnosti. Husserl empirizam vidi kao svojevrsan skepticizam, gdje se svako razumijevanje Descarteovski negira, preispituje i podvrgava vlastitoj iskustvenoj spoznaji. Upravo u toj vlastitoj spoznaji Husserl uočava problem – ona nikako ne može biti općenita, jer je nužno individualna, i čak i egzaktne znanosti istinitom smatraju tek onu tezu koja je više puta dovela do istog iskustva, odnosno do istog rezultata. Iako je takva metoda pokusa i danas važeća u prirodnim znanostima, ona je ipak nedostatna za dolaženje do bitnog razumijevanja stvarnosti. Također, postoje mnogi aspekti stvarnosti koji jednostavno nisu dokazivi ovom metodom, npr. bilo koji doživljaj koji ima emocionalnu komponentu. Husserl stoga određuje da– „zbijski je svaki iskaz koji ne čini ništa drugo nego daje izraz takvim danostima putem čiste eksplikacije i značenja koja su im točno primjerena (...).“²¹ Ovaj princip uključuje i princip prirodnjaka da u svom istraživanju zahtijevaju iskustvenu dokazivost kao kriterij istinitosti, ali i šire, „fizički nedokazive“ fenomene koji su ipak dio realnosti.

Husserl, kako smo već spomenuli, ne umanjuje vrijednost doživljaja, samo doživljaj shvaća puno šire nego to čine empiricisti. U odjesečku 27 – „Svijet prirodnoga stava: Ja i moj okolni svijet“ uzima u razmatranje upravo doživljaj. Prvenstveno spominje neposredno iskustvo svijeta oko sebe – predmete iz našeg okoliša doživljavamo primarno iskustveno, oni su dio naše realnosti u smislu o nama neovisnog postojanja u našoj neposrednoj okolini. S nekim predmetima imamo interakciju, s nekima ne, ali smo ipak svjesni njihove egzistencije, funkcije, suodnosa u okolini. Također, Husserl naglašava da nije nužno da se neko biće nalazi u našoj neposrednoj blizini, odnosno kako kaže „zamjedbenom polju“, da bismo ga razumijevali kao zbijsko. Znanje o tim bićima koje su van područja naše izravne observacije Husserl objašnjava kao gotovo podsvjesno, nepojmovno. Tek svjesnim usmjeravanjem pozornosti dolazimo do jasnog zrenja. Također, spominje horizont neodređene zbijsnosti, čije si predmete možemo manje ili više uspješno predočiti, i koji čini vanjski svijet. Iako s njim nismo u izravnom kontaktu kao s neposrednom okolinom, svjesni smo njegove realnosti. Područje te neodređene okoline je zapravo beskonačno, jer iako smo svjesni nekakvog horizonta, on je predalek i mutan da bi ga se moglo jasno odrediti.

²¹ Ibid., str. 52

U područje te beskonačne, neodređene okoline ne spada samo realnost sadašnjosti u smislu razumijevanja fizičke okoline. Protok vremena također je dio neodređene zbiljnosti. Svijet u kojem živimo, koji doživljavamo kao područje realnosti, ima i svoju realnu budućnost. Štoviše, Husserl tu budućnost vidi kao poznatu i nepoznatu, živu i neživu. Svijet se stalno sadržajno mijenja, i mi smo ga kontinuirano svjesni iz perspektive jednog od njegovih elemenata. Također, svijet pri tom ne znači samo materijalnu stvarnost, nego i sve apstraktnije odnose i vrijednosti koje u njemu egzistiraju. Neke od tih vrijednosti su također podložne promjeni, kako izvanjskoj, neovisno o nama, tako i o promjeni koja je zapravo posljedica promjene naše vlastite percepcije²² ili dojma, pa s vremenom dolazi do promjene nekih stavova, odnosa ili čak generalnih principa.

Uočavamo da iako Husserl ne smatra egzaktni, materijalistički pristup dovoljno sveobuhvatnim da bi se moglo razumjeti realnost, ipak materijalne elemente ne negira. Za razliku od Descarteovskog principa sumnjanja i preispitivanja apsolutno svega izvanjskog, on vanjske materijalne objekte doživljava jednostavno kao takve – izvanjske, materijalne i egzistirajuće neovisno o našoj refleksiji o njima. On prihvaća materijalnost realnog svijeta, samo je ne smatra dosegom istine, nego u observaciji ide dalje i uključuje i nematerijalno²³. Realnost tako postaje promjenjiva, samim tim apstraktnija. Okolni svijet je podložan reinterpretaciji, a realnost fluidna. Uzimajući u obzir kompleksnost spontanosti svijesti, Husserl realnost vidi kao kronično preoblikovanje uzrokovano upravo tom spotanošću. Realitet se u tom pogledu može shvatiti kao aktualnost okolonosti i shvaćanja, u vječnoj blizini promjene. Realno je ono što nam je u tom trenutku razumski prihvatljivo kao realno, ali ta realnost nije ograničena materijalnim aspektima svijeta, niti strogo fiksni koncept. U tome je i bit Husserlova pojma fenomena koji nagovještava promjenu ne samo u tradiciji fenomenologije koja je fenomen određivala pukom empirijskom pojavom (od Platona do Kanta), nego i u razumijevanju svijeta koji se sve više daje na fenomenalan način. To pak u Husserlovu razumijevanju fenomena znači sliku koja je utemeljena putem intencionalne svijesti. Predmet svijesti (fenomen) ne mora biti ništa empirijsko (realno), dovoljno je da bude posviješćeno kao idejni predmet. Svijet nakon Husserlova utjecaja više nije isti jer se otvaraju goleme mogućnosti razumijevanja svijeta kao slike, kao predstave opažajuće svijesti, čemu svjedoči i ogroman zamah fenomenologije, od Heideggera nadalje. Heidegger će zato

²² Usp. Barry Smith; Smith, David Woodruff (ur.), *The Cambridge Companion to Husserl*, Cambridge University Press, 1995.

²³ Usp. Sunajko, Goran, Ontologija »objektivnog neprijatelja« kao nebića: Hannah Arendt i Carl Schmitt, *Filozofska istraživanja* 36(2016)4, str. 753-774.

odrediti fenomen kao onaj koji se, za razliku od pojave, pojavljuje na samome sebi.²⁴ Takvo razumijevanje realnosti otvara prostor interpretaciji virtualne realnosti online-sfere kao fenomena koji ne mora imati doticaj s nečim stvarnim što bi mu stajalo u temelju. Fenomen se odljepljuje od empirijske zadanosti i funkcionira kao slika. Odnosno, time se on daje u vidu jednog oblika realnosti, te razumijevanju istinitosti realnog i virtualnog svijeta kao dvaju odvojenih, ali povezanih sfera realnosti, gdje preduvjeti istinitosti unutar jedne ne moraju nužno negirati različite preduvjete istinitosti unutar druge sfere.

Iako empiristima spočitava temeljnije spoznaje na neposrednom iskustvu, Husserl, kako smo već spomenuli, ipak ne isključuje doživljaj kao važan element. Važno je razlučiti da doživljaj i iskustvo naravno nisu sinonimi. Doživljaj Husserl definira kao „svijest o nečemu“. Upravo u tom je ključna razlika u odnosu na iskustvo na kakvom se temelje egzaktne znanosti, doživljaj iste stvari naime može biti dijametralno suprotan u dva različita trenutka. Čak i preispitivanje neke stvari može dovesti do promjene u doživljaju. Također je važno uzeti u obzir da se ovdje ne radi o doživljaju u užem smislu psihološke/emocionalne reakcije, nego o doživljaju prema samim bitima stvari. Husserl opseg doživljaja širi na sve ono što se može naći u struji svijesti, intencionalno ili ne. Intencionalni doživljaj je pod-kategorija doživljaja koja označava usmjerenost subjekta na neki objekt.

Doživljaj, za razliku od iskustva, nikad nije razumski zaokružen – ne zamjećujemo ga do kraja i njegova cjelina nije u potpunosti razumski shvatljiva, jednako kao što je bio slučaj s horizontom neodređene zbiljnosti. Sama granica doživljaja također je tek mutni horizont u daljini, jer doživljaj nije dovoljno mala instanca da bismo ga mogli precizno ograditi i uobličiti. S obzirom na njegovu kompleksnost, možemo se svjesno fokusirati tek na u danom trenutku značajne elemente, ali poput bilo kojeg složenog organizma, ti elementi nisu neovisni ni izolirani. Na njih utječe čitav niz drugih elemenata, koje je, u kontekstu doživljaja, jednostavno nemoguće u cijelosti uočiti i vidjeti kao jasno razgraničen i definitivan sustav. Doživljaji se također prelijevaju jedan u drugi, i imaju međusoban utjecaj, pa je cjelokupan doživljaj jedne osobe zapravo nepregledna mreža međusobno povezanih doživljaja.

Takav pristup doživljavanju realnosti, odnosno realnosti stvorene kroz kompleksne sustave intencionalnog i neintencionalnog doživljavanja, zahvalan je za daljnju raspravu o mogućoj realnosti virtualnog svijeta. Iz svega toga također je jasno da egzistencija našeg

²⁴ Usp. Martin, Heidegger, *Bitak i vrijeme*, Naprijed, Zagreb 1985.

svijeta, realnog u kontekstu svih tih idejnih i doživljajnih percepcija i racionaliziranja, ne isključuje mogućnost egzistencije nekog drugog svijeta, svijeta izvan našeg svijeta, koji bi u nekim okolnostima također bio realan. Husserl objašnjava da se zbiljski svijet „nadaje kao specijalni slučaj raznovrsnih mogućih svjetova i okolnih svjetova koji sa svoje strane nisu ništa drugo nego korelati bitno-mogućih izvedbi ideje iskušavajuće svijesti s više ili manje uređenim iskustvenim sklopovima.“²⁵ Priroda zapravo svoju egzistenciju realizira upravo u korelaciji sa svijesti, a „svaka realnost bivstvuje putem davanja smisla.“²⁶ Davanje smisla još je jedan faktor razumijevanja realnosti koji će poslije biti ključan u odnosu stvarnog (u smislu fizičkog) i virtualnog svijeta. Jer fenomen je za Husserla nastao kao pročišćen od stečenog smisla u regiji čiste svijesti, gdje je, oslobođen dosadašnjih psihologizama, zaživio kao čist fenomen, kao *noema* koja nam predstavlja nov smisao.

Za kontekst rasprave o subjektivnosti (naročito u perspektivi virtualnog svijeta), interesantno je i Husserlovo razmišljanje o „čistom Ja“. Redukcijom na niz događaja, čini se da to Ja postaje isključeno. Ipak, neko Ja je vječno prisutno, te nije samo kontinuirani „tupo trajući“²⁷ doživljaj. Također, to Ja pripada i budućnosti, dakle i svim budućim doživljajima. To Ja stoga mora biti nešto identično, u biti nepromjenjivo i isključeno od individualnih elemenata stvarnog svijeta (iako mu doživljaji tih elemenata pripadaju jer ono ne postoji bez empirijskoga Ja) – to „čisto Ja“ može se shvatiti kao imaginarna mreža koja drži sve prošle, sadašnje i buduće doživljaje na okupu, dajući im identitet doživljaja jedne jedinstvene osobe.

2.7. Jonas: odgovornost subjekta

Nakon što smo uz pomoć velikih imena povijesti filozofije pokušali prikazati problematiku ideje subjekta, razlučivanja pojmova, fenomena, mjesto koje subjekt zauzima u svojoj okolini, načine interakcije u društvu te pitanje subjektiviteta države, vrijeme je da se osvrnemo na još jedno veliko ime, i povežemo subjekt s modernim svijetom i tehnikom. Hans Jonas u knjizi „Princip odgovornost“²⁸ otvara upravo problematiku odnosa čovjeka i tehnologije, te nas dovodi još bliže našoj problematici subjekta upravo u svijetu nastalom kao posljedica integracije tehnologije u čovjekov svakodnevni život.

²⁵ Edmund Husserl, *Ideje za čistu fenomenologiju i fenomenologijsku filozofiju*, str.105

²⁶ Ibid., str.125

²⁷ Ibid., str.128

²⁸ Jonas, Hans, *Princip odgovornost*, Sarajevo, 1990.

Jonas se pitanjima prirode, tehnologije i čovjeka bavio i prije pisanja navedene knjige“, u članku „Aktualni etički problemi iz židovske perspektive“. Taj se članak može shvatiti kao uvertira u njegov rad poslije, jer u njemu preispituje ideju čovjeka kroz moderne teorije (koje su u kontrastu s religijskim teorijama o stvaranju čovjeka)²⁹. Također u kontekstu modernih znanosti preispituje i ideje prirode, te uvodi problematiku moderne tehnologije. Čovjek od svojih početaka živi i napreduje tako da ovladava prirodom i za razliku od drugih živih bića, više prilagođava prirodu sebi, nego sebe prirodi. Pojava moderne tehnologije dodatno daje prednost čovjeku nad prirodom i omogućava sve veće uplitanje u prirodu i interferiranje u prirodni sustav. Jonas uočava da je tehnologija kao sredstvo pojačane integracije dvosjekli mač – iako sama po sebi nije ni dobra ni loša, ona je ipak dala čovjeku nevjerojatnu prednost. Podnaslov Jonasovoj knjizi „Princip odgovornost – pokušaj jedne etike za znanstveno-tehnološku civilizaciju“ pokazuje koliko je rano Jonas uočio da razvoj tehnologije uz sebe vuče i ozbiljna etička pitanja, te da je odgovornost ključan pojam o kojem bi trebali razmišljati kad razmišljamo o tehnologiji. Jonas je tim dao temelj ne samo raspravi o značaju tehnologije u stvarnom svijetu, nego na neki način i temelje budućoj etici vezanoj upravo uz cyber-sferu.

Jonas je i sam dosta orijentiran prema budućnosti. Osim što radi radi razliku između stare i nove etike, naglašavajući pritom koliko je stara etika nedostatna u novim okolnostima stvarnog svijeta, upućuje i na to da ta nova etika treba gledati dalje od aktualne situacije, i osigurati i budućnost. Etika je oduvijek uključivala pitanja odgovornosti, ali područje utjecaja te odgovornosti se napretkom tehnologije znatno proširilo, a težina objekta te odgovornosti itekako porasla. Raspon odgovornosti mora rasti paralelno s rasponom mogućnosti djelovanja, a kako je razvoj tehnike značajno povećao ljudsku moć nad prirodom, svijest o djelovanju i odgovorno djelovanje moraju pratiti ritam da bi se izbjegla katastrofa. Razvoj tehnologije za čovjeka jednako može značiti i progres i propast, a ključnu ulogu na tom putu nosi upravo odgovornost.

