

Irēna Kucina

Privātuma un vārda brīvības apdraudējumi digitālajā komunikācijā un Eiropas Savienības jaunie priekšlikumi par lielo tiešsaistes platformu regulēšanu

Digitalizācija ir devusi sabiedrībai jaunas tehnoloģiskas iespējas uzlabot savu materiālo pasauli un indivīda dzīvi. Visi zina par digitālo tehnoloģiju lietojumu medicīnā, vides piesārņojumu samazināšanā, resursu taupīšanā un citās jomās. Arī par to, ka Saeima, valdība, iestādes, skolas, uzņēmumi šajā pandēmijas laikā turpina darboties attālināti, nodrošinot zināmu valsts, ekonomikas un sabiedrības funkcionēšanu laikā, kad cilvēku tiešā saskarsme ir ierobežota, ir jāpateicas digitālajām tehnoloģijām. Pirms 30 gadiem dzīve pandēmijas apstākļos būtu bijusi daudz grūtāka.

Digitālā revolūcija rit pilnā sparā. Mūsu saražoto datu apjoms katru gadu dubultojas. Ilustratīvi katru minūti mēs ražojam simtiem tūkstošu *Google* meklējumu un *Facebook* ziņu. Tajos ir informācija, kas atklāj, kā mēs domājam un jūtam. Drīz lietas, kas mums ir visapkārt, iespējams, pat mūsu apģērbs, arī būs savienotas ar internetu.

Var sagaidīt, ka kvantu superdatori drīz pārspēs cilvēku iespējas gandrīz visās jomās. Šķiet, ka šīs attīstības rezultātā vajadzētu veidoties viedām valstīm un viedai planētai.¹

Taču līdzšinējā tehnoloģiskā eiforija bieži nav ļāvusi saskatīt arī digitalizācijas radītos apdraudējumus demokrātijai, cilvēka brīvībai un tiesībām. Digitalizācija sola lielas iespējas, bet ir saistīta arī lieliem riskiem, it sevišķi demokrātijai un tiesiskas valsts principiem.

¹ Will Democracy Survive Big Data and Artificial Intelligence? Essays on the Dark and Light Sides of the Digital Revolution. Pieejams: https://www.researchgate.net/publication/327271384_Will_Democracy_Survive_Big_Data_and_Artificial_Intelligence_Essays_on_the_Dark_and_Light_Sides_of_the_Digital_Revolution

2020. gada 15. decembrī Eiropas Komisija nāca klajā ar diviem jauniem regulējumu priekšlikumiem (regulu formām) – Digitālo pakalpojumu tiesību akta² un Digitālo tirgu tiesību akta³ projektiem. To primārais mērķis ir uzlabot cilvēka darbības drošumu interneta vidē, it sevišķi kā preču un pakalpojumu patērētājam, taču pirmo reizi šie priekšlikumi satur arī punktus, kas ir svarīgi, lai mazinātu digitalizācijas apdraudējumu demokrātijai un tiesiskas valsts principiem.

Šeit autore vēlētos no tiesību viedokļa ieskicēt divus būtiskus riskus, kas saistīti ar digitalizāciju, – Lielo datu radīto apdraudējumu cilvēka pamattiesībām uz privātumu un vārda brīvības apdraudējumu sociālajos medijos, lai pēc tam apskatītu Eiropas Komisijas 2020. gada 15. decembrī publicētos savstarpēji saistītos Digitālo pakalpojumu akta un Digitālo tirgu akta projektus un īsumā izvērtētu to dotās (un nedotās) atbildes uz šiem riskiem. Beigās autore izvirza dažas tēzes, kāda varētu būt Latvijas attieksme šo projektu apspriešanas gaitā.

1. Lielie dati un privātuma apdraudējums

Lielie dati

Digitalizācija nozīmē arī Lielo datu (*Big Data*) izveidošanos.⁴ Lielie Dati ir divpakāpju procesa rezultāts. Vispirms dati tiek savākti, un tas notiek arvien intensīvāk. Tad – un tā ir otrā pakāpe – tie tiek sasaistīti, savesti kopā, tādā veidā daudzkārt multiplicējot informāciju, ko šie dati satur.⁵

Lielos datus angļu valodā raksturo trīs “V”: to lielais apjoms (*Volume*), to milzīgais uzkrāšanas un pārstrādes ātrums (*Velocity*) un to dažādība (*Variety*).⁶

Lielie dati pirmām kārtām nozīmē lielu datu apjomu (*Volume*). Piemēram, sociālo mediju telpā apjoms attiecas uz datu daudzumu, kas ģenerēts vietnēs, portālos un tiešsaistes lietojumprogrammās. Apjoms aptver pieejamos datus, kas tur atrodas un kuru atbilstība ir jānovērtē. *Facebook* ir 2 miljardi lietotāju, *YouTube* – 1 miljards lietotāju, *Instagram* – 700 miljoni lietotāju, *Twitter* – 350 miljoni lietotāju. Katru dienu šie lietotāji ģenerē miljardiem ziņu, attēlu,

² Pieejams: <https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020PC0825&from=LV>

³ Turpat.

