REPUBLIKA H
VISOKI UPRAVNI SUD REPUBLIKE HRVATSKE
ZAGREB
Frankopanska 16

Klasifikacijski broj: UsII-118/23-7

U IME REPUBLIKE HRVATSKE

PRESUDA

Visoki upravni sud Republike Hrvatske u vijeću sastavljenom od sudaca toga suda Senke Orlić-Zaninović predsjednice vijeća, Eveline Čolović Tomić i Jelene Rajić, članica vijeća te sudske savjetnice Nele Petrović, zapisničarke, u upravnom sporu tužitelja TELEMACH HRVATSKAd.o.o., Zagreb, Josipa Marohnića 1, OIB: 70133616033, po opunomoćeniku odvjetniku iz Odvjetničkog društva protiv tuženika HRVATSKE REGULATORNE AGENCIJE ZA MREŽNE DJELATNOSTI, Zagreb, Ulica Roberta Frangeša-Mihanovića 9, OIB: 87950783661, radi povrede odredbe članka 43. Zakona o elektroničkim komunikacijama, na sjednici vijeća održanoj 3. listopada 2023.

presudio je

I Odbija se tužbeni zahtjev tužitelja za poništavanje odluke Hrvatske regulatorne agencije za mrežne djelatnosti, KLASA: UP/I-344-07/23-01/33, URBROJ: 376-05-2-23-07 od 6. srpnja 2023.

II Odbija se prijedlog za određivanje privremene mjere.

III Odbija se zahtjev za naknadu troškova postupka.

Obrazloženje

1. Rješenjem tuženika utvrđeno je da tužitelj postupa protivno odredbi članka 43. stavku 1. i stavku 2. Zakona o elektroničkim komunikacijama ("Narodne novine, broj 76/22, dalje: ZEK) na način da nadzire SMS promet između krajnjih korisnika i blokira određene vrste SMS poruka koje ne predstavljaju sigurnosni rizik ili napad na elektroničke komunikacijske mreže i usluge te koje mjere nisu nužne za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga, pa mu se zabranjuje primjena mjera nadzora SMS prometa i blokade SMS poruka koje ne predstavljaju sigurnosni rizik ili napad na elektroničke komunikacijske mreže i usluge i koje nisu nužne za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga te mu se nalaže da odmah po primitku rješenja uskladi svoje postupanje s člankom 43. stavkom 2. ZEK-a i ukine primjenu takvih mjera nadzora i blokade SMS prometa, sve uz prijetnju izricanja novčane kazne, odgovornoj osobi izvršenika, u iznosu od 7.000,00 eura/152.741,50 kn i daljnje novčane kazne za slučaj neispunjenja naloga.