Jonas također napominje i da se promjenom okolnosti u kojima egzistiramo promijenila i sama narav našeg djelovanja. Stvaranje nove etike nužno je i iz te perspektive, jer ako je promjena ne samo u vanjskom aspektu djelovanja, nego i u unutarnjim principima naravi djelovanja, jasno je da stara pravila i norme jednostavno više ne vrijede. Iako je teza o promjeni same naravi djelovanja interesantna, jer se naizgled čini da opcija novog alata ne bi

²⁹ Usp. Jurić, Hrvoje, *Etika odgovornosti Hansa Jonasa*, Zagreb, 2010.

trebala utjecati toliko temeljito na samu osobu, ta pozicija ipak ne čudi. Jonas gleda širu sliku i pokušava ne ispuštati iz vida potencijalne dalekosežne posljedice upotrebe moderne tehnologije. Iako su razvoji mnogih strojeva u ljudskoj povijesti ne samo značajno unaprijedili efikasnost nekih djelovanja, nego čak i potaknuli čitave revolucije (kao što je npr. bio slučaj s parnim strojem i industrijskom revolucijom koja je uslijedila), razvoj moderne tehnologije napravio je toliko nezamisliv skok u rasponu ljudske moći, da ljudi odjednom raspolazu mogućnošću manipuliranja prirodom kakvu prije nisu mogli ni približno zamisliti. U tako drastičnoj promjeni okolnosti, jasno je da se sukladno tome dogodila i promjena same naravi djelovanja. Iz današnje perspektive gledano, taj je proces sve intenzivniji i sve brži, i znanstveno-tehnološki skok koji smo napravili u zadnjih samo pedesetak godina nemjerljivo je veći od tehnološkog napretka koji se događao kroz prethodna stoljeća. Usporedimo li sadašnjost sa samo nekoliko godina unatrag napredak je nevjerojatan, a timovi i timovi znanstvenika diljem svijeta rade na tom da taj napredak bude još eksplozivniji. Granice realnosti pomiču se praktički svakodnevno, pa se Jonasovo naglašavanje važnosti prilagođavanja odgovornosti i formiranja etike fokusirane i na budućnost čini gotovo proročki.

Ta je potreba za nastankom nove etike temeljene na promijenjenoj naravi djelovanja naročito značajna za kontekst etike u cyber-sferi, gdje je uopće ideja osobe u potpunosti drugačija od ideje osobe u realnom svijetu, a među-odnosi sasvim izmijenjeni. Cyber-sfera, iako gotovo apsolutno različita od područja realnog svijeta, ipak nije izolirani virtualni vakuum, i djelovanje unutar nje ima itekako odraza i na stvarnost. Zbog toga je Jonasova etika odgovornosti vrlo značajan trenutak u promišljanju odnosa tih dvaju sustava i načina ljudskog djelovanja između njih.

Dodatna specifičnost te nove etike u odnosu na staru leži i u tom što je sveobuhvatna. U kontekstu onog starog, pred-moderno-tehnološkog svijeta, etika je ipak bila vezana za individuu, iako se odnosila na opće principe. Svaki pojedinac je za sebe odlučivao hoće li se nekim alatom koristiti, ili sudjelovati u određenom djelovanju, pa iako su etička načela bila opća, individualno se moglo ne razmišljati o nekim aspektima koji se ne tiču pojedinca osobno. U pogledu svijeta u kojem postoji moderna tehnologija to više nije moguće. Neovisno o našem osobnom stavu o tehnologiji, ne možemo više zamišljati svijet bez nje, i nemoguće je ne imati interakciju s tehnologijom barem u nekoj mjeri. Ona je jednostavno sveprisutan element, već i u Jonasovom razmišljanju, a kamoli danas. Pojavom Interneta

realnost svijeta dobija još jednu dimenziju, i sve je očitija nužnost etike koja u sebi uključuje i pitanja tehnologije.

3. Problem subjekta u cyber-sferi

3.1. Kako postojati *online*?

Vidjeli smo već koliko cyber sfera nije tek virtualna preslika realnog svijeta. Odnosi su kompliciraniji, definicije (ako uopće postoje) labavije, vrijednosni sustavi okrenuti u potpunosti individualno. Definiranje subjekta u cyber-sferi onda također ne može biti preslika definicije subjekta koju imamo u realnom svijetu. Kako objasniti subjekt u cyber-sferi, i trebamo li čak raditi distinkciju subjekt/cyber-subjekt?

Kada u svakodnevnom govoru kažemo subjekt, u principu mislimo ili na gramatičku kategoriju nositelja radnje, ili na pravnu kategoriju, ili na neku konkretnu fizičku osobu. Ta je osoba definirana čitavim nizom odrednica. Definirana je imenom, spolom, dobi, pripadnošću nekom narodu, rasi, obitelji. Pripada i u razne druge grupe: religijski, interesima, obrazovanjem, hobijima, društveno-političkim stavovima, prehrambenim navikama, krvnom grupom i nebrojenim drugim sitnim detaljima koje nikada ne bismo mogli do kraja pobrojati. Neke se od tih nebrojenih diferencijalnih crta s vremenom i promijene, ali subjekt koji je njima bio definiran i dalje ostaje isti subjekt, kao što smo vidjeli već kod Aristotelovog objašnjavanja bića, ili Husserlovog „čistog Ja“. Kategorije se s vremenom i pojavljuju i gube, pa je tako ista osoba u jednom periodu dijete, a u drugom otac ili djed, i dalje ostajući ista osoba. Kontinuitet je jedna od glavnih karakteristika subjekta, unatoč svim promjenama, pa i naizgled pauzama (npr. san ili koma), i dok god neka osoba „traje“, odnosno živi, prepoznajemo je kao zaseban subjekt. Mogli bismo reći da ljudska egzistencija zapravo znači kontinuiranost promjene, dok je ipak „ono nešto“ drži stabilnom i statičnom.

Online-sfera nije područje kontinuirane promjene, dapače, to je sfera isprekidane nepromjenjivosti. Sve ono što se ikad registrira *online*, ostaje vječno zapisano negdje u bespuću virtualnog prostora. Slično fizičkom dnevniku ili foto-albumu, podatak u cyber-sferi ostaje vječno ulovljen u određenom trenutku, izvučen manje ili više izvan konteksta. Može se pratiti nekakav razvoj u smislu promjena informacija s vremenom, ali zapravo ne možemo uistinu govoriti o promjeni, samo o ažuriranju. Do stare se informacije i dalje može doći, i ona na taj način zapravo ostaje nepromjenjiva. Internet je tako virtualni svijet duhova, gdje „mrtve“ informacije ostaju vječno prisutne, neovisno o tom koliko više nisu istinite ili relevantne. Za razliku od realnog svijeta u kojem nas netko može upoznati samo onakve kakvi u nekom trenutku jesmo, *online* postojimo u svim varijantama koje smo ikada

registrirali, i naša slika *online* s vremenom može postati vrlo različita od nas u realnom svijetu.

Osim što je naše postojanje *online* uvijek nekakav čudan hibrid prošlosti i vječne sadašnjosti, još jedna razlika u postojanju u realnom svijetu i postojanju u cyber-sferi je u tom što u realnom svijetu postojimo kao jedna izrazito kompleksna cjelina, dok u cyber-sferi postojimo kao jako puno jednostavnih i raspršenih detalja, koji zapravo ne čine nikakvu koherentnu cjelinu. Također, *online* postojimo sve intenzivnije i sve je više tih malih fragmenata rasprostranjeno sve šire po virtualnom svijetu. Dok naše ime i osobni identifikacijski broj u realnom svijetu označavaju kompletnu cjelinu, naš korisnički ID u virtualnom svijetu ne označava jasno ništa, štoviše, većina nas ga niti zna niti razmišlja o njemu, to je samo polazišna točka naše interakcije s virtualnim svijetom. Pa ipak, u tom svijetu sve više postojimo.

U današnjem svijetu, nemoguće je izbjeći online-postojanje. U virtualnom svijetu egzistiraju naši zdravstveni kartoni, bankovni računi, informacije o obrazovanju (od e-Dnevnika u osnovnim školama do Studomata na sveučilišnoj razini). Online putem se naručujemo na medicinske preglede, online putem registriramo čak i veterinarske preglede naših kućnih ljubimaca, pa čak i servisiranje kućanskih aparata ili osobnih automobila. U virtualnom prostoru se odvija dobar dio naše svakodnevne interakcije sa svijetom, od komunikacije s drugim korisnicima pa nadalje. Najčešće niti ne razmišljamo o tome koliko svakodnevno traga ostavljamo u cyber-sferi. Tamo su nam osobni kalendari, alarmi, razni podsjetnici, pošta, putokazi, novčanici, foto-albumi. Čak i ako mi svjesno ne registriramo svaki naš korak *online*, rade to za nas naši mobilni telefoni i ostali aparati koji prate signal. Virtualna sfera sve te enormne količine informacija samo prima, kao kad pospremamo puzzle u kutiju, tamo se pri tom ne stvara neka konkretna slika, informacije samo upadaju i ostaju vječno zapisane – negdje. To je, naravno, problem. Spomenuli smo već da za razliku od realnog svijeta, cyber-sfera ne poznaje toliko promjenu koliko ažuriranje podataka. Stari podatci i dalje postoje. To znači da je Internet zapravo pun dezinformacija, koje se van konteksta mogu činiti kao još uvijek važeće informacije. Osim što je dezinformiranje problematično već samo po sebi, širenje dezinformacija može prouzročiti negativne društvene fenomene poput masovnih histerija, straha, jačanja negativnih društvenih strujanja (poput jačanja raznih ekstremizama i netrpeljivosti) što može predstavljati vrlo ozbiljnu prijetnju sigurnosti u granicama realnog svijeta. Fragmentiranost sustava također omogućuje prostor mikro-prijetnjama, u obliku raznih virusa koji kao sitni nametnici lako mogu proći

neprimjećeno, pa su korisnici raznih online-usluga u riziku da u potpunosti nesvjesno budu posrednici u ilegalnim aktivnostima na internetu, ili alat u zloupotrebi sustava. Npr. virus na računalu programiran da bude toliko sitan da ga korisnik ni ne osjeti može incognito stvarati smetnje u nekom većem sustavu (npr. prosljeđivanjem e-mail reklama)³⁰, koji pod napadom milijuna takvih smetnji onda ne može normalno funkcionirati i njegovo rušenje ometa rad neke npr. bolnice ili banke. Takvih „mušica“ virusa je internet pun, i svakodnevno se pojavljuju novi. Stoga je izrazito važno u našem online postojanju biti svjestan odgovornosti koju to zahtijeva, i da samo zato što ne znamo da naše računalo/mobitel/bilo koji uređaj s pristupom internetu nešto radi, to ne znači da odgovornost za to djelovanje nije na nama.

To nas dovodi do pitanja zaštite i odgovornog ponašanja na internetu. U stvarnom smo svijetu svjesni opasnosti koje nam prijete i od malena nas se uči kako se što je moguće više osigurati i zaštititi. No to je puno teži posao u sferi u kojoj je upitno koliko uopće, i na koji način, postojimo, i u kojoj ne razumijemo u potpunosti načine na koje smo u nju uključeni. Djelići nas postoje u čitavom nizu ladica koje čine virtualni svijet, i moramo biti svjesni toga da nosimo odgovornost za svaki od tih djelića i njegovu interakciju unutar dane ladice, ali i šire. Zbog toga je internetska pismenost vrlo važna i ide znatno dalje od razumijevanja tehničkih principa rada uređaja. Naša dužnost je držati svaki od naših virtualnih komadića na okupu u realnoj svijesti stvarnog svijeta, jer virtualni svijet je ipak na neki način usidren u realnom. Koliko god virtualna stvarnost djelovala primamljivo, ne smijemo smetnuti s uma da naše virtualno djelovanje može itekako utjecati na realni svijet, bili mi tog djelovanja svjesni ili ne. Naučiti se zaštititi, i spriječiti to da svjesno ili nesvjesno budemo medij aktivnostima koje mogu imati opasne posljedice u *offline* svijetu od esencijalne je važnosti za postojanje *online*, jer kao što nas je već Jonas upozorio u naše djelovanje danas ne riskira samo trenutne, nego i buduće posljedica, koje mogu biti vrlo dalekosežne.

³⁰ Usp. Stefan Kiltz, Andreas Lang, and Jana Dittmann, *Malware: Specialized Trojan Horse*, u: Janczewski, Lech; Colarik, Andrew M., *Cyber Warfare and Cyber Terrorism*, Information Science Reference, Hershey - New York, 2008.

3.2. Realni vs. virtualni subjekt

U prošlom poglavlju dotakli smo se načina na koji postoji naše virtualno ja, i na koji način to virtualno ja ipak ima uporište i efekt u realnom svijetu. No jesu li realni i virtualni subjekt uopće razlučivi pojmovi, ili je jedan samo zrcalni odraz ili sjena drugog u nekoj drugoj sferi? Tko je uistinu taj virtualni subjekt? I ako uzmemo u obzir prije spomenute rasprave o realnosti, bismo li tom virtualnom subjektu ipak priznati individualnu istinitost, čak i ako je tek (iskrivljena) sjena?

Pojavom brzog i lako dostupnog interneta otvorile su se brojne mogućnosti samorealizacije bilo kojeg pojedinca u cyber-sferi. Seljenjem u virtualni svijet, warholovskih 15 minuta slave odjednom više nije bilo rezervirano za pojedince koji će se kombinacijom rada, sreće i talenta s vremenom progurati na svjetsku scenu. Otvorila su se vrata novim oblicima stjecanja slave, i svaki „anonimac“ dobio je priliku poslati svoju poruku svijetu i prestati biti „anonimac“³¹. Vrlo rana pojava vala osobnih blogova na web-portalima, koji su doslovno dotad pomno sakrivane osobne dnevnike s ključem odjednom izvadili ispod jastuka, otključali i servirali čitavom svijetu na čitanje, pokazuje uistinu koliku ljudi imaju potrebu za individualizacijom te priznanjem okoline da su više od samo još jednog kotačića u sustavu. Internet je omogućio ne samo da svatko ostvari individualno formiranje, nego i da to objavi ostatku svijeta i bude viđen i „slavan“. Blogovi³² su vrlo brzo počeli vrviti raznim oblicima aktivizma, a revolucije se polako, ali sigurno, počele seliti s ulica realnog svijeta u virtualni svijet, u nadi da će masovno online-preodgajanje i reformiranje društva odjeknuti i na offline-razini.