⁴ Pääkkönen, P., Pakkala, D. (2015, December). Architecture and Classification of Technologies, Products and Services for Big Data Systems. *Big Data Research*, 2(4), 166–186. Pieejams: <https://www.sciencedirect.com/science/article/pii/S2214579615000027>

⁵ Turpat.

⁶ Turpat.

videoklipu, tvītu utt., kas ir ārkārtīgi liels datu apjoms. Tie visi tiek sasaistīti kopā Lielajos datos.⁷

Uzkrāšanas un pārstrādes ātrums (*Velocity*) ir datu ģenerēšanas ātrums. Paļiekot pie sociālo mediju piemēra, katru dienu *Google* tiek veikti 3,5 miljardi meklēšanas vaicājumi, *Facebook* tiek augšupielādēti 900 miljoni fotoattēlu, *Twitter* tiek ievietoti 500 miljoni tvītu. Lielie dati palīdz to lietotājam ātri saņemt ienākošo datu plūsmu un vienlaikus tos tikpat ātri apstrādāt.⁸

Dažādība (*Variety*) ir Lielo datu daudzveidība, kas attiecas uz datiem, kurus ir iespējams iegūt vai nu no cilvēkiem, vai mašīnām (datoriem, tehniskām ierīcēm u. c.). Visbiežāk tiek pievienoti strukturēti – teksti, tvīti, attēli, videoklipi u. c. Tomēr Lielajos datos iekļauti un apstrādāti tiek arī nestrukturēti dati, piemēram, e-pasta ziņojumi, balss pasta ziņojumi, ar roku rakstīti teksti, audio ieraksti utt. Lielie dati spēj klasificēt ienākošos datus dažādās kategorijās.⁹ Visa šī datu daudzveidība veido Lielo datu dažādības vektoru.

Trīs “V” apraksta analizējamus datus. Analītika ir process, kā no šiem datiem iegūt vērtību kādam lietotāja nolūkam.¹⁰

Datu avoti

Lielie dati būtiski ietekmē un turpmāk vēl vairāk ietekmēs sabiedrības un indivīda dzīvi. Jautājums ir – vai un ko mēs no tiem vēlamies?

Datu avoti var tikt iedalīti divās daļās – tehniskie avoti un cilvēki. Piemēram, ja ar modernajiem lieljaudas datoriem, drīzumā arī kvantu datoriem, tiek uztverti magnētiskie viļņi no tālām galaksijām, novērotas Covid-19 vīrusa mutācijas vai testētu materiālu stiprība – šādu tehnisko datu vākšana, uzkrāšana un izmantošana no sabiedrības un tiesību viedokļa nav tik sensitīva kā tad, ja datu avots ir cilvēki, kuru dati nav anonimizēti. Tāpēc problemātiku, kas saistīta ar datiem no tehniskiem avotiem, kā arī ar anonimizētiem datiem par cilvēkiem, autore turpmāk neanalizēs.

Ja turpretim tiek vākti, uzkrāti, izmantoti neanonimizēti dati par individualizētu, konkrētu cilvēku, par viņa izturēšanos, par viņa atrašanās vietu, par komunikāciju ar citiem cilvēkiem, par viņa ķermeni – tad jau tā ir pavisam cita

⁷ Understanding the 3 vs of Big Data – Volume, Velocity and Variety. (2017, September 8). Pieejams: <https://www.whishworks.com/blog/data-analytics/understanding-the-3-vs-of-big-data-volume-velocity-and-variety/>

⁸ Turpat.

⁹ Turpat.

¹⁰ Volume, velocity, and variety: Understanding the three V's of big data, 2018. Pieejams: <https://www.zdnet.com/article/volume-velocity-and-variety-understanding-the-three-vs-of-big-data/>

dimensija. Tas ir ne tikai zinātnes un tehnoloģijas, bet arī sabiedrības, demokrātijas, politikas un tiesību jautājums.