2. Tužitelj osporava zakonitost takvog rješenja tvrdnjom da je u rješenju, kao i tijekom provedenog inspekcijskog postupka, pogrešno i nepotpuno utvrđeno činjenično stanje te je potom pogrešno primijenjeno relevantno materijalno pravo. Pojašnjava da je u obrazloženju pobijanog rješenja navedeno je da je tuženik dana 3. ožujka 2023. pokrenuo postupak inspekcijskog nadzora nad tužiteljem temeljem čl. 16. st. 1. t. 25. i čl.161. i 162. ZEK-a, a u vezi s utvrđivanjem postupanja tužitelja sukladno odredbi čl. 43. ZEK-a, da je inspektor samostalnom provjerom u vremenskom razdoblju od 24. veljače 2023. do 2. ožujka 2023., slanjem SMS poruka s brojeva na brojeve, koji se nalaze u TELEMACH mreži, čiji je sadržaj identičan ili sličan sadržaju poruka koje aplikacije redovito šalju korisnicima prilikom verifikacije korisničkih računa (npr. Facebook, Google, Instagram i sl.) utvrdio kako predmetne poruke nisu isporučene primateljima, dok su istovremeno istim primateljima isporučene poruke sadržaja ,,Test ili/i ,,Proba". Primjeri sadržaja poruka koje nisu isporučene su sljedeći: ,,Account is your Samsung account verification code", "Use for two-factor authentification on Facebook" te "G- is your Google verification code". Dalje je navedeno da su poruke istih sadržaja upućene u mreže drugih operatora zaprimljene bez ograničenja. Zaključno, u pobijanom rješenju se navodi da je inspektor zaključio da je tužitelj postupio protivno čl. 43. st. 1. i 2. ZJN-a iz razloga što je implementirao mjere nadzora sadržaja SMS poruka bez valjanog opravdanja ili argumentacije iz koje bi proizlazilo da je isto nužno potrebno te da ničim nije opravdao da blokirane SMS poruke predstavljaju sigurnosni rizik ili bilo kakvu vrstu opasnosti za elektroničke komunikacijske mreže ili usluge. Nadalje, činjenica da konkretne poruke ne predstavljaju standardne verifikacijske poruke koje šalju partneri (koji su prethodno dostavili sadržaj svojih standardnih poruka), ne znači istodobno da prijenos ili zaprimanje takvih poruka može potencijalno ugroziti sigurnost mreža ili usluga, a da tužitelj u svojim očitovanjima tijekom inspekcijskog postupka nije obrazložio konkretni rizik ili opasnost za sigurnost mreža ili usluga, niti je obrazložio da bi blokiranje takvih poruka bilo nužno za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža ili usluga, ili za otkrivanje tehničkih kvarova i/ili pogrešaka, sigurnosnih rizika ili napada na elektroničke komunikacijske mreže i usluge već da se tužitelj opravdao zaštitom krajnjih korisnika od eventualnih zloporaba te se pozivao na obveze iz GDPR-a, NIS2 Direktive i ENISA-ine dokumente, a da nije pojasnio konkretne obveze zbog kojih je nadzor implementiran. Iz svega toga proizlazi, kako stoji u obrazloženju pobijanog rješenja, da postupanje tužitelja podrazumijeva nadzor SMS poruka koji se, između ostalih parametara, vrši

, pa

inspektor tuženika zaključuje kako implementirani sustav tužitelja vrši nadzor cjelokupnog SMS prometa, odnosno, provodi nadzor sadržaja SMS poruka, pri temu automatizirani nadzor bez ljudskog posredovanja, mjera kriptiranja ili ograničavanja uvida u zapise nije od utjecaja. Protivno navodima u pobijanom rješenju, tužitelj je detaljno elaborirao sve bitne okolnosti ovog konkretnog slučaja, odnosno, predmetnog postupanja koje se pobijanim rješenjem kvalificira nedopuštenima i protivnim čl. 43. ZEK-a. Naime, na usmenoj raspravi održanoj dana 27.04.2023.9. predstavnici tužitelja su detaljno pojasnili razloge uvođenja mjera zaštite mreže i usluga za svoje korisnike, a koje mjere odgovaraju najboljoj praksi u EU i svijetu. Nadalje, detaljno su opisali funkcioniranje zaštite (eng. Firewalla) kojeg primjenjuje tužitelj te su svoje navode dodatno pojasnili i u očitovanjima koja su prethodila usmenoj raspravi. Firewall (vatrozid) je vrsta sigurnosne zaištite čija je svrha sprječavanje zlonamjernih upada u

mreže i sustave. U tu svrhu tužitelj koristi firewall renomiranog partnera čija je svrha automatizirani nadzor SMS prometa, a postavke automatskog nadzora implementirane su unutar SMS firewalla te ne ugrožavaju i/ili zadiru u zajamčenu tajnost komunikacija. Tužitelj je tijekom postupka dostavio i izjavu spomenutog dobavljača, u kojoj je navedeno da je njihov osmišljen na način da zaštiti i operatora i korisnika od različitih vrsta prijevara uz jamstvo zaištite tajnosti podataka. Tužitelj je istaknuo kako njegov sustav (eng.)
Nadalje, tužitelj je u tom očitovanju istaknuo da se ne radi o mjerama nadzora i provjere sadržaja već o automatiziranim postavkama usporedbe

Kodirani meta podatak je zaštićeni (kriptirani) podatak koji opisuje drugi podatak. Pojašnjenja radi, u pitanju su poslovne transakcije koje se sastoje od slanja kodova, primjerice: u bankarskom ili kartičnom poslovanju, dvofaktorske autentifikacije pristup računima Google-a, Facebook-a, TikToka, i sl, dakle, na tržištu je prisutan niz legitimnih poslovnih transakcija u kojima određeni pošiljatelj poruke šalje različite verifikacijske kodove za pristup nekom od svojih servisa. Sustav tužitelja primjenjuje se u svrhu detekcije potencijalne zlouporabe, odnosno, zaštite sigurnosti i cjelovitosti komunikacijske mreže i njezinih korisnika, sprječavanja nedopuštenog usmjeravanja prometa i neželjene elektroničke komunikacije (eng. Spam). Nadalje, sustav tužitelja u tu svrhu

u svrhu
sprječavanja neželjene i potencijalno zlonamjerne komunikacije. Pritom je tužitelj prethodno od