Boom blogova pratila je bombastična epidemija društvenih mreža³³. Od mjesta za lakše komuniciranje³⁴ s ljudima koji nam nisu fizički blizu, postale su svojevrsni zasebni univerzumi. Nisu više samo mjesto na kojem su skupljeni virtualni arhivi s osobnim podacima i fotografijama ljudi, nego čitavi društveni sustavi koji uključuju izmjenu informacija, novine, grupe okupljene oko određenih interesa ili ideja, javne kalendare događanja kako u virtualnom tako i u realnom svijetu, igrališta, pa i trgovine. Društvene

³¹ Usp. Polettiand, Anna; Rak, Julie (ur.), *Identity Technologies Constructing the Self Online*, The University of Wisconsin Press, 2014.

³² blog = internetska verzija osobnog dnevnika koju osoba piše na za to specijaliziranim web-stranicama.

³³ Usp. Polettiand, A.; Rak, J. (ur.), *Ibid.*

³⁴ Usp. Wood, Andrew F.; Smith, Matthew J., *Online Communication – Linking Technology, Identity, and Culture*, Lawrence Erlbaum Associates, Mahwah, New Jersey, 2005.,

mreže postale su više od samo mreža, te postale izrazito kompleksne cjeline. No taj rast je bio toliko brz, da se društvene mreže nisu stigle organizirati u uistinu funkcionalna virtualna društva, jer u njima još uvijek ne postoji formalni zakon, nego eventualno smjernice za ponašanje.

Eksplozija društvenih mreža, napredak mobilne tehnologije i brzi Internet pružili su nam više od mogućnosti da svakodnevnim dokumentiranjem i objavljivanjem detalja iz vlastitog života, pisanjem osvrta i iznošenjem stavova postanemo slavni. Odjednom nam se pružila prilika i da budemo netko drugi, ili čak nitko. Ipak, ne smijemo smetnuti s uma da je virtualan svijet ipak i dalje samo virtualan, unatoč realnosti svoje egzistencije kao zasebnog fenomena, i postoji samo na temelju onog što mi na njega *uploadamo*³⁵. Osoba prezentirana *online* i osoba koja režira taj online-život iz stvarnog svijeta ne moraju zapravo uopće biti ista osoba. S jedne se strane to čini bezazleno, nikakvo zlo u tom da si netko malo „uljepša“ fotografiju ili objavi samo filtrirane, pozitivne događaje, slavni ljudi to po medijima ionako već rade desetljećima. No s druge strane, lažno predstavljanje može otići i u ekstrem i biti način za manipuliranje bilo ciljanim pojedincima (djecom, marginaliziranim ljudima, starijim ljudima itd.), bilo čitavim ciljanim skupinama, gdje jedna izmišljena osoba, iza koje može stajati vrlo nestabilan pojedinac, ili možda čak čitav tim, postaje svojsvrnsni alternativni, virtualni vladar i vođa.

Koliko god je internet javan, toliko je zapravo anonimn. Vrlo je jednostavno u potpunosti anonimno djelovati, bez ikakvog odraza na stvaran život osobe u realnom svijetu. Cyber-sfera je područje koje se čini nemoguće za koherentnu regulaciju. Previše je apstraktna i previše brza da bi bila podložna standardnim pravnim regulacijama. Čak i na osnovnijoj razini interakcije osobe s okolinom, cyber-sfera je problematična. S jedne strane omogućuje gotovo apsolutnu individualizaciju, osoba je u svojoj anonimnosti okrenuta u potpunosti prema sebi i realizaciji svojih potreba, bez potrebe za prilagođavanjem i kompromisima koji su u realnom svijetu nužni za funkcioniranje u zajednici. To samo po sebi ne zvuči nužno loše, ako se uzme pod pretpostavkom da govorimo o u realnom svijetu već formiranoj osobi, razvijene socijalne inteligencije, moralnih vrijednosti i osjećaja za osobnu odgovornost, koja se u beskrajnim opcijama cyber-sfere dodatno definira, usmjerava i unaprjeđuje. Problem je u tom što internetu pristup imaju gotovo svi, a sigurnost anonimnosti omogućuje vrlo jednostavan bijeg od odgovornosti i socijalno uvjetovanih sustava vrijednosti. Naizgled

³⁵ "upload" – engleski termin koji u kontekstu interneta označava proces pohranjivanja podataka na web-stranicu.

društveno funkcionalna individua sada ima opciju „hraniti“ inače zatomljene elemente svoje osobnosti, povezivati se s istomišljenicima i izvrtati realnost sve do stadija potpune deluzije. Jednostavnost spontanog djelovanja i izostanak izravne osude lako vodi u radikalizaciju ideja, iskrivljavanje individualnog sustava vrijednosti, utišavanje racionalnog promišljanja i potpuno odvajanje online-subjekta od offline-subjekta.

To lako može labilnije osobe odvesti u stadij depersonalizacije³⁶, u kojem svoje online- djelovanje više ne vide ni kao svoje, ni kao realno. Internet omogućava eskapizam, pa po mnogim portalima svjedočimo masovnom krivom načinu nošenja s osobnim neuspjesima i frustracijama, koje nerijetko prijeđe u nasilje, bilo u cyber-sferi, bilo u stvarnom svijetu. Posebna opasnost tu leži upravo u spomenutoj jednostavnosti radikalizacije ideja, gdje vrlo brzo možda i relativno benignan stav, pod okriljem masovnosti online grupe i predoziranje negativnim diskursom, prelazi u fanatizam. Inače možda bezopasni pojedinci, koji se iz ovog ili onog razloga osjete isključenima ili neprihvaćenima u realnom svijetu, vrlo su laka meta brze *online* radikalizacije.

Opcija incognito eksperimentiranja također je čest okidač za odvajanje subjekta i stvaranje online persone koja nije u doticaju s offline-osobom. Naizgled nevin eksperiment npr. hakiranja³⁷ lako odvede do ozbiljnih kriminalnih radnji, a znatiželja sve teže razlučuje „mogu“ od „trebam li“ ili „smijem li“. Dok se u stvarnom svijetu ne vodi previše rasprave o tom je li vlasnik prethodno dobro zaključao kuću ukoliko je došlo do provale, i provalnika se ništa manje neće smatrati krivim ako je bila zaključana samo jedna, a ne dvije brave, u cyber-sferi se odgovornost češće svaljuje na nedovoljnu prevenciju. Nedovoljno zaštićena jedinica smatra se otvorenim pozivom na korištenje, bez pretjeranog razmišljanja o „trebanju“, pa je i osjećaj odgovornosti umanjen i podređen osjećaju mogućnosti³⁸.

Ukoliko su online-subjekt i offline-subjekt u potpunosti odvojeni, koji od njih nosi odgovornost, i može li se očekivati da offline-subjekt ima kontrolu nad online-subjektom? Vidjeli smo već koliko cyber-sfera nije tek virtualna preslika realnog svijeta. Odnosi su kompliciraniji, definicije (ako uopće postoje) labavije, vrijednosni sustavi okrenuti u

³⁶ depersonalizacija = promjena u percepciji ili doživljavanju samog sebe tako da se osoba osjeća odvojena od sebe i kao da je vanjski promatrač svog psihičkog procesa ili tijela; prema Folnegović-Šmalc, Vera (ur.), *DSM-IV – Dijagnostički i Statistički Priručnik za Duševne Poremećaje*, Američka psihijatrijska udruga, Jastrebarsko, 1996.

³⁷ hakiranje = proces nelegalnog i neautoriziranog, te uglavnom zlonamjernog ulaženja u informatički sustav, najčešće malverzacijom programa za zaštitu sustava i reprogramiranjem.

³⁸ Usp. Colarik, Andrew M., *Cyber terrorism – Political and Economic Implications*, Idea Group Inc., London, 2006.

potpunosti individualno. Definiranje subjekta u cyber-sferi onda također ne može biti preslika definicije subjekta koju imamo u realnom svijetu. Kako dakle objasniti subjekt u cyber-sferi, i trebamo li čak raditi distinkciju subjekt/cyber subjekt?

Pitanja subjektivnosti već u realnom svijetu, kao što smo pokazali, izazivaju polemike još od antičkih vremena, te postoje bezbrojne teorije o subjektivitetu, ne samo iz filozofske perspektive, nego i iz brojnih drugih. Uzmimo zato ovdje za primjer subjekt u pravnom smislu. Kako takvo određenje prenijeti u sferu u kojoj zakoni ili ne postoje ili ih je jako teško provoditi? Sveprisutnost maloljetnika na internetu dodatno otežava problem. Dok pravni sustav realnog svijeta ima detaljno razrađena pitanja pravne odgovornosti maloljetnika, djelovanje u virtualnom svijetu teže je podložno istoj regulaciji – razina razumijevanja maloljetnika je još osjetljivija nego u realnom svijetu jer su posljedice djelovanja znatno apstraktnije. Isto vrijedi i za ljude slabijih mentalnih sposobnosti ili ljude s raznim psihičkim poremećajima. Kako regulirati njihovo online djelovanje, i možemo li ih uopće nadzirati? Također, veliko, a u kontekstu cyber-ratovanja i vrlo značajno pitanje je i trebaju li osobe lišene slobode biti lišene i virtualne slobode, odnosno pristupa internetu, naročito ako se uzme u obzir koliko se organiziranog kriminala odvija upravo putem interneta.

No vratimo se korak unatrag, na pitanje odnosa ta dva subjekta. Upitno je zapravo možemo li unutar virtualnog svijeta uopće govoriti o nečem tako jedinstvenom kao što je subjekt u realnom svijetu. Samostalno online-djelovanje toliko je nevidljivo, a iako je digitalni footprint prosječne osobe na Zapadu danas već toliko velik da je sama ta činjenica zanimljiv aspekt u promatranju osobnog identiteta, svi ti otisci toliko su raštrkani i izgubljeni u moru podataka, da se zapravo može postaviti pitanje postoje li uopće kao nekakva cjelina koju bi se moglo nazvati subjektom, i koliko su relevantni elementi u osobnosti one realne osobe koja ih je ostavila u virtualnom svijetu. Možda je rješenje uistinu u tom da se ne pokušava povezati ono što bi smo nazivali cyber-subjektom, s riječju 'subjekt' koju koristimo u realnom svijetu. Uostalom, u virtualnom svijetu egzistiramo samo fragmentalno, s rupama u kontinuitetu koje se nikako ne mogu usporediti sa recimo snom ili komom u realnom svijetu, pa se možemo zapitati postoji li takvo nešto kao subjekt u sferi u kojoj ne postoji kontinuitet, a koja bez filtriranja registrira svaki naš korak? U realnom svijetu definirani smo karakternim crtama, preferencama i djelovanjem, ali sva su ta obilježja podložna promjeni. Nakon nekog vremena nešto što nas je u jednom trenutku definiralo (npr. zelena kosa, punk faza, interes za vrtlarjenje) ne definira nas više (sad smo recimo plavokosi, od punka nas boli

glava, a vrtlarjenje je zamijenio interes za vlakove). No u cyber-sferi svaki podatak ostaje izvučen i iz vremena i iz konteksta, nepromjenjiv.

Pretpostavke su da je „mrtvi internet“ već debelo prerastao aktivni internet, pa u bespućima neaktivnog interneta i dalje pasivno postoje (jer upitno je može li se uopće reći egzistiraju) nebrojeni entiteti nečeg što u realnom svijetu ne da je promijenjeno ili više ne postoji, nego je gotovo do te mjere zaboravljeno, da se čini apstraktnim govoriti da je uopće ikada postojalo. Osobni blogovi, web-stranice razreda osnovnih škola čiji učenici već lagano ispraćaju vlastitu djecu u školu, informacije o radnom vremenu trgovina kojih se više nitko ni ne sjeća, vremenske prognoze, vijesti, stanja na glazbenim top-ljestvicama, programi kina, pa između svega toga, i profili na društvenim mrežama i raznim drugim stranicama ljudi koji u realnom svijetu možda uopće nisu ni živi. Nešto ili netko može na neki način postojati, smrznut u binarnom kodu bez vremena, a da uopće ne postoji, ako je ikada i postojao. Kako onda možemo govoriti o subjektu?

Tu je također pitanje i lažnih profila ili bilo kakvog oblika alternativne realnosti u virtualnom svijetu. Detaljno razrađen profil može imati sve karakteristike koje bismo uzeli za definiranje subjekta, a da pri tom nema nikakvo uporište u realnosti. Ako netko provodi dobar dio dana *online*, recimo u RPG-u³⁹, posvećuje vrijeme aktivnom sudjelovanju u virtualnom svijetu, izgrađuje odnose, radi na sebi, ostvaruje uspjehe, doživljava poraze i stvara nekakav „životni“ put, je li to nešto što se može negirati kao zasebna osoba, odvojena od osobe koja njom upravlja iz realnog svijeta? Ta dva bića mogu biti u potpunosti drugačija, i po svim klasifikacijama psihologije ne biti ista osoba. Kao i kod ljudi s poremećajem ličnosti, kako odrediti koja osoba je „ona prava“? Koju priznati u pravnom smislu? Objek? Može li virtualna osoba, ma kako karakterno razrađena i samoostvarena, biti uistinu priznata kao osoba? Ukoliko može, otvaramo čitav niz problema, od banalnog pitanja ako je virtualni lik osoba, a realni „vlasnik tijela“ izbriše korisnički račun, je li počinio ubojstvo; pa do vrlo ozbiljnih pitanja poput onoga ako su virtualna i realna osoba dva različita subjekta, i virtualni počini kriminalno djelo, možemo li suditi realnom?