Tiesības uz privātumu

Demokrātiskā un tiesiskā valstī cilvēkam tiek garantēts privātums.

Šīs tiesības pirmo reizi postulēja ASV Augstākās tiesas tiesnesis Luiss Brandeiss savā rakstā *Right to Privacy* 1890. gadā *Harvard Law Review*.¹¹ Tur arī ir formulēta šo tiesību jēga un pamats – *the right to be left alone*. Tātad tiesības “palikt vienam”, t. i., lai citi ļauj būt man pašam.

Lai arī kopš šīs publikācijas ir pagājuši 130 gadi un privātuma tiesību izpratnes apjoms gan praksē, gan tiesību zinātnē tagad ir daudz plašāks un dziļāks, to saturs, mērķis un jēga nav mainījušies. Šīm tiesībām, kas ir cieši saistītas ar cilvēka cieņu un cilvēka subjektivitāti, ir jānodrošina iespēja būt pašam ar sevi, savā brīvā telpā, kurā viņš neatkarīgi no ārējās ietekmes var autonomi veidot savus uzskatus, savu identitāti, un lai viņš kā subjektīva persona tiktu respektēts un kā vienlīdzīgs sabiedrības loceklis darbotos publiskajā telpā, piedalītos publiskajā diskursā.¹²

Latvijā šīs tiesības ir garantētas Satversmes 96. pantā. Demokrātija, kuras dziļākā jēga ir cilvēka kā sabiedrības locekļa pašnoteikšanās publiskajā sfērā, nevar darboties, ja šīs tiesības netiek ievērotas. Ja tās tiek nepieļautami ierobežotas, tiek grauta demokrātiskas un tiesiskas valsts konstitūcija, valsts iekārta un sabiedrība.

Tiesību uz privātumu apdraudējums

Cilvēka digitālā novērošana jeb *tracking*, varētu teikt arī – izspiegošana, kas Lielajos datos uzkrāj neskaitāmi daudz pavisam dažādu datu, cilvēka profilēšana (*profiling*)¹³, kas dod iespēju ar algoritmu palīdzību paredzēt viņa rīcību atkarībā no konkrētā informatīvā konteksta (*prediction*), un šīs paredzētās rīcībās izmantošana, radot katram cilvēkam attiecīgu informatīvo kontekstu vai “burbuli”, lai

¹¹ Warren, S., Brandeis, L. The Right to Privacy. *Harvard Law Review*, 4, 193 (Dec. 15, 1890).

¹² Benn, S. Privacy, freedom, and respect for persons. In: In Ferdinand Schoeman (ed.). *Philosophical Dimensions of Privacy: An Anthology*. Cambridge University Press, 1984, p. 223.

¹³ Profilēšanas definīcija ir sniegta Vispārīgās datu aizsardzības regulas 4. panta 4. punktā: “profilēšana” ir jebkura veida automatizēta personas datu apstrāde, kas izpaužas kā personas datu izmantošana nolūkā izvērtēt konkrētus ar fizisku personu saistītus personiskus aspektus, jo īpaši analizēt vai prognozēt aspektus saistībā ar minētās fiziskās personas sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm, interesēm, uzticamību, uzvedību, atrašanās vietu vai pārvietošanos.

mērķtiecīgi panāktu noteiktu viņa rīcību – mikromērķēšana (*micro-targeting*) –, tas ir lielo, visiem zināmo globālo tiešsaistes platformu biznesa modelis.¹⁴

Tieši šis biznesa modelis rada privātuma apdraudējumu digitālajā vidē. Šodienas realitāte ir tāda, ka cilvēks, ieejot interneta vidē, tiek izsekots un profilēts. No tā izvairīties praktiski nav iespējams¹⁵, pretējā gadījumā cilvēks internetu var lietot tikai ar ļoti lieliem ierobežojumiem, tas savukārt praktiski nozīmē izslēgšanu no sociālās aprites. Taču šajā izsekošanā – kas ir pretrunā ar cilvēka tiesībām uz privātumu – no globālo tiešsaistes platformu un to uzņēmumu un citu struktūru viedokļa, kas ar šo platformu starpniecību to izmanto, ir ļoti skaidra jēga – cilvēks mērķēšana, vēl labāk – mikromērķēšana nolūkā panākt kādu noteiktu cilvēka rīcību.

Parasti šo manipulāciju cilvēks nejut un neuztver. Šis manipulācijas var būt mērķētas, lai panāktu noteiktu cilvēka ekonomisko uzvedību