(kao što
su banke, Facebook, Google, TikTok i sl.)
Sustav, kod usporedbe uzorka teksta, uzorak uspoređuje sa sadržajem dobivenim isključivo od autoriziranih, odnosno, akreditiranih pošiljatelja. Zaključno, tužitelj naglašava i za to priložio potvrdu proizvođača sustava kako nitko nema pristup sadržaju SMS poruka, pa ni administrator firewalla, a blokirani SMS-ovi se dalje ne pohranjuju i nije moguće otključavanje kodiranih meta podataka. Tužitelj je u svojim očitovanjima isticao da su SMS poruke inspektora u suštini simulirano postupanje koje firewall prepoznaje kao potencijalno prijevarno postupanje jer su poruke poslane od strane neautoriziranog pošiljatelja (privatnog mobilnog broja) na druge privatne mobilne brojeve krajnjih korisnika. Takvim slanjem poruka simulira se lažno predstavljanje pa je prema tome reakcija tužiteljevog sustava (blokiranje prometa) bila opravdana. SMS Firewall tužitelja takve SMS poruke automatski identificira kao smishing poruku (SMS phishing), čime sprječava lažno predstavljanje i eventualnu kradu identiteta ili neovlašteno korištenje osobnih podataka krajnjeg korisnika. Nadalje, tužitelj je tijekom postupka objasnio da autorizirani partnerski kanal predstavlja ugovorni odnos tužitelja s trećom stranom koja je njihov jedini partner kao agregator za sav A2P SMS međunarodni promet (što predstavljaju sporne poruke od Googl-a, Facebook-a, Samsung-a i sl.) te je samo promet koji dolazi od poslovnih pošiljatelja navedenog sadržaja po toj ruti autoriziran, dok se sav promet koji ima u sadržaju poruke poput predmetnih poruka koje je slao inspektor tuženika („Account is your Samsung account verification code", „use for two-factor authentification on Facebook'„ „G- is your Google verification code,) smatra

lažnim prijavljivanjem (fizička osoba šalje poruku u ime poslovnog subjekta) te se kao takvim smatra neautoriziranim te se blokira.

2.1. U nastavku tužbe detaljno opisuje i pojašnjava pojedine tehničke pojmove, smatra da temeljem čl. 43 st. 2. ZEK-a ima pravo putem navedenog automatiziranog sustava u SMS firewallu detektirati mogući sigurnosni rizik u SMS-komunikaciji i za svoju mrežu, i za krajnjeg korisnika, odnosno, potrošača, a koji sigurnosni rizik bi mogao u najgorem slučaju prouzročiti sigurnosni incident, što predstavlja najopasniju i najalarmantniju vrstu ugroze sigurnosti. Ako tužitelj ne bude u mogućnosti u budućnosti na opisani automatizirani način sprječavati SMS sigurnosne prijetnje, korisnici tužitelja će biti potpuno izloženih svim mogućim oblicima krade identiteta i osobnih podataka, koji će se slučajevi rješavati tek nakon što se navedene krađe dogode i nastane šteta za tužitelja i njegove korisnike, koju štetu procjenjuje na minimalno eura po korisniku.

2.2. Tužitelj je slijedeći najbolje EU prakse i preporuke ENISA-e, implementirao mjere zaštite svoje mreže i usluga, implementirane je mjere u skladu sa zahtjevima iz čl. 43., st. 1., 2. i 3. 7EK-a, kojima se propisuje obveza zaštite tajnosti podataka, ali i iznimka od te obveze. Budući da se sigurnosne prijetnje konstantno razvijaju, mora se razvijati i zaštita od istih. Stoga je i sam zakonodavac ostavio širok pojam u čl. 41. ZEK-a kojim obvezuje operatore da "moraju poduzeti odgovarajte tehničke i ustrojstvene mjere kako bi se zaštitila sigurnost njihovih mreža i usluga.". Dakle, zakonodavac ne specificira mjere koje operator treba poduzeti ali jasno navodi: "poduzete mjere moraju osigurati razinu sigurnosti koja odgovara postojećoj razini opasnosti za sigurnost mreže i usluga, voditi računa o raspoloživima tehničkim i tehnološkim rješenjima.", a konkretna (u ovom slučaju prilikom testiranja simulirana) sigurnosna prijetnja se nalazi na listi prijetnji prepoznati od strane ENISA-e.