Odluka o tretiranju virtualnog subjekta značajna je možda i najviše upravo u domeni cyber-ratovanja i terorizma. Naravno da nije zanemarivo ni ostalo opasno djelovanje u cyber-sferi, od vršnjačkog zlostavljanja pa nadalje, no dobar dio takvog djelovanja da se rješavati na

³⁹ „role playing game“, engleski termin za tip društvenih igara u kojima igrači aktivno preuzimaju alternativni lik i igraju ulogu.

mikro-razini, bilo *online* (administratorskim izbacivanjem problematičnog člana iz grupe, savjetovanjem, privremenim ili trajnim blokiranjem korisničkog računa itd.), bilo *offline* (od razgovora s učiteljima, psiholozima, intervencije socijalnih institucija, pa do pravnog sustava i kazni unutar pravne sfere realnog svijeta). No kada je u pitanju sigurnost veće skupine (npr. vjerskih skupina, raznih civilnih udruga, većeg broja ljudi na osnovi neke karakteristike ili čak čitavih država/nacija), cyber-sfera je još uvijek u problemu manjkavosti regulacije i pravnih sustava. Ukoliko se cyber-subjekt tretira kao odvojen od realnog subjekta, to bi vodilo u problem kažnjavanja, jer kako jednu osobu kazniti za djelovanje druge osobe? I u realnom svijetu poznati su slučajevi obrane na račun privremene ili trajne neuračunljivosti, psihoza, raznih poremećaja ličnosti itd. Taj problem se u realnom svijetu rješava prisilnim ili dobrovoljnim liječenjem osobe u zatvorenim psihijatrijskim institucijama, i iako ih se ne kažnjava u strogom smislu riječi, ipak ih se sprječava od daljnjeg djelovanja privremenim ili trajnim izoliranjem iz zajednice (ovisno o izlječivosti stanja). Čak i u takvom kontekstu za neke prekršaje postoji eventualno umanjena kazna zbog okolnosti, ali ipak ne izostaje u potpunosti, neovisno o tom što se osoba brani tim da u trenutku počinjenja djela nije bila svjesna svog djelovanja, pa stoga ne može snositi odgovornost.

Iako se može povući paralela s psihijatrijom, problem odnosa cyber-subjekt/realni subjekt je primarno u tom što ta dva subjekta nisu fizički povezana – jedan egzistira u cyber-sferi, a jedan u realnom svijetu. Koliko god u slučaju psihičkog poremećaja osoba možda i nije u stanju moralno razlučivati, pa stoga nije „kriva“ za svoje djelovanje, fizičko tijelo je i dalje to koje je djelovalo, ostavilo neku posljedicu, i snosi nekakav oblik „kazne“ – bilo u smislu prave kazne (ukoliko psiholozi i psihijatri ustanove da je svijest o djelovanju ipak postojala), bilo u smislu institucionaliziranog liječenja zatvorenog tipa. U cyber-sferi nema tog tijela koje bi ipak snosilo odgovornost. Ukoliko osobu koja je *online* počnemo tretirati kao individualni subjekt koji živi unutar svoje sfere, presjekli smo vrlo važnu konekciju s realnim svijetom i oslobodili realni subjekt svake odgovornosti za išta što je počinjeno u virtualnom svijetu, makar to imalo efekta i na realni. Čak i kada bismo najstrože pravne sustave realnog svijeta prepisali u virtualni (pod pretpostavkom da smo uopće uspjeli regulirati područje djelovanja pravnog sustava online i jasno odredili državne granice unutar virtualnog svijeta), kako bi se ti zakoni provodili⁴⁰?

⁴⁰ Usp. Colarik, Andrew M., *Cyber terrorism – Political and Economic Implications*.

Pretpostavimo li da je smrtna kazna najstroža kazna u realnom svijetu, što bi ona značila u virtualnom? Brisanje korisničkog ID-a⁴¹? Bi li ta kazna uključivala i brisanje cjelokupnog virtualnog footprints? Jer kod smrtne kazne u realnom svijetu iza osuđenika ipak ostaje trag – njegovo tijelo, grob, osobne stvari, fotografije, no ostavljanje podataka u virtualnom svijetu nakon brisanja korisničkog ID-a značilo bi da u principu nije napravljeno ništa, jer je problem i dalje aktivan (npr. *post* ili čitava web-stranica posvećena sustavnoj eskalaciji mržnje prema određenoj društvenoj grupi i pozivanje na nasilje protiv iste). Naravno, brisanje cyber-subjekta iz virtualnog svijeta uistinu i ne bi bilo ni kazna ni efektan čin, s obzirom da bi subjekt iz realnog svijeta bio „kažnjen“ samo u smislu izgubljenog vremena, jer bi morao početi ispočetka graditi cyber-subjekt koji bi ponovno djelovao u cyber-sferi. Spomenuto je također da iza jednog cyber-subjekta može stajati i više realnih, koji bi se također mogli jednostavno ograditi od djelovanja, s obzirom da je njihova odgovornost bila samo povremena, ili samo za neki fragment subjekta. Treća varijanta je da cyber-subjekt uopće nije subjekt, čak ni u vrlo rastegnutom shvaćanju pojma „subjekt“ unutar cyber-sfere, nego da je ciljano anonimna tvorevina, „duh“, kojem je jedina funkcija ciljano djelovanje, i iza koje stoji čitav niz oprezno anonimnih pojedinaca. Takve svjesno anonimne grupacije smo već imali prilike vidjeti – pokreti Occupy⁴² i Anonymous⁴³ bili su upravo to.

No ukoliko subjekt shvatimo u širem smislu, kao identitet definiran nekom jasnom distinktivnom crtom, utoliko i anonimne „duh“ pojave i razne organizirane grupacije postaju subjekt. U takvom kontekstu, i njihovi upravljači iz realnog svijeta ulaze unutar te definicije, kao jedna djelatna jedinica unutar sustava, pa prema tome mogu snositi i pravnu odgovornost za svoj doprinos. Takav mehanicistički pogled rješava problem dihotomije virtualnog i realnog subjekta, a samim time i virtualne i realne odgovornosti, te vraća pravnu problematiku natrag u sferu realnog, kao što ćemo vidjeti da se prakticira u kontekstu odgovornosti tijekom oružanih sukoba. No tu problemi ipak ne staju. U realnom svijetu odgovornost snosi ili pojedinac, ili grupa (od manjih grupa pa sve do država ili čak međunarodnih udruženja), i u grupama postoji jasna hijerarhija odgovornosti. No da bi netko mogao snositi odgovornost, mora biti prihvaćen kao nositelj odgovornosti od strane sustava.

⁴¹ *user ID*, ili korisnički ID = kod pomoću kojeg se identificira svakog korisnika nekog elektroničkog softwera, bilo na internet ili u bilo kojem elektroničkom sustavu poput osobnih računala.

⁴² Occupy Movement =međunarodni socio-politički pokret usmjeren protiv socijalne nejednakosti i “nedostatka prave demokracije”, kojem su društvene mreže glavna platforma za izmjenu informacija i organizaciju protesta.

⁴³ Anonymous = decentralizirana, međunarodna grupa “haktivista” (aktivista hakera) odgovorna za niz cyber-napada protiv raznih vlada i državnih organizacija.

Djeca tako nisu nositelji odgovornosti, jer ih sustav ne priznaje kao pravni subjekt, ali tu ulogu zato preuzimaju njihovi skrbnici. U slučaju međunarodnih konflikta, nositelj odgovornosti je država, odnosno državni vrh. Samoproglašena država stoga nije dio sustava jer nije priznata kao takva i nema suverenitet, pa se njen „vrh“, odnosno samoproglašeni vladar, tretira kao kriminalac unutar sustava države koja je na tom teritoriju priznata. Terorističke grupe zbog tog su već unutar realnog sustava problem, jer zapravo nisu službeno prepoznate kao jedinstven „subjekt“, a u cyber-sferi taj se problem multiplicira.

3. 3. Hiperindividualizacijom prema nestanku: gdje je nestao subjekt

Problematika disocijacije realne i virtualne osobe spomenuta u prethodnom poglavlju vodi, kako je već bilo riječi, u jedan sasvim neočekivan zaokret. U trenutku pojave onih prvih blogova na kojima su ostvareni prvi koraci seljenja u virtualni svijet gdje uistinu svatko može biti što god poželi, i gdje je uistinu svatko barem malo slavan, nitko nije pomišljao o tom koliki metež će nastati u toj sferi, koliko more profila kroz koje se gotovo nemoguće snaći. Svatko je (barem malo) slavan, i svi su opet jednako utopljeni u masu. Društvene mreže prekrane su milijunima profila koji na prvi pogled izgledaju identično. Mnogi korisnici paralelno imaju i više profila, za privatnu upotrebu, poslovnu upotrebu, posvećenih isključivo nekom hobiju ili interesu. Također smo već spomenuli i naše *online* postojanje o kojem zapravo većinu vremena ni ne razmišljamo, a to su razne službene stranice, online baze u zdravstvenom i školskom sustavu, bankama, raznim administracijama i slično. Virtualni komadići našeg svakodnevnog života razbacani su diljem cyber-sfere.

Za razliku od realnog svijeta, gdje nas ljudi upoznaju u kontekstu neke situacije, pa onda dalje s vremenom otkrivaju druge detalje i karakteristike naše osobnosti, u cyber-sferi sve je trenutno. Svojoj virtualnoj varijanti⁴⁴ odmah lijepimo čitav niz etiketa, koje doduše postoje i u realnom svijetu, ali nisu toliko vidljive. Sama registracija na sve veći broj stranica, čak i onih koje nisu orijentirane prema društvenoj interakciji, zahtijeva čitav niz podataka kao što su ime, spol, datum rođenja, e-mail adresa. Društvene mreže zahtijevaju i registraciju niza osobnih karakteristika, pa se tako odmah na samome početku kategoriziramo po seksualnoj orijentaciji, političkoj opredjeljenosti, religijskom usmjerenju, horoskopskom znaku, pripadnosti supkulturama, pripadnosti različitim udrugama i organizacijama, pa čak i po

⁴⁴ Usp. Wood, Andrew F.; Smith, Matthew J., *Online Communication – Linking Technology, Identity, and Culture*, Lawrence Erlbaum Associates, Mahwah, New Jersey, 2005.

pripadnosti fan-bazama pop-kulture, pa se Trekkieji⁴⁵ ne vole sa Star Wars fanovima, „djeca 90ih“ se možda ne sjećaju točno u kojem su razrednom opredjeljenju bili u osnovnoj školi, ali su ponosni na „svoj dom“ u Hogwartsu⁴⁶ itd. Sve te silne detalje izlistavamo odmah ispod imena i fotografije. Fenomen prenaplašene političke korektnosti u cyber-sferi dodatno je naglasio tu potrebu ne samo za detaljnom klasifikacijom, nego i kao načinom preliminarnog ograđivanja, pa nije rijetkost na početku komentara na forumima vidjeti konstrukcije poput „Kao straight bijelkinja, želim naglasiti da JA ne stojim iza ovakve akcije...“ ili „Kao transrodni afroamerikanac, važno mi je da ljudi shvate da...“. Hiperindividualizacija je otišla toliko daleko da profili društvenih mreža ne samo da slične na nekadašnje stranice školskih leksikona, u kojima smo pisali sve o sebi, od najdraže boje do omiljenog glumca, nego su na njima sad naglašeni i neki sasvim novi društveni fenomeni, poput preferiranih zamjenica kod transrodne ili gender-fluid osobe, osobnog osjećaja pripadnosti u neku skupinu u koju pojedinac zapravo ne pripada itd. Među mladim Kinezima se tako unatrag nekoliko mjeseci pojavio trend masovne „duhovne pripadnosti“ Finskoj, pa se mnogi mladi Kinezi deklariraju kao spiritualni Finci.

Ironično, u toj masovnoj hiperindividualizaciji koja bi, kad bismo se tako ponašali u realnom svijetu, dovela do naglog porasta postotka stanovništva s dijagnosticiranim poremećajima ličnosti. Zapravo bi se do kraja razbila ikakva iluzija o cjelini koju bi mogli nazvati subjektom. Ovisno o kontekstu, predstavljamo se kroz neku od naših karakteristika. Sami naši profili obiluju kategorijama i „heštegovima“⁴⁷ koji upravo i služe kao filteri za lakše snalaženje kroz kategorije koje nas zanimaju. Ali sva ta detaljna deskripcija dovodi do tog da više uopće ne zvučimo kao jedinstvena osoba, nego kao popis sastojaka. Naše *online* predstavljanje zvuči otprilike jednako kao kad bismo u slastičarnici naručili detaljno pobrojane sastojke, umjesto da jednostavno kažemo ime torte koju želimo. Tako smo zapravo, u pokušaju da se što detaljnije i što individualnije formiramo *online*, zapravo sami prouzročili to da taj cyber-subjekt eksplodira na tisuće malih detalja, koji definitivno više ne čine cjelinu.

Drugi udarac cyber-subjektu zadao je sam sustav. S porastom cyber-kriminala, zloupotrebom podataka, lažnih predstavljanja, manipulacije djecom i sličnih sve brojnijih

⁴⁵ obožavatelji TV-serijala "Star Trek"

⁴⁶ Hogwarts School Of Witchcraft And Wizardry, škola magije iz popularnog Harry Potter serijala autorice J. K. Rowling.

⁴⁷ "hešteg", link na web-stranici označen simbolom "#" koji omogućuje lakše pretraživanje stranice upisivanjem ključne riječi u tražilicu.

problema koji proizlaze iz anonimnosti i masovnosti interneta, porasla je i potreba za što efikasnijom zaštitom korisnika. Web-stranicama je prevelik rizik ostaviti korisnike nedovoljno zaštićene, jer bilo koja rupa ili pogreška u sustavu može vlasnika stranice koštati milijunske tužbe ili čak potpunu financijsku propast uslijed masovnog bojkota korisnika nakon afere za koju možda sam vlasnik stranice nije izravno kriv. Tu se vraćamo na prije spomenuto shvaćanje nedovoljno zaštićenog korisničkog profila (ili čitave stranice) kao otvorene pozivnice za zloupotrebu. Sve više stranica zbog tog ulaže u vrlo složene sustave enkripcije i antivirusne programe, ali ni takvi sustavi nisu u potpunosti sigurni, jer se novi virusi i mehanizmi probijanja kroz virtualne zaštite programiraju svakodnevno, i naravno, u potpunosti anonimno, bez najave. Alternativno rješenje tog problema nalazi se u jednostavnom sprječavanju korisnika da na stranicu registriraju ikakav potencijalno opasan podatak. Gdje su se donedavno, radi verifikacije i sigurnosnih pitanja, zahtijevali točni podaci da bi se uopće moglo početi s radom, sada se, paradoksalno, opet radi sigurnosnih pitanja, sugerira ne-korištenje osobnih podataka, ili pristanak na to da se vlasnik stranice obveže koristiti osobne podatke isključivo transparentno i u svrhu omogućivanja kvalitetnije usluge korisniku, ali i na ograđivanje vlasnika stranice od odgovornosti i snošenja pravnih posljedica ukoliko s neke treće strane ipak dođe do krađe i zloupotrebe podataka, unatoč svim preventivnim mjerama.

Ironičan rezultat toga je da naši razni profili na raznim stranicama sada sve više gube osnovni osobni identitet, jer se ide prema zaštiti pod okriljem anonimnosti, ali i dalje na njih registriramo ne samo sve one prije spomenute etikete i kategorizacije, nego pohranjujemo fotografije, najavljujemo svoj dolazak na razna društvena događanja, „tagiramo“ se po kafićima, restoranima, turističkim lokacijama, itd. Sve smo više bezimni, dok istovremeno cijelom svijetu omogućujemo vrlo detaljnu rekonstrukciju naših svakodnevnih gibanja i aktivnosti. Sukladno tomu, osobe iz javnog života, od starleta do predsjednika država, postaju još javnije i dostupnije, jer sve više web-stranica svoje slavne korisnike verificira plavom kvačicom kao potvrdom da se radi uistinu o profilu te osobe, a ne lažnom predstavljajući. „Plave kvačice“ su nam tako stalno nadohvat ruke, pa umjesto da čitamo povremeni intervju ili čujemo poneku izjavu za javnost, sada možemo biti u potpunosti uključeni u njihove živote, od fotografija doručka do jasnog izjašnjavanja o nekom društvenom ili političkom problemu.

Obje te krajnosti ponovno nisu rješenje sigurnosnim prijetnjama – naprotiv. Među javnim osobama, kao i među ljudima općenito, postoje i odgovorni i neodgovorni pojedinci,

stavovi variraju od potpune nezainteresiranosti do radikalnih ideja, neki trče pred rudo dok neki detaljnije istražuju prije nego iznesu stav. Problem je u činjenici što javna osoba nosi odgovornost utjecanja na određen dio javnosti, pa problematična ili možda samo nespretno formulirana izjava može vrlo lako eskalirati u skandal, unutarnje ili vanjsko-politički problem, pa čak i potencijalno konflikt ili agresivno djelovanje radikalnih skupina. Manji je problem kad takav nered prouzrokuje nogometaš ili glumica, ali kada neoprezne izjave *online* počnu davati visoki državni dužnosnici, situacija može vrlo brzo prerasti u izrazito opasnu. Iz te perspektive gledan, možda bi bilo bolje da se i javnim osobama sugerira ne-korištenje osobnih podataka, no jasno je da bi se to proturječilo ideji javne osobe. Netko tko je sam sebe pretvorio u brend svakako ne želi odjednom postati anonimn, na platformi koja omogućava toliko jednostavno i široko rasprostranjeno reklamiranje. Plave kvačice su, u tom kontekstu, možda zasad ipak najbolje rješenje.

Finalni paradoks pitanju online-subjekta dolazi u obliku ekstremističkih organizacija. Terorističke su skupine u tom smislu već bile spomenute u svom javnom pokušaju preuzimanja odgovornosti za bilo koji incident koji bi im mogao koristiti u manipulaciji općim stanjem straha unutar neke grupe. Dok se prosječni korisnik toliko fragmentirao da ga više uopće nema kao cjeline, a uz to je sve više lišen čak i vlastitog imena kao nekog primarnog simbola individualnosti i subjektivnosti, radikalne skupine pokušavaju upravo suprotno. Preuzimanjem odgovornosti za određeni čin (čak i kada je to apsolutno apsurdno i očigledno neistina), oni pokušavaju u onom pravnom razumijevanju nositelja odgovornosti postati subjekt. Na taj način omogućavaju svojoj grupi legitimaciju, daju si koherentan identitet s jasnom distinktivnom karakteristikom – onaj tko je odgovoran. U kontekstu terorizma, upravo je to ono što „službeni“ sustav želi izbjeći. Prihvaćajući radikalne skupine kao legitiman subjekt, daje im važnost i snagu, a djelovanje za koje oni preuzimaju odgovornost (bilo to realno ili ne) postaje sredstvo širenja straha⁴⁸. Zbog toga se takvi pokušaji kolektivnog preuzimanja odgovornosti od strane čitave organizacije odbijaju. Uostalom, kolektivno preuzimanje odgovornosti za čin koji je vrlo očito počinio pojedinac, opet je prikrivanje subjekta i raspršivanje prividno preuzete odgovornosti, jer za takvu „odgovornost“ čitav anonimni kolektiv ujedinjen samo pod imenom organizacije kojoj se ne zna ni članstvo ni vođe, opet ne može snositi nikakve konkretne posljedice. Sustav odgovornost pripisuje (često nestabilnom, društveno izoliranom ili socijalno nefunkcionalnom) pojedincu, kao izoliran čin jedne osobe, negirajući tako preuzetu

⁴⁸ Usp. Colarik, A. M., *Cyber terrorism – Political and Economic Implications*.

kolektivnu odgovornost. Nadalje, taj pojedinac najčešće dobije samo inicijale u medijima, uglavnom u svrhu sprječavanja rađanja kulta ili pojavljivanja imitatora, što opet vodi do potpunog nestanka subjekta u čitavoj sferi.

U takvom kaosu okolnosti i pravnih poteškoća, u kojem pravni sustav realnog svijeta pokušava žonglirati sve većim brojem problemskih loptica virtualnog svijeta, čini se da se ideja subjekta zapravo u potpunosti izgubila, i da je subjekt kao jasno definiran, odgovoran, svjestan i kompletan član neke zajednice, nešto što u cyber-sferi zapravo i ne postoji.

4. Pravne implikacije cyber-ratovanja

4.1. Pravni problemi: što je napad u cyber-sferi?

U prethodnom smo poglavlju pokušali usporediti cyber-sferu i realni svijet, te njihove stanovnike. Pokazali smo da je cyber-sfera daleko od tek virtualnog ogledala realnom svijetu. Vidjeli smo da su te dvije sfere izrazito različite, ali i izrazito isprepletene, i djelovanje u jednoj itekako može imati posljedice vidljive u drugoj. Naznačeno je također koliko je pravna regulacija cyber-sfere izazov čija realizacija tek čeka pravnike i zakonodavna tijela, te koliko to uistinu neće biti jednostavan zadatak.

Fokusirajmo se sada na same konfliktne situacije unutar cyber-sfere, i probleme specifične za to područje. Prvi problematičan pojam na koji tu nailazimo je upravo „napad“. Napad u cyber-sferi, odnosno cyber-napad, ključno je pokušati što jasnije definirati. Za razliku od napada jedne države na drugu u realnoj sferi u kojoj napad bude jasno prepoznat, cyber-sfera uključuje puno šire područje napada. Teško je razlučiti koja štetna djelovanja su „samo“ štetna djelovanja, a koja se mogu svrstati u domenu pravog napada, uz sve posljedice kojima to vodi.

Upravo je pokušaj stvaranja nekakvih općih smjernica i sugestija za buduću pravnu regulaciju bila ideja za nastanak dokumenta *Tallinn Manual on the International Law Applicable to Cyber Operations*. Taj je priručnik, koji je u međuvremenu doživio i drugo, prošireno izdanje, najbliže nekakvoj pravnoj regulaciji koju trenutno imamo u kontekstu pravila cyber-ratovanja. *Tallinn Manual* nije službeni dokument, ali je pokušaj izrade pravnog priručnika koji bi se fokusirao upravo na pitanja međunarodnog prava u cyber-ratovanju. U tom pogledu, nasljednik je nekoliko priručnika slične funkcije, poput priručnika o oružanim sukobima na moru (*San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, 1994.), ili u zračnom području (*Manual on the International Law Applicable to Air and Missile Warfare*, 2009.). Na njemu je radio međunarodni tim stručnjaka, s ciljem osvrta i neutralne analize trenutnih zakona i praksi, te predlaganja mogućih praksi u budućnosti s obzirom na trenutne zakone i stanje u cyber-sferi. Priručnik se također pokušava baviti i pitanjem subjekta, civila, suvereniteta i pitanja državne odgovornosti unutar cyber-sfere uopće, bilo u stanju rata, bilo u periodu mira.

Tallinn Manual u pokušaju općenitog definiranja cyber-napada navodi da je to “cyber operacija, bilo ofenzivna ili defenzivna, za koju se može razumski očekivati da će škoditi ili

uzrokovati smrt osoba, ili oštećenje ili uništenje objekata.”⁴⁹ Tu se definiciju također navodi kao važeću i u međunarodnim i u oružanim sukobima unutar neke države. No Manual ne staje samo na tom, to je tek polazišna točka. Preliminarno je također naglašeno da iako su cyber-operacije relativna novost u ratovanju, i samim time nedovoljno (odnosno gotovo uopće ne) regulirane, standardni zakoni vezani za oružane sukobe bi trebali vrijediti i u cyber-sferi. Nije svaka cyber operacija nužno i cyber napad, pa Manual pokušava razlučiti i kategorizirati vrste napada i što sve spada u napad, koji je napad u kojim uvjetima prihvatljiv a koji ne, te kako bi država u kojim od tih slučajeva trebala reagirati. Da bi operacija bila u domeni napada, mora uključivati državnu involviranost, te ne prepoznaje individualne akcije pojedinaca u tom kontekstu. Cyber-napad dakle podrazumijeva upletenost države u virtualni svijet, i prelijevanje međunarodnih odnosa i na cyber-sferu.

Manual se zbog tog odmah na početku bavi i pitanjem suvereniteta, te protežnosti suvereniteta na cyber-sferu. Prvo pravilo priručnika tako doslovno započinje naizgled vrlo jasnom rečenicom – „Princip suvereniteta države odnosi se i na cyber-sferu.”⁵⁰ Nadalje je naglašeno da različiti aspekti cyber-sfere i cyber-operacija nisu van dosega suvereniteta države, te da su „fizički, logički, i društveni slojevi cyber-sfere uključeni u princip suvereniteta.”⁵¹ Iako se cyber-sferu često smatra globalnim područjem, pa kao takva ne bi trebala ulaziti u područje državnih podjela, u kontekst cyber-ratovanja ulaze operacije koje se izvode i na fizičkom teritoriju, uključuju razne objekte, te ih izvode osobe nad kojima država ima moć. Također, suverenitet države se proteže i na cyber-infrastrukturu, osobe i cyber-aktivnosti locirane unutar državnog teritorija. Država je slobodna izvoditi cyber-aktivnosti u međunarodnim odnosima, ali u skladu s međunarodnim zakonima, te njeno djelovanje u cyber-sferi ne smije ugrožavati ili povrijediti suverenitet druge države.

Što se samih napada tiče, *Manual* uključuje i kategorije „međunarodno štetnih cyber-djelovanja“, te povrede internacionalnih pravnih dužnosti. Država također snosi odgovornost i za cyber-djelovanje državnih organa ili službenih osoba. Cyber-operacije provedene u kontekstu oružanog sukoba podložne su već postojećim zakonima o oružanim sukobima, pa se primjenjuju standardna pravila poput zabrane nanošenja nepotrebne patnje.

⁴⁹ Michael N. Schmitt (ur.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017., str. 415, Rule 92.

⁵⁰ Ibid, str.11, Rule 1

⁵¹ Ibid, str.12, Rule 1

U definiciju cyber-napada ne ulaze nenasilni činovi, poput špijunaže, iako, ukoliko je kao sredstvo špijunaže korištena nekakva metoda čije posljedice ulaze u definiciju napada, špijunaža ipak ulazi u sferu napada. Isto vrijedi i za druga cyber-djelovanja koja sama po sebi nužno nisu napad. „Nasilje“ se u tom kontekstu ne shvaća samo u smislu fizičke upotrebe sile (*Manual* koristi termin „kinetička“ sila), nasilje se shvaća u smislu nasilnih posljedica koje nisu limitirane na sam nasilan čin. Dakle, ukoliko je posljedica nekog naizgled ne-nasilnog djelovanja uzrokovala destruktivne posljedice, utoliko se smatra napadom. Cyber-napad se također može odnositi i na same podatke, a ne samo na fizičke osobe ili fizičke objekte. Tako npr. Pravilo 41 izričito naglašava da su arhivi, dokumenti ili službene korespondencije diplomatske prirode koji su u elektroničkom obliku nepovredivi. No podatci se ne mogu smatrati izravnim ciljem napada, jer cilj je definiran time da je „vidljiv i dodirljiv“. Ipak, *Manual* dodatno pojašnjava da „cyber-operacija koja za cilj ima podatke može biti smatrana cyber-napadom ukoliko utječe na funkcionalnost infrastrukture ili ima druge posljedice koje definiraju napad.“⁵²

U pokušaju definiranja napada i razlučivanja različitih potencijalno opasnih djelovanja od samog napada, također je važno ne brkati objekt napada s neprijateljem. Napad nije nužno samo na neprijatelja, i status objekta nije ono što definira napad, napad definiraju prvenstveno posljedice. Cyber-djelovanje koje kao posljedicu ima povredu civila ili drugih zaštićenih osoba, i dalje je napad. Terorizam se također u tom pogledu može smatrati napadom, jer je posljedica terora psihološka patnja, dakle nasilje nad osobama. Cyber-operacija koja je za cilj imala prouzrokovanje štete, ali je na vrijeme spriječena ili zaustavljena pa ne rezultira u fizičkoj šteti i dalje se smatra napadom.⁵³

Neki napadi su opravdani, a neki strogo zabranjeni. Kao i u „regularnom“ ratovanju u realnom svijetu, civili i neke određene kategorije zaštićenih osoba nikako ne smiju biti cilj napada. Na ovom je mjestu distinkcija cilja i slučajne žrtve krajnje problematično pitanje, jer iako civili ne smiju biti cilj napada, ukoliko spletom okolnosti budu žrtve zakonski dopuštenog napada (npr. na vojni objekt), taj se napad ne smatra napadom na civile. Iako to djeluje kao preciziranje u pravnom smislu, jasno je da dolazimo do etičkog problema, jer se takvom distinkcijom može manipulirati i zloupotrebjavati nijanse sive zone. Također, ukoliko je civil u nekom trenutku izravno angažiran u agresiju, gubi status civila i zaštitu, što je također opasno koketiranje sa sivom zonom.