2.3. Tužitelj ističe da je postupio u skladu s rješenjem tuženika, ali zbog toga trpi štetu, a ugroženi su i krajnji korisnici, jer ako tužitelj ne može na automatizirani način sprječavati SMS sigurnosne prijetnje, korisnici tužitelja su potpuno izloženi svim mogućim oblicima krade identiteta i osobnih podataka, a bez primjene automatiziranog načina sprječavanja SMS sigurnosne prijetnje, procjenjuje se da će stizati takvih poruka mjesečino, što posljedično predstavlja nemjerljivu štetu za mrežu, korisnike i ugled tužitelja.

2.4. Predlaže stoga saslušati predložene svjedoke i provesti vještačenje, a potom poništiti rješenje tuženika, utvrditi da tužitelj ne postupa protivno odredbi čl. 43. st. 1. i st. 2. ZEK-a na način da nadzire SMS promet između krajnjih korisnika i blokira određene vrste SMS poruka koje ne predstavljaju sigurnosni rizik ili napad na elektroničke komunikacijske mreže i usluge te koje mjere nisu nužne za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga, donijeti privremenu mjeru odgode izvršenja točke II. i III. izreke rješenja tuženika i naknaditi tužitelju trošak ovog spora.

3. U odgovoru na tužbu tuženik navodi da je pobijanim Rješenjem od strane inspektora elektroničkih komunikacija utvrđeno postupanje Tuženika protivno članku 43. stavku 1. i 2. ZEK-u, u odnosu na primjenu nadzora SMS prometa između krajnjih korisnika i blokiranja određenih vrsta SMS poruka koje ne predstavljaju sigurnosni rizik ili napad na elektroničke komunikacijske mreže i usluge te koje mjere nisu nužne za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga.