⁵² Ibid.,str.437, Rule 100.

⁵³ Ibid.,str.419, Rule 92.

Što se tiče samih civila i zaštićenih osoba, ukoliko postoji nejasnost oko statusa pojedine osobe, preliminarno ju se smatra civilom. Osobe koje mogu biti objekti napada su prema Pravilu 96 pripadnici oružanih snaga, pripadnici organiziranih oružanih grupa, civili onoliko dugo dok su aktivni u agresiji i sudionici „*levée en masse*“⁵⁴. Teroristički napadi su također zabranjeni neovisno o tom radi li se o vremenu mira ili rata. Također, teroristički se napadi po svom cilju ili načinu provođenja uglavnom kategoriziraju kao napadi na civile, što ponovno spada u strogo zabranjenu kategoriju napada. Ovakvom kategorizacijom terorističkog napada također dolazimo do tog da se pokušava umanjiti snaga upravo toga teror elementa. Sintagma „teroristički napad“⁵⁵ sama po sebi kao cilj ima upravljanje strahom. Skidajući napadu „status“ terorističkog, i tretirajući ga kao napad na civile koji je po Međunarodnom ratnom pravu ionako strogo zabranjen, uzima mu se upravo ta snaga kontrole putem straha. Element straha naravno i dalje postoji, ali težina napada je preseljena sa straha kao cilja, na sigurnost civila kao cilj. S obzirom da je ideja terorizma u kontroli straha, ovaj način zapravo može biti vrlo efikasan način umanjivanja moći terorizmu. No ono što je zanimljivo u kontekstu terorističkih napada je to da iako su u kontekstu terora nad civilima (odnosno napada na civile) strogo zabranjeni, ako je cilj teroriziranja izazivanje straha kod neprijateljske vojske, taj tip napada nije zabranjen, što je s etičke strane problematično, čak i u kontekstu ratnog razdoblja. Ako kao područje djelovanja terorizma vidimo ljudsku psihu, i strah kao oblik psihološke patnje, onda bi i teroristički napad nad neprijateljskom vojskom ili osobama čiji status nije zaštićen, trebao ulaziti u područje nanošenja bespotrebne boli, što je prema Međunarodnom ratnom pravu zabranjeno.

Osim zaštićenih osoba, postoje i zaštićena područja. Civilni objekti ne smiju biti cilj cyber-napada, a cyber-infrastruktura može biti meta isključivo ako se smatra vojnom domenom. Iz obrnute perspektive, vojni objekti cyber-infrastrukture koji se primarno koriste u civilne svrhe također ne smiju biti ciljevi napada. Iz ovih preciziranih distinkcija vidljivo je koliko je uopće za regulaciju cyber-napada značajna distinkcija između civila i službene osobe, o čemu će više riječi biti dalje u tekstu. U kontekstu samog definiranja zakonitog ili nezakonitog cyber-napada, značajno je činiti distinkciju između civila kao mete napada i civila kao kolateralne žrtve zakonski dopuštenog napada (gdje je povreda civila nenamjerna i slučajna).

⁵⁴ Ibid.,str.425, Rule 425.

⁵⁵ Janczewski, Lech; Colarik, Andrew M., *Cyber Warfare and Cyber Terrorism*, Information Science Reference, Hershey – New York, 2008.

Značajna razlika između zakonitog i nezakonitog cyber-napada je i u svjesnosti i odgovornom donošenju odluka od strane zapovjednika i izvršitelja napada. U njihovo područje pravne odgovornosti ulazi uzeti u obzir sve preventivne mjere da bi se zaštitili civili i spriječila ili uvelike smanjila opasnost od kolateralnih žrtava, sa što je moguće većom sigurnošću procijeniti regularnost cilja napada i osigurati da su načini i sredstva provedbe cyber-napada u skladu sa zakonom. Država također snosi odgovornost zaštite vlastitog teritorija i cyber-infrastrukture u svrhu sprječavanja nanošenja štete drugoj državi (npr. kao nesvjesni posrednik cyber-napada).

Sve države koje sudjeluju u oružanim sukobima, bilo u realnom svijetu bilo u cyber-sferi, dužne su zaštititi određene skupine ljudi, te omogućiti nesmetano djelovanje nekih organizacija. Djeca su tako u potpunosti zaštićena kategorija, ne smiju ni na koji način sudjelovati u oružanim sukobima, ni kao akteri ni kao ciljevi napada. Država je dužna podnijeti sve mjere da se djecu (pod tim se smatraju sve osobe mlađe od petnaest godina) izuzme iz vojnih operacija, uključivo sa cyber-operacijama. Cyber-sfera to otežava zbog lake dostupnosti interneta te *online* angažmana djece, pa je pitanje zaštite djece u tom kontekstu šire od samo ratnog prava.

Pod osobe čija sigurnost i nesmetano djelovanje mora biti osigurano i nikad ne smije biti cilj cyber-napada (ili ikakvog vojnog napada) spadaju medicinsko osoblje, vjerske udruge, novinari i humanitarna pomoć. Osim što oni sami ne smiju biti cilj napada, bilo koji cyber-napad koji bi kao posljedicu imao ometanje ili potpuno sprječavanje djelovanja bilo koje od gore navedenih frakcija smatra se nezakonitim. Jednak status imaju i pripadnici ovih struktura na okupiranom ili neutralnom području, gdje je njihovo nesmetano djelovanje i dalje prioritet i smatra se zaštićenim od svakog, pa i cyber-napada.

Naposljetku, od cyber-napada moraju biti zaštićeni i prirodni okoliš te kulturno naslijeđe, koji se smatraju civilnim područjima, pa za njih vrijede ista pravila kao i pravila o zaštiti civila.

Iz ovog pokušaja ne samo definiranja, nego i stroge klasifikacije napada u cyber sferi, te utjecaja cyber-napada na realni svijet, može se uočiti koliko je važnosti stavljeno na odgovornost sudionika te nekakve ne samo pravne, nego i moralne kodekse ljudskog djelovanja, kako u okolnostima mira, tako i u okolnostima oružanih sukoba. Cyber-sfera, koliko god bila apstraktni, virtualni svijet, i dalje dodatnu vrijednost daje civilima, djeci te djelatnicima udruga čiji cilj je ne samo zaštita, nego generalna dobrobit ljudi. Sam napad je u

odnosu svih tih aktera, odnosno subjekta, i njihovih meta, odnosno objekta, a status i značaj mete ono je što čini najznačajniju razliku između zakonitog i neprihvatljivog napada.

4.2. Subjekt u cyber-ratovanju

U prethodnom smo poglavlju pokušali objasniti i kategorizirati vrste cyber-napada. U ovom je cilj pozabaviti se organizatorima i izvršiteljima tih napada. Vidjeli smo da je sam napad već izrazito kompleksan pojam čija klasifikacija uvelike ovisi o njegovom cilju i potencijalnim rezultatima. Subjekt je prema tome više od samog izvršitelja konkretnog napada, to je ona osoba koja snosi svu odgovornost za potencijalne posljedice o kojima je već bilo riječi. Prvo pitanje koje se tu postavlja je može li subjekt cyber-napada uopće biti fizička individualna osoba?

Već je spomenuta uloga države u cyber-ratovanju, pa možemo reći da je jedan od mogućih subjekata upravo država. Unutar same države, tu ulogu možemo dodijeliti vojsci, odnosno dodjeljivati odgovornost kao temeljni kriterij subjekta prema vojnoj hijerarhiji, od predsjednika kao vrhovnog zapovjednika pa niže po zapovjedništvima, sve do samog vojnika. Ako shvatimo subjekt cyber-ratovanja kao onog tko je nositelj odgovornosti za organizaciju, provedbu i rezultate cyber-napada, onda pod tu definiciju mogu spadati i razne državne institucije koje iz nekog razloga sudjeluju u cyber-sferi oružanih sukoba, ali i instance više od samih država, odnosno međunarodne organizacije i institucije, ili bilo koji savez dviju ili više država povezanih nekim međunarodnim sporazumom ili zajedničkim interesom.

Ratno pravo, pa u skladu s njim i *Tallinn Manual* prepoznaje sve ove kategorije kao moguće subjekte u cyber-operacijama. No sama osoba, pojedinac, bez etikete službene funkcije ili kolektivnog identiteta unutar neke od navedenih grupa, je problematična točka. Jednako kao što se civil uglavnom spominje kao (nedopuštena) meta, odnosno objekt djelovanja, te mu se nužno daje funkcija „zaštićene osobe“ koja mu se automatski oduzima ukoliko se civil angažira u agresiji i na bilo koji način aktivno sudjeluje u cyber-napadima, isto tako se individui dodjeljuje status civila, toliko dugo dok je se ne može kategorizirati pod jednu od gore navedenih „aktivnih“ skupina (pripadnik oružanih snaga, pripadnik političkog vrha, pripadnik sigurnosne agencije, pripadnik međunarodne organizacije, itd.) ili pod neku od „zaštićenih skupina“ (liječnik, djelatnik humanitarne udruge, misionar, novinar, itd.). Kao što smo u prethodnoj cjelini pokazali raspršivanje pojedinca u cyber-sferi općenito, i

nestajanje samog subjekta kao takvog, čini se da i cyber-ratovanje preferira manje ili više grupne „funkcije“ kao aktivne subjekte i nositelje odgovornosti.

Unutar samog *Manuala* primjetan je pokušaj da se čak i djelovanje službenih osoba svede pod odgovornost same države. Pravilo 15, već na samom početku *Manuala*, tako glasi: „Cyber-operacije koje provode organi države, ili osobe ili entiteti koji prema zakonima te države imaju autoritet državnog tijela, pripisuju se državi“⁵⁶. To pripisivanje odgovornosti proteže se dalje i na neke primjere naizgled individualne odgovornosti pojedinca, ili na grupe ili organizacije koje nisu dio službenih državnih tijela, ali surađuju s državom na određenim funkcijama unutar cyber-sfere (npr. timovi zaduženi za online-forenziku). Za takve slučajeve važno je naglasiti da država mora biti službeno nadležna djelovanju tih udruga da bi se njihovo cyber-djelovanje pripisalo odgovornosti države. Djelovanje koje bi izlazilo van okvira takvog dogovora više se ne pripisuje državi, ali na državi je i dalje da prema svojim zakonima reagira na moguće nezakonito djelovanje. Djelovanje službenih osoba koje se ne pripisuje državi su ratni zločini, za koje u cyber-sferi vrijede isti zakoni kao i u ratovanju općenito. Za ratne zločine provedene putem cyber-sfere odgovaraju njihovi organizatori i provoditelji, no država, odnosno konkretni zapovjednici preuzimaju odgovornost ukoliko je pod njihovom nadležnošću počinjen ratni zločin za koji su znali, ili pod danim okolnostima trebali znati te preventivno djelovati. Država je također odgovorna i za upotrebu cyber-strukture koja joj pripada, što dovodi do prvog većeg problema kod pitanja odgovornosti u cyber-ratovanju, a to je hakiranje.

U vremenu sveprisutnosti i dostupnosti interneta, nije teško zamisliti situaciju u kojoj anonimni pojedinac ili grupa hakira cyber-infrastrukturu⁵⁷ neke države da bi kreiranjem „zombie računala“⁵⁸ izvršila cyber-napad ili neku nezakonitu cyber-operaciju usmjerenu bilo lokalno, bilo globalno. Primjer takvog djelovanja može biti interferiranje u, primjerice, bankovni sustav jedne države, ili čak međunarodni bankovni sustav, čije makar privremeno nefunkcioniranje može imati izrazito negativne i dugoročne posljedice. Iako su računala koja su „krivci“ za takvu situaciju pod kontrolom jedne ili više država, ne može se preliminarno

⁵⁶ M. N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, str. 87., Rule 15

⁵⁷ cyber-infrastruktura uključuje sve elemente u realnom svijetu (računala, razne druge uređaje itd.) koja služe realizaciji elektroničkog sustava.

⁵⁸ način referiranja na osobna računala na koja je bez vlasnikovog znanja i pristanka instaliran malware (zlonamjerni software, npr. virus), i koja autor tog malwarea zloupotrebljava za napad na neki drugi software, npr. bankovnog sustava; koristi se riječ “zombie” jer računala tad poput zombija provode operacije kojih njihovi vlasnici nisu svjesni.

pripisati odgovornost tim državama, a lociranje pravog subjekta iza čitave situacije može biti izrazito teško. Čak i ako se subjekt locira, pitanje pod čiju jurisdikciju spada provođenje kaznenih mjera je problematično.

Za ovakve situacije nije teško pronaći primjere u stvarnom svijetu. Haker koji po zakonima spada u sustav jedne države može u ime druge države ili pojedinih članova te države raditi protiv treće države, njenih članova ili institucija, ili čak čitavih međunarodnih udruženja. Vrlo je nezgodno u takvoj mreži odlučiti tko je uistinu djelovao kao subjekt. Ukoliko hacker npr. *online* prodaje uslugu provaljivanja u neku sustavom (od jednostavnih šifri do složenih sustava) zaštićenu cyber-lokaciju, to samo po sebi već spada u cyber-zločin, i država čiji je dotični hacker stanovnik ima pravo u skladu sa važećim zakonima kazniti to djelovanje. Postavlja se pitanje kako regulirati sustav kazne takvim prekršajima. Jedan fragment takvih prekršaja može spadati u špijunažu, npr. provala u nečiji osobni blog ili profil na društvenoj mreži, no po tom bi se trebao kažnjavati i svaki privatni detektiv koji prodaje uslugu praćenja neke osobe i fotografira njeno kretanje. Druga strana spektra su provale u sustave koji imaju puno šire područje djelovanja, i čije narušavanje može imati dalekosežne posljedice za puno veće skupine ljudi, pa i čitave države. Nadalje, hacker se uvijek može braniti neupućenošću u širu sliku. On „samo prodaje uslugu razbijanja šifre“, ne mora pritom uopće znati što ta šifra štiti. Kažnjavanje se opet svodi samo na odgovornost za sam čin provale, a ostale se posljedice pripisuju kupcu usluge. Taj kupac usluge onda opet može biti u potpunosti anonimn i do njega može biti gotovo nemoguće doći.

Ili, kao što je slučaj s cyber-grupom Anonymous, može istovremeno biti i anonimn i javan. Pod vrlo otvorenim imenom grupe može se skrivati bilo tko, a kolektivitet grupe preuzima odgovornost za bilo koji čin. Kažnjavanje čina tako je sličan lovu na duhove, i to na globalnoj razini, jer nemoguće je istovremeno provoditi suđenje nad tolikom grupom ljudi, čak i kad bi njihov identitet bio poznat. Isti problem se pojavljuje i kod preuzimanja odgovornosti od strane terorističkih grupa, o čemu je već bilo riječi.

Pitanje tko je u cyber-ratovanju subjekt može također izaći iz konteksta odgovornosti samih ljudi. Sve više *online* sustava programirano je s ciljem približavanja umjetnoj inteligenciji. Ti sustavi (poput Google Translatea⁵⁹) programirani su da s vremenom i interakcijom s korisnicima skupljaju informacije i pritom „uče“. Osnova njihovog djelovanja

⁵⁹ Google Translate = usluga korporacije Google za automatsko online prevođenje teksta s jednog jezika na drugi.

je programirana, ali detaljnije postupke uređaj, odnosno sustav, formira sam. To na prvi pogled može zvučati kao scenarij SF filma, ali zapravo, takvim smo sustavima svi već okruženi. Računala se sama spajaju na Internet i provjeravaju nove informacije o potencijalnim virusima, šalju međusobno informacije, sami optimiziraju sustav. Pametni telefoni koje danas na Zapadu posjeduje već i gotovo svaki maloljetnik, sami rade ažuriranje čitavog sustava i nadograđuju aplikacije. Čitav niz uređaja s kojima imamo svakodnevnu interakciju, ima određenu nijansu „autonomije“ rada, gotovo neovisno o nama. Razni sateliti i uređaji poslani u svemir bez ljudske posade sami rade manje ili više složene popravke i informiraju o tom svoje centrale. Već je spomenuto koliko jednostavno je bilo koji od tih uređaja pretvoriti u „zombie“ uređaj, o čijem pozadinskom funkcioniranju ne moramo uopće imati pojma, ali to je posljedica direktnog napada na uređaj. No što ako se dogodi da uređaj ili sustav koji je programiran sam „učiti“ i proširivati svoje područje djelovanja, „nauči“ nešto krivo? Što ako dođe do neke greške u sustavu koja potencijalno može rezultirati, ili uistinu rezultira, takvim nanošenjem štete da se može po prije navedenoj klasifikaciji proglasiti cyber-napadom? Snosi li programer odgovornost? Država u čijoj cyber-strukturi je došlo do greške? Ukoliko se radi o međunarodnom sustavu (npr. već spomenuti Google), može li se krivnja pripisati državi na čijem je teritoriju sasvim slučajno, greškom koja je van ičijeg svjesnog djelovanja, došlo do „spontanog djelovanja“ uređaja ili sustava? Može li AI⁶⁰ završiti na sudu kao osumnjičenik?

Ta se pitanja mogu činiti apsurdna, ali u vremenu sve bržeg razvoja cyber-svijeta, a tim i cyber-ratovanja, mogućnost pojavljivanja ne-ljudskog cyber-subjekta, i njegovo potencijalno mjesto u sustavu, nije nešto što bismo trebali olako odbaciti. Naravno, uvijek se možemo voditi za tim da je svijest, kao mogućnost racionalizacije koja je tipično ljudska, nužan preduvjet za odgovornost djelovanja i samim tim mogućnost da se bude subjekt u bilo kojem kontekstu, pa tako i u pravnom. Uostalom po istom principu su djeca isključena iz pravne odgovornosti (zbog još nedovoljno razvijene mogućnosti racionalizacije), i po istom principu ne „krivimo“ i ne provodimo suđenja nad životinjama ili elementarnim nepogodama, ma koliko štete i ljudske patnje skrivile. No ako prihvatimo da je u srži umjetne inteligencije (ili čak jednostavnijih oblika automatizacije programa ili uređaja) samostalno učenje i reprogramiranje (koje se može shvatiti kao ona promjena koju smo već spominjali kao jednu od glavnih karakteristika čovjeka kao bića), možemo li sa sigurnošću isključiti govor o racionalizaciji unutar djelovanja sustava ili uređaja? I djeca učenjem i upijanjem informacija

⁶⁰ Artificial Intelligence (umjetna inteligencija).

kroz interakciju s okolinom dolaze do razvijene mogućnosti racionalizacije i statusa odrasle osobe, pa ukoliko automatizirani sustav, ili možda u jednom trenutku uistinu umjetna inteligencija, istim principima uči i razvija se, za pretpostaviti je da dolazi i do tog da ima dovoljno informacija i mehanizama za filtriranje podataka i opcija, što bi se moglo smatrati umjetnom racionalizacijom. Uključivanje umjetne inteligencije u pravni sustav se pod takvim pretpostavkama više čini kao neizbježno, nego kao apsurdno, i vraća nas pitanju – može li subjekt u cyber-ratovanju biti nešto što uopće nije čovjek? No to pitanje zasad ostaje otvoreno, iako je jedan fragment njega već postavljen u kontekstu javnih rasprava o upotrebi bespilotnih letjelica i dronova u ratovanju. Dronovi se čine kao efikasna zamjena pilotu, jer iako njima ipak netko mora pilotirati, to pilotiranje se radi sa sigurne udaljenosti, štiteći život pilota tako što ga se direktno uklanja s bojišnice. To iz moralne perspektive zvuči kao odlična alternativa riziku ljudskog života, no realnost je drukčija. Činjenica je da dronovi ostavljaju puno prostora za pogrešku i riskiranje života civila, a koketiraju i sa problematikom ciljanih ubojstava, koja su već vrlo nezgodna siva zona. Problem je i način procjene civila, jer npr. “Američke procjene o ekstremno malom broju ili o nepostojanju civilnih žrtava u napadima dronovima temelje se na suženoj definiciji 'civila', prema kojoj se pretpostavlja da su, osim ako se ne dokaže suprotno, pojedinci ubijeni u napadima bili militant”.⁶¹

Što se tiče statusa subjekta unutar samih oružanih sukoba, članovi oružanih snaga i volonteri suradnici oružanim snagama su, barem u kontekstu ratovanja u realnom svijetu, jasno definirani. Prema Ženevskoj Konvenciji, moraju nositi vidljive oznake i mora ih se moći jasno na prvi pogled razlikovati od civila, eventualno oružje također mora biti jasno vidljivo, moraju djelovati pod zapovjedništvom jasno definirane službene osobe te provoditi operacije u skladu sa zakonima o oružanim sukobima. Prema tim je kriterijima definiran status ratnika donosi i određene beneficije, poput zakona o tretiranju ratnih zarobljenika i određenih imuniteta. Iste beneficije bi se trebale prenositi i na one subjekte koji sudjeluju u cyber-operacijama, naravno pod pretpostavkom da zadovoljavaju gore navedene kriterije. No, u slučaju sudionika u cyber-operacijama, prioritet je stavljen na pripadanje jasno definiranoj i strukturiranoj organizaciji. Inače bi se riskiralo to da se status ratnika oslabi u kontekstu prevelike pojave raznih samoproglašanih virtualnih organizacija, koje bi mogle zadovoljavati sve gore navedene kriterije, a da zapravo nisu suradnici ili dio službenih oružanih snaga. Vrlo je važno raditi distinkciju između takvih aktera, jer naizgled identične cyber-operacije mogu

⁶¹ Kelam, Ivica, U sjeni dronova – etički aspekti upotrebe dronova u ratu protiv terorizma, *Filozofska istraživanja*, 36(2016)4, str. 671-691.

imati u potpunosti različite ciljeve i posljedice, i prema tim razlikama ulaziti ili izlaziti iz domene legalnog cyber-ratovanja. Svaki akter u cyber-sferi ne može biti shvaćen i kao subjekt cyber-ratovanja, jer je ono što bi trebalo biti glavna distinkcija subjekta u cyber-ratovanju, i online-subjekta općenito, upravo u razlici odgovornog djelovanja i podložnosti operacije različitim tipovima zakona. Subjekt u cyber-ratovanju tako bi trebao biti onaj akter čije djelovanje je regulirano zakonom o oružanim sukobima, dok drugi provoditelji cyber-operacija spadaju pod druge jurisdikcije.

4.3. Cyber-subjekt vs. cyber-civil

Odvojivši u prethodnom dijelu subjekt cyber-rata od subjekta u cyber-sferi općenito, vrijeme je napokon postaviti pitanje tko je onda u cyber-sferi civil, naročito u kontekstu cyber-ratovanja. Vidjeli smo da je kroz razne pravne regulacije i zakone (naročito zakone o oružanim sukobima), bilo realnog svijeta bilo cyber-sfere, civil u principu prikazan kao gotovo pasivan objekt kojeg se promatra ili u kontekstu načina na koji ga se može i treba zaštititi, ili u kontekstu nedozvoljene mete napada ili kolateralne žrtve. Uz regulacije vezane uz prava i zaštitu civila u oružanim sukobima vrlo često stoji dodatno preciziranje da ukoliko civil svjesno i odgovorno počini ikakav čin kojim bi sudjelovao u agresiji, automatski gubi status i prava civila – dakle postaje subjekt, a ne više objekt. Takav naizgled paternalistički pristup prema civilima ima smisla s pravne strane, jer ikakvim aktivnim djelovanjem civili izravno ulaze u sustav, i njihovo se djelovanje gleda iz perspektive legalnog ili nelegalnog.

Također, vidljiva je tendencija da se svako djelovanje u kontekstu oružanog sukoba klasificira ili kao izravno vojno (bilo u sklopu same vojske, bilo u sklopu organizacija koje djeluju pod okriljem ili u suradnji s vojskom), ili kao neko od zaštićenih (liječnici, volonteri, novinari itd.) djelovanja. Bilo koji čin koji uključuje svjesno i odgovorno djelovanje time je oduzet civilima – moglo bi se reći da im se zapravo oduzima subjektivitet, i da ih se uistinu gura u kategoriju pasivnog objekta, jer svako djelovanje je prijelaz u domenu odgovornog subjekta, a to se nadalje kategorizira i gotovo nužno izlazi iz kategorije civila.

No postoji li u kontekstu cyber-sfere, pa i samog cyber-ratovanja, uistinu takva pozicija na kojoj je osoba samo pasivni objekt-civil? Jasno je tko su civili u realnom svijetu – praktički svi oni ljudi koji nisu u nekom obliku uniforme i ne izvršavaju neku jasnu službenu

funkciju u ratu. Ipak, samim spajanjem u virtualni svijet mi u njemu postajemo aktivni i preuzimamo nekakav oblik odgovornosti. Jesmo li onda *online* ikada uistinu civili?

Država kao „glavna“ instanca u cyber-ratovanju, kao vrhovni odgovorni subjekt, dužna je pokušati preventivno zaštititi svoje cyber-sustave koji se na bilo koji način tiču civila i koji mogu imati utjecaj na civile. To se naravno odnosi na velike sustave i na same cyber-operacije u kojima se treba osigurati da prilikom njihovog izvođenja civili ne budu oštećeni, i da nemaju negativne posljedice za civile. Ipak, već tu je postavljena iznimka individualne odgovornosti civila. Tako, na primjer, ukoliko se civili slučajno, ili na vlastitu odgovornost nađu u blizini objekta koji je legitimna meta cyber-napada, te kao takvi budu kolateralna žrtva, država se ne može držati odgovornom što ih nije zaštitila. Isti se princip može primijeniti i na samo *online* djelovanje civila. Spomenuti su već zombie-uređaji kao rezultat ili mehanizam *incognito* cyber-napada. Ne može se očekivati da država bude ta koja štiti svaki osobni uređaj svojih civilnih građana, štoviše, pokušaj takvog preventivnog djelovanja značio bi narušavanje privatnosti i temeljnih sloboda građana.

Osobna odgovornost trebala bi stoga biti preduvjet aktiviranju *online* uopće. Individualno preventivno djelovanje i upućenost u rad uređaja i sustava koje koristimo *online* trebale bi biti norma odgovornog egzistiranja u cyber-sferi, jer neznanje i nemar mogu imati dugotrajne i opasne posljedice. Civil koji u oružanom sukobu postane aktivno uključen u agresiju gubi status civila – isto pravilo bi se moglo primijeniti i na online-sferu. Moramo biti svjesni mogućnosti koje otvaramo svojim djelovanjem *online*, i sami se osigurati od tog da iz neznanja ili nezainteresiranosti postanemo zombie-subjekt, odnosno nesvjesni akter u cyber-napadima. Neznanje i nezainteresiranost, u vremenu sve veće isprepletenosti online-sfere i realnog svijeta te vrlo realnih fizičkih posljedica virtualnog djelovanja, ne smiju biti razlog izuzimanju iz odgovornosti.

Pitanje odgovornosti civila ne staje samo na zaštiti osobnih uređaja i sprječavanju neautoriziranog djelovanja tim uređajima. Pitanje civilne odgovornosti postaje nezgodno kad su u pitanju objave na web-stranicama. Dok npr. objavljivanje potencijalno problematičnih podataka na osobnim blogovima ili profilima na društvenim mrežama može državi prouzročiti nezgodnu, pa i potencijalno opasnu situaciju, ipak nije na državi da intervenira u takvo objavljivanje, dok god ono spada u slobodu govora, a ne krši neki drugi zakon (npr. dok se ne radi o govoru mržnje ili huškanju na nasilje). No ukoliko neka web-stranica koja je vezana uz državno relevantne funkcije i usluge (npr. za plaćanje i prijavu poreza) postane

kompromitirana, država mora djelovati i ugasiti ju. Dakle iako država ne može intervenirati u svako djelovanje online, na samim civilima je da procijene i razluče koji način djelovanja je prihvatljiv na kojoj web-stranici, i da budu svjesni toga da je objavljivanje na web-stranicama podložno zakonu, baš kao i svako javno i privatno djelovanje u realnom svijetu.