3.1. Tuženik uvodno ističe kako je člankom 43. stavak 1. ZEK-a propisana zabrana bilo kakvog slušanja, prisluškivanja, pohranjivanja te svaki oblik presretanja ili nadzora elektroničkih komunikacija i pripadajućih prometnih podataka, osim u slučajevima iz članka 52. ZEK-a te u slučajevima utvrđenima posebnim zakonima, sve to u svrhu osiguravanja tajnosti elektroničkih komunikacija i pripadajućih prometnih podataka u javnim komunikacijskim mrežama i javno dostupnim komunikacijskim uslugama. Dakle, tajnost elektroničkih komunikacija izravno je vezana odredba uz Ustavom zajamčeno pravo slobode i tajnosti dopisivanja (članak 36. Ustava Republike Hrvatske) koje predstavlja ključno načelo koje samo iznimno može biti ograničeno. Sukladno članku 52. ZEK-a, radi se o situacijama primjene mjera tajnog nadzora elektroničkih komunikacijskih mreža i usluga koje su propisane propisima kojima se uređuje sigurnosno-obavještajni sustav, te u slučajevima iz članka 43. stavka 2. ZEK-a na koji se upravo poziva Tužitelj. Imajući u vidu osjetljivost sadržaja komunikacije i priopćenja koje se razmjenjuju putem elektroničkih komunikacija, svaku vrstu nadzora i primjene sličnih mjera kontrole sadržaja komunikacije treba tumačiti izuzetno restriktivno. U tom smislu trebalo bi se raditi o zaista iznimnim slučajevima i situacijama koje mogu predstavljati stvarni rizik te slučajevima koji se nikako ne mogu i ne smiju opravdavati komercijalnim (naplatnim) ugovorima i interesima. U svojoj tužbi Tužitelj se poziva na obveze koje proizlaze iz članka 41. ZEK-a, a koje obvezuju sve operatore na primjenu „tehničkih i ustrojstvenih mjera kako bi se zaštitila sigurnost njihovih mreža i usluga". Navedena obveza nije sporna i ona podrazumijeva primjenu niza mjera (uključujući i kriptiranje podataka) koje su propisane Pravilnikom o načinu i rokovima provedbe mjera zaštite sigurnosti mreža i usluga (NN br. 52/23). Međutim, i takve mjere moraju se poduzimati u okviru zakonskih ograničenja propisanih drugim odredbama, a prije svega osnovnom načelu zabrane bilo kakvog presretanja i nadzora sadržaja komunikacije. Osporava tvrdnju tužitelja da Tuženik nije uzeo u obzir sve izvedene dokaze niti navode tužitelja. Prije svega, Tužitelj je vrlo načelno, ne ulazeći u detalje, u svojim očitovanjima tijekom postupka navodio da su mjere implementirane radi sprečavanja različitih vrsta zlouporaba, uključujući i zlouporaba putem SMS poruka. Međutim, u svojim očitovanjima nije ničim ukazao da bi konkretne SMS poruke predstavljale stvarno ugrožavanje odnosno rizik za sigurnost mreža ili usluga, već se isključivo pozivao na brigu o interesima krajnjih korisnika. Isto tako, Tužitelj je naveo kako se ne radi o nadzoru sadržaja komunikacije budući da se u konkretnom slučaju radi o metodi usporedbe uzorka teksta, koji je pri tome i kriptiran. Takvi navodi Tužitelja su potpuno neosnovani. Naime, sama činjenica da je određeni podatak ili metapodatak kriptiran ni na koji način ne utječe na zaključak da se radi o nadzoru sadržaja. Kriptiranje poruka ili bilo kojeg podatka je sigurnosna mjera pretvaranja podatka u šifrirani tekst, kojim se umanjuje rizik mogućnosti presretanja ili uvida u sadržaj od strane treće, neovlaštene osobe. Međutim, kriptiranje podataka ne utječe na činjenicu da sustav koji je pod nadzorom Tužitelja vrši kontrolu sadržaja (točnije uzorka teksta) koji se razmjenjuje između krajnjih korisnika, koja je odredbom članka 43. stavak 2. ZEK-a dopuštena samo u iznimnim slučajevima (kada je to nužno za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga, ili za otkrivanje tehničkih kvarova i/ili pogrešaka, sigurnosnih rizika ili napada na elektroničke komunikacijske mreže i usluge). Ni jednu od ovih okolnosti Tužitelj tijekom postupka, pa ni sada u okviru upravne tužbe, nije dokazao. Predmetne poruke ni na koji način ne ugrožavaju sigurnost mreža ili usluga, pa čak ni krajnjih korisnika. Tužitelj nije ukazao na bilo koji slučaj s kojim se u praksi susreo, a koji bi poslužio kao dokaz

da SMS poruke koje su predmet ovog postupka predstavljaju sigurnosni rizik za mrežu ili usluge operatora. Nadalje, sama činjenica da pošiljatelj šalje određeni kod za autentifikaciju putem SMS poruke ne može sama po sebi ugroziti sigurnost krajnjih korisnika. Budući da se ne radi o kodu koji pripada tom krajnjem korisniku, neovlašteni primatelj takvog koda odnosno poruke ne može učiniti nikakvu povredu. Drži da je ključni razlog za primjenu ove sporne mjere nadzora SMS poruka komercijalni interes Telemacha koji je implementirao mjere nadzora putem vatrozida koji omogućava propuštanje poruka određenih pošiljatelja (kao što su Facebook, Google, Tik-Tok i sl.) putem , a koje pošiljatelje Tužitelj naziva „akreditiranim partnerima". Ovakvo usmjeravanje i nadzor SMS prometa primjenjuje se neovisno o eventualnom ugrožavanju sigurnosti mreža ili usluga operatora. Naime, niti se Tužitelj u praksi susreo s navodnom zlouporabom koju primjenom mjera nadzora pokušava spriječiti niti se takve zlouporabe događaju u mrežama drugih operatora koji ne primjenjuju ove mjere. Naime, kako je i u samom Rješenju opisano, sporne SMS poruke bez bilo kakvih ograničenja su bile dostavljene i u mrežu i u mrežu Navedeni operatori imaju daleko veći broj korisnika od Tužitelja te bi stoga neprimjena spornih mjera u njihovim mrežama, prema procjenama sigurnosnih rizika Tužitelja, trebala uzrokovati enormne štete i za krajnje korisnike i za te operatore.

3.2. Tuženik smatra da je navod Tužitelja kako je Tuženik propustio rizik vezan uz tzv. „dvofaktorsku autentifikaciju" (2FA) kvalificirati kao sigurnosni rizik, potpuno promašen. Naime, konkretne poruke koje su primjenom komercijalnog interesa blokirane u mreži Tužitelja ne mogu predstavljati rizik kako ga opisuje Tužitelj. Unos koda koji zaprimi neovlašteni primatelj (a koji pripada nekoj drugoj osobi) ne može se zloupotrijebiti budući da ta osoba unosom tog koda u npr. svoj profil na društvenoj mreži ne može učiniti nikakvu zlouporabu. Stoga je primjena mjera nadzora sadržaja u svrhu navodne zaštite krajnjih korisnika od eventualnih zlouporaba samo promašeno opravdanje nezakonitog postupanja. Ostaje nejasno zašto algoritmi Tužitelja, primjenjujući istu logiku zaštite osobnih podataka korisnika i sprečavanja sigurnosnih rizika koje opisuje Tužitelj, ne primjenjuju prepoznavanje primjerice OIB-a ili broja bankovnog računa u SMS poruci, već isključivo kodova pošiljatelja koji usmjeravaju promet isključivo putem koja je ruta određena od strane Tužitelja. Prema tome Tužitelj u svojoj mreži propušta do primatelja samo poruke čiji sadržaj je prethodno dostavljen Tužitelju od strane poznatih pošiljatelja. Svaka poruka koja ne odgovara takvom predefiniranom sadržaju je blokirana, neovisno o njenom potencijalnom učinku na sigurnost mreža ili usluga te se radi o izravnom utjecaju na krajnje korisnike na način da se sadržaj poruka koje se razmjenjuju između njih nadzire kako bi se zadovoljio komercijalni dogovor između operatora i velikih „akreditiranih partnera", što je izričito zabranjeno člankom 43. stavak 1. ZEK-a.

3.3. Tuženik osporava navode Tužitelja kako je Tuženik propustio postupanje inspektora slanjem spornih poruka okarakterizirati kao sigurnosni rizik, i to konkretno sigurnosni rizik „man in the middle", temeljem čega bi prema mišljenju Tužitelja, ovakvo postupanje bilo zakonito. Prije svega, u konkretnom slučaju ne radi se o riziku koji se u praksi prepoznaje po spomenutom nazivu budući da se slanjem poruka nije prikrivao stvarni pošiljatelj, već se radilo samo o slanju sadržaja poruke koji je odgovarao predefiniranom sadržaju od strane „akreditiranih partnera". Na opisani način primatelj poruke nikako nije mogao zaključiti da je pošiljatelj poruke Facebook, Google ili drugi

sličan pošiljatelj, već upravo određeni konkretni broj. Rizik „man in the middle" u praksi predstavlja slučajeve presretanja komunikacije i lažnog prikazivanja stvarnog pošiljatelja kako bi se primatelja navelo na poduzimanje određenih aktivnosti (otvaranje poveznice u poruci, upisivanje osjetljivih podataka ili slično). Međutim, kako je i prethodno opisano, čak i kada bi se konkretne poruke mogle okarakterizirati kao pokušaj pogrešnog prikazivanja pošiljatelja, one i dalje ne zadovoljavaju uvjet iz članka 43. stavka 5. ZEK-a koji pretpostavlja nužne slučajeve za održavanje sigurnosti elektroničkih komunikacijskih mreža ili usluga, budući da navedene poruke ne predstavljaju takvu vrstu rizika.

3.4. U odnosu na prijedlog za donošenje privremene mjere Tuženik ističe da Tužitelj ničime nije učinio vjerojatnim nastanak bilo kakve štete. Kako je Tuženik i prethodno istaknuo, druga dva operatora nemaju implementirane identične mjere nadzora, pa unatoč navedenoj činjenici nikakva nenadoknadiva šteta ne nastaje, a posebice ugroza sigurnosti mreža ili usluga. Paušalni izračun štete koja prema navodima Tužitelja nastaje krajnjim korisnicima je teško i komentirati budući da ostaje nejasno kako je Tužitelj došao do izračuna od eura za koji iznos će svaki od potencijalno zahvaćenih korisnika biti oštećen. Sukladno svemu navedenom, Tuženik smatra da su tužba Tužitelja, kao i prijedlog za određivanje privremene mjere u cijelosti neosnovani, te predlaže Sudu da ih odbije kao neosnovane.

4. Tužbeni zahtjev nije osnovan.

5. Obzirom na to da u ovoj upravnoj stvari utvrđene činjenice nisu sporne, već je sporna primjena prava na utvrđene činjenice, ovaj Sud nije provodio predloženi dokazni postupak.

6. Naime, iz podataka u spisu predmeta te prema navodima stranaka, nije sporno da je u inspekcijskoj kontroli od strane tuženika utvrđeno da vatrozid (Firewall) u sustavu tužitelja ne propušta SMS-ove koji imaju u sadržaju poruke:"Account is your Samsung account verification code", ili "use for two-factor authentification on Facebook", ili ,"G- is your Google verification code", jer ih smatra lažnim prijavljivanjem (fizička osoba šalje poruku u ime poslovnog subjekta) te se kao takvim smatra neautoriziranim i blokira.

7. Tužitelj je stava da takvim vatrozidom štiti svoju mrežu i sve korisnike od lažnog predstavljanje, krađe identiteta i sl. te da mu to odredbe ZEK-a omogućuju, štoviše da mu obvezu zaštite mreže zakonske odredbe nalažu, dok tuženik smatra da vatrozid tužitelja omogućava nezakoniti nadzor poruka (koje, iako kriptirane nisu zaštićene u sadržaju) odnosno onemogućava SMS promet između krajnjih korisnika i blokira određene vrste SMS poruka, iako one ne predstavljaju sigurnosni rizik ili napad na elektroničke komunikacijske mreže i usluge pa takve mjere nisu nužne za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga.

8. Mjerodavna odredba ZEK-a, o kojoj ovisi pravilna primjena materijalnog prava u ovom slučaju, je odredba članka 43. ZEK-a, koja uređuje tajnost elektroničkih komunikacija u javnim komunikacijskim mrežama i javno dostupnim komunikacijskim uslugama te zabranjuje slušanje, prisluškivanje, pohranjivanje te svaki oblik presretanja ili nadzora elektroničkih komunikacija i pripadajućih prometnih podataka, osim u slučajevima iz članka 52. ovoga Zakona (tajni nadzor) te u slučajevima utvrđenima posebnim zakonima (stavak1.). Zabrana iz stavka 1. ovoga članka ne primjenjuje se na tehničku pohranu podataka koja je nužna za prijenos komunikacije, ni u slučajevima kada je to nužno za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga, ili za otkrivanje tehničkih kvarova i/ili

pogrešaka, sigurnosnih rizika ili napada na elektroničke komunikacijske mreže i usluge, ne zadirući pri tome u načela zaštite tajnosti podataka. Odredbe stavaka 1. i 2. ovoga članka ne odnose se na zakonski ovlašteno bilježenje komunikacija i pripadajućih prometnih podataka tijekom zakonitih poslovnih radnja u svrhu pružanja dokaza o trgovačkim transakcijama ili drugim poslovnim komunikacijama. Uporaba elektroničkih komunikacijskih mreža za pohranu podataka ili za pristup već pohranjenim podacima u terminalnoj opremi krajnjeg korisnika ili korisnika dopušteno je samo u slučaju kada je taj krajnji korisnik ili korisnik dao svoju privolu, nakon što je dobio jasnu i potpunu obavijest u skladu s propisima o zaštiti osobnih podataka, i to osobito o svrhama obrade podataka. Time se ne može spriječiti tehnička pohrana podataka ili pristup podacima isključivo u svrhu obavljanja prijenosa komunikacija putem elektroničke komunikacijske mreže, ili, ako je to nužno, radi pružanja usluga informacijskog društva na izričit zahtjev krajnjeg korisnika ili korisnika.

9. Prema citiranoj odredbi, kako to navodi i tuženik, uz tajnost elektroničkih komunikacija izravno je vezano Ustavom zajamčeno pravo slobode i tajnosti dopisivanja (članak 36. Ustava Republike Hrvatske) koje predstavlja ključno načelo koje samo iznimno može biti ograničeno, kada to nalažu propisi kojima se uređuje sigurnosno-obavještajni sustav te u slučajevima iz članka 43. stavka 2. ZEK-a, to jest kad je pohrana podataka nužna za prijenos komunikacije, u slučajevima kada je to nužno za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga, ili za otkrivanje tehničkih kvarova i/ili pogrešaka, sigurnosnih rizika ili napada na elektroničke komunikacijske mreže i usluge, ne zadirući pri tome u načela zaštite tajnosti podataka.

10. Tužitelj je stava da je upravo u skladu sa svojom obvezom osiguranja sigurnosti mreže, uporabom kvalitetnog programa zaštite onemogućio kolanje pojedinačnih SMS-ova, koje smatra sigurnosnom prijetnjom, a koja se nalazi na listi prijetnji prepoznati od strane ENISA-e, jer ti (blokirani SMS-ovi) nemaju sadržaj koji je implementiran kao uzorak teksta u SMS firewall. Ovo zato što, sustav tužitelja, kod usporedbe uzorka teksta, uzorak uspoređuje sa sadržajem dobivenim isključivo od autoriziranih, odnosno, akreditiranih pošiljatelja. Pritom je tajnost osigurana jer nitko nema pristup sadržaju SMS poruka pa ni administrator firewalla, a blokirani SMS-ovi se dalje ne pohranjuju i nije moguće otključavanje kodiranih meta podataka.

11. Nasuprot tome tuženik imajući u vidu osjetljivost sadržaja komunikacije i priopćenja koje se razmjenjuju putem elektroničkih komunikacija, drži da svaku vrstu nadzora i primjene mjera kontrole sadržaja komunikacije treba tumačiti izuzetno restriktivno, a u konkretnom slučaju nije utvrđena sigurnosna potreba za vatrozidom kakav je koristio tužitelj prilikom inspekcijskog nadzora.

12. Ovakav zaključak tuženika prihvaća i ovaj Sud, jer u podacima i dokumentaciji spisa nema niti jednog dokaza da bi SMS-ovi koji nemaju sadržaj kakav je implementiran kao uzorak teksta u SMS firewall tužitelja, uzrokovali sigurnosnu ugrozu za korisnike ili za mrežu, jer su bez ikakvih takvih posljedica slani i u mreže drugih operatora ( ).

13. Upravo ova činjenica u korelaciji s pojašnjenjem tužitelja da je uzorkovanje za potrebe detekcije SMS-ova neakreditiranih pošiljatelja posljedica autoriziranog partnerskog kanala, koji predstavlja ugovorni odnos tužitelja s trećom stranom, a koja je njihov jedini partner kao agregator za sav A2P SMS međunarodni promet, ukazuje na komercijalni karakter nadzora, što je u smislu odredbe članka 43. ZEK-a zabranjeno.

14. Stoga nije prihvatljivo pojašnjenje tužitelja da u svrhu zaštite mreže i korisnika od nemjerljive štete omogućuje samo promet koji dolazi od poslovnih pošiljatelja autoriziranog sadržaja, dok se sav promet koji ima u sadržaju poruke poput predmetnih poruka koje je slao inspektor tuženika blokiraju.
15. Slijedom navedenog Sud nalazi da nije osnovan tužbeni zahtjev tužitelja, a nema ni razloga za određivanje privremene mjere.
16. Obzirom da tužitelj u ovom sporu nije uspio, nema pravo ni na naknadu troškova spora, pa je sukladno članku 79. stavku 4. Zakona o upravnim sporovima ("Narodne novine", broj 20/10., 143/12., 152/14., 94/16., 29/17., 110/21., dalje: ZUS) i taj zahtjev odbijen.
17. Slijedom svega naprijed navedenog, a temeljem članka 57. stavka 1. ZUS-a, odlučeno je kao u izreci.

U Zagrebu, 3. listopada 2023.

Predsjednica vijeća:
Senka Orlić-Zaninović

Dokument je elektronički potpisan:
Senka Orlić-Zaninović

Vrijeme potpisivanja:
17-10-2023
08:12:14

DN:
C=HR
O=VISOKI UPRAVNI SUD REPUBLIKE HRVATSKE
2.5.4.97=#0C1156415448522D313336313333363030363638
OU=Signature
S=Orlić-Zaninović
G=Senka
CN=Senka Orlić-Zaninović