Individualno djelovanje također može biti puno veće i s puno dalekosežnijim posljedicama od objavljivanja blog postova ili Youtube⁶² videa s osobnim stavovima o političkim pitanjima. Zanimljiva situacija koju *Tallinn Manual* navodi kao primjer je cyber-napad jedne države na drugu, u kojoj država čiji je suverenitet na taj način povrijeđen iz nekog razloga ipak ne reagira protu-mjerama na koje realno ima pravo. U takvoj se situaciji može dogoditi da neka individualna privatna osoba, koja ima dovoljno znanja i resursa, počini cyber-akciju koja bi kontrirala državi-agresoru i natjerala je da zaustavi svoje štetno cyber-djelovanje. Takav gotovo romantičan, „junački“ čin bi s moralnog gledišta možda i bio razumljiv, ali je u kontekstu cyber-ratovanja ipak nelegalan, i može dovesti do tog da ona prva država sada legitimno reagira protumjerama protiv već napadnute države, jer ta druga država nije spriječila svog stanovnika da privatnim djelovanjem i korištenjem cyber-infrastrukture sa svog teritorija ugrozi sigurnost druge države. Unatoč herojskoj namjeri obrane vlastite države, privatna osoba nije autorizirana za takvo djelovanje u cyber-sferi, te ulazi u područje svjesnog sudjelovanja u agresiji u kontekstu međunarodnog sukoba. Već je napomenuto da u takvim okolnostima osoba gubi status civila, iz čega proizlazi da je zapravo temeljna odgovornost civila u online sferi upravo to da osigura samom sebi zadržavanje statusa civila u svom online djelovanju. Štoviše, pravila 91 i 97 u *Tallinn Manualu* izričito naglašavaju da iako civilima nije izravno zabranjeno sudjelovanje u cyber-operacijama, oni ipak gube status civila i svu zaštitu koja iz tog slijedi dok god su aktivni u operaciji ili bilo kojem drugom djelovanju koje se može shvatiti kao agresija ili cyber-napad. Dakle civili teoretski mogu postati subjekt u cyber-ratovanju, ali samo teoretski, jer u trenutku prelaska iz teorije u praksu gube status civila dok god imaju status subjekta.

Iz svega navedenog proizlazi da su, barem u kontekstu cyber-ratovanja, civil i subjekt (odnosno cyber-civil i cyber-subjekt) pojmovi koji se međusobno isključuju. Civil je onaj koji je u potpunosti zaštićen, ali samo dok je pasivan – subjekt se postaje aktivnim djelovanjem i preuzimanjem (određene doze) odgovornosti za čin. No u trenutku postajanja subjektom, prestaje se biti civil. Subjekt u cyber-ratovanju može biti bilo koja službeno

⁶² Youtube = web-stranica koja pruža uslugu uploadanja videa na osobne kanale i gledanje drugih videa, od glazbenih spotova do osobnih vlogova (video blogova)

prepoznata osoba, od volontera do vojnih osoba; organizacija ili čak čitavih država ili alijansi više država. Čak i međunarodne organizacije mogu biti subjekti. No civil u cyber-ratovanju svoje mjesto nalazi tek kao minimalno aktivan objekt, čija se aktivnost svodi na individualno preventivno djelovanje i oprezno ophođenje u vlastitom online-djelovanju. Sve dalje od toga nužno vodi u promjenu statusa.

5. Zaključak: subjekt na kušnji

Određenje subjekta jedno je od najtežih određenja u povijesti filozofije. Pokazali smo u prvome dijelu kako se subjekt postupno formirao u pozicijama pojedinih filozofa i epoha u kojima su djelovali. Nakon što se u filozofijskim teorijama uspjelo odrediti subjekt u njegovu misaonom i stvarnom postavljanju, suvremeno nas je doba svojim tehnološkim dostignućima – syber-sferom, ponovno vratilo pitanju određenja subjekta. Novo, tehnološko doba ponovno je subjekt učinilo problematičnom kategorijom – on u svojoj raskrivenosti ponovno postaje skriven, što pred filozofiju predstavlja nove izazove i upravo nju proziva da formuliра svoj sud. U sad već čuvenoj Heideggerovoj izjavi kako znanosti na misle, odnosno kako pitanje o tehnici nije tehničko pitanje jer se znanosti ne pitaju o biti tehnike, nalazimo se kao filozofi prozvani dati svoje mišljenje upravo o ovoj biti tehnike i tehnologije. Pojavom i razvojem interneta ponovo se otvorilo pitanje subjekta. Što, odnosno tko je subjekt, kako ga i po kojim kriterijima definirati, te na koji način ga smjestiti u svijet u kojem egzistira, pitanja su na koja je teško odgovoriti i kada se govori isključivo u kontekstu realnog svijeta. Unatoč tome što filozofi, a i drugi znanstvenici kako prirodnih, tako i društvenih i humanističkih znanosti, tu raspravu vode još od antičkih vremena, čini se da do danas nije ni približno zaključena čak ni kad se gleda samo fizička stvarnost. Postoje razne teorije i struje razmišljanja o subjektu, ali jasnog konsenzusa nema – subjekt i dalje ostaje natuknica u rječniku koja uz sebe veže mnoga moguća objašnjenja. Uz pitanje subjekta nužno ide i pitanje realnosti uopće. Svijet i iskustvo svijeta tako su teme koje su paralelno zaokupljale pažnju filozofa.

Internet, i seljenje jednog dijela ljudskog života u virtualni svijet, dodatno kompliciraju situaciju. Taj nejasno definiran subjekt prelazi iz sfere realnog u sferu virtualnog. Ipak, subjekt tamo nije samo avatar, virtualna varijanta fizičke osobe. To biće unutar virtualnog svijeta je dio onog bića iz realnog svijeta (kako smo pokazali kod Husserla da transcendentalno Ja pretpostavlja empirijsko Ja), nisu jasno odvojivi, njihova djelovanja se preklapaju i s vremenom njihovi svjetovi postaju sve isprepleteniji. Aktivnosti koje provodimo online imaju i utemeljenje i posljedice u svijetu „offline“ – realnom svijetu. Virtualno je u potpunosti zamijenilo mnoge elemente do nedavno rezervirane za realno – od novca kojim raspolažemo do međuljudske interakcije. Također, kako je još Husserl natuknuo u svom analiziranju ideje realnosti, virtualni svijet možda i nije fizički dio realnog, ali to ne umanjuje logičku mogućnost da ga se razumije kao uistinu realan svijet izvan nama poznatog realnog svijeta.

Osim što je sfera virtualnog sama po sebi problematična za definiranje i reguliranje, jer je njen prostor nešto toliko apstraktno da nam ga je gotovo nemoguće zamisliti, ta sfera također brzo raste. Nešto što je prije tridesetak godina jedva bilo u začetku, i za što se činilo kako nikada neće postati dostupno publici široj od one vrlo uske grupe informatičara koji su se tada time bavili, postalo je svakodnevnica širokom spektru ljudi. Internet je dostupan gotovo u svakom trenutku, s gotovo svakog djelića Zemlje. Prosječna osoba na Zapadu posjeduje barem jedan do dva uređaja preko kojih u bilo kojem trenutku može biti umrežena. Štoviše, velika većina zapadnjaka danas ne samo da u bilo kojem trenutku može biti *online*, nego je stalno *online*, makar pasivno. Mnogi uređaji iz svakodnevne upotrebe samostalno se spajaju na Internet, „uče“, rade stvari umjesto nas, i dobar dio ljudi uglavnom niti ne zna koje sve procese i aktivnosti njihovi elektronički uređaji rade.

Naravno, sama tehnologija po sebi nije ni dobra ni loša – ta klasifikacija ipak ovisi o ljudskom djelovanju i načinima na koji tehnologiju koristimo. Sudjelovanje u virtualnom svijetu pretpostavlja razinu svijesti i odgovornosti koju bi svaki pojedinac trebao prvo naučiti u realnom svijetu, a onda prenijeti u cyber-sferu. No to postaje sve teže. Sve se ranije spajamo na internet i aktiviramo u virtualni svijet, a on ipak nije čista preslika realnog da bismo se mogli pouzdati u intuitivno djelovanje i to da će ljudi (a naročito djeca), koji nisu još racionalno i moralno formirani i učvršćeni ni u stvarnom svijetu, odgovorno i moralno djelovati i u cyber-sferi. Djelovanje *online* fragmentarno je, rascjepkano i vremenski i prostorno, i teško je sve naše virtualne aktivnosti gledati kao koherentno djelovanje jedne osobe. Dapače, individualne instance našeg djelovanja u području virtualnog vrlo su često apsolutno nepovezane i kontekstualno odvojene.

U kontekstu cyber-ratovanja, tendencija je pokušati što je moguće efikasnije prenijeti međunarodne ratne zakone i pravila na cyber-sferu. Jedan od ključnih procesa tu je odvojiti legitimno od nelegitimnog djelovanja, dozvoljene od nedozvoljenih meta napada i metoda ratovanja, te na poslijetku, službene aktere od neautoriziranih individua koje djeluju samoinicijativno. Subjektom se u cyber-ratovanju tako smatraju razne osobe na sustavno definiranim funkcijama, čije djelovanje autorizira nositelj odgovornosti prema hijerarhiji. Osobe bez „službenog statusa“, bilo aktivno vojnog, bilo u smislu zaštićenih osoba poput humanitaraca i liječnika, smatraju se civilima, ali civil je u tom kontekstu tek minimalno aktivan, ili u potpunosti pasivan objekt kojeg treba maksimalno zaštititi i zapravo izolirati iz aktivnosti. Bilo kakvim aktivnim sudjelovanjem status civila se gubi.

Vidljiva je tendencija da se pojam 'subjekt' sve više veže uz apstraktnu funkciju, a sve manje uz individualne osobe. Uzme li se u obzir još i fragmentiranost i nekoherentnost digitalnog footprints koji ostavljamo u virtualnom svijetu, pitanje o tom tko je subjekt u cyber-sferi, ili preciznije u cyber-ratovanju, sve više počinje izgledati kao pitanje postoji li uopće *subjekt* u virtualnom svijetu. Ta pitanja zasad ostaju neodgovorena, a subjekt kakvog smo dosad poznavali, ostaje na kušnji.

Popis literature:

- Aristotel, *Fizika*, Sveučilišna Naklada Liber, Zagreb, 1987.
- Barnes, Jonathan (ur.), *The Cambridge Companion to Aristotle*, Cambridge University Press, 1995.
- Barry Smith; Smith, David (ur.), *The Cambridge Companion to Husserl*, Cambridge University Press, 1995.
- Colarik, Andrew M., *Cyber terrorism – Political and Economic Implications*, Idea Group Inc., London, 2006.
- Descartes, René, *Discours de la méthode*, Éditions Gallimard, Paris, 2009.
- Ferrari, G. R. F (ur.), *The Cambridge Companion to Plato's Republic*, University of California, Berkeley, Cambridge University Press, 2007.
- Folnegović-Šmalc, Vera, *DSM-IV- Dijagnostički i statistički priručnik za duševne poremećaje*, Naklada Slap, Jastrebarsko, 1996.
- Guyer, Paul (ur.), *The Cambridge Companion to Kant*, Cambridge University Press, 1992.
- Hill, Thomas E, Jr (ur.), *The Blackwell Guide to Kant's Ethics*, Blackwell Publishing Ltd., Oxford, 2009.
- Hobbes, Thomas, *Levijatan*, Naklada Jesenski i Turk, Zagreb, 2013.
- Husserl, Edmund, *Ideje za čistu fenomenologiju i fenomenologijsku filozofiju*, Naklada Breza, Zagreb, 2007.
- Martin, Heidegger, *Bitak i vrijeme*, Naprijed, Zagreb 1985.
- Janczewski, Lech; Colarik, Andrew M., *Cyber Warfare and Cyber Terrorism*, Information Science Reference, Hershey – New York, 2008.
- John Cottingham, John (ur.), *The Cambridge Companion to Descartes*, Cambridge University Press, 1992.
- Jonas, Hans, *Princip odgovornost*, Veselin Mesleša, Sarajevo, 1990.
- Jurić, Hrvoje, *Etika odgovornosti Hansa Jonasa*, Pergamena, Zagreb, 2010.

- Kant, Immanuel, *Pravno-politički spisi*, Politička kultura, Zagreb, 2000.
- Kelam, Ivica, U sjeni dronova – etički aspekti upotrebe dronova u ratu protiv terorizma, *Filozofska istraživanja*, 36(2016)4, str. 671-691.
- Platon, *Država*, Naklada Jurčić d.o.o, Zagreb, 2009.
- Polettiand, Anna; Rak, Julie (ur.), *Identity Technologies Constructing the Self Online*, The University of Wisconsin Press, 2014.
- Santas, Gerasimos (ur.), *The Blackwell Guide to Plato's Republic*, Blackwell Publishing Ltd, Oxford, 2006.
- Schmitt, N. (ur.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.
- Simon, Robert L. (ur.), *The Blackwell Guide to Social and Political Philosophy*, Blackwell Publishers Ltd, Oxford, 2002.
- Sorell, Tom (ur.), *The Cambridge Companion to Hobbes*, Cambridge University Press, 1996.
- Springborg, Patricia (ur.), *The Cambridge Companion to Hobbes's Leviathan*, Cambridge University Press, 2007.
- Sunajko Goran, *Metafizika i suverenost – Analiza modernih teorija suverenosti*, Hrvatsko filozofsko društvo, Zagreb, 2015.
- Sunajko, Goran, Ontologija »objektivnog neprijatelja« kao nebića: Hannah Arendt i Carl Schmitt, *Filozofska istraživanja* 36(2016)4, str. 753-774.
- Wood, Andrew F.; Smith, Matthew J., *Online Communication – Linking Technology, Identity, and Culture*, Lawrence Erlbaum Associates, Mahwah, New Jersey, 2005.
- Zovko, Jure (ur.), *Klasici metafizike*, Hegelovo društvo, Zadar, 2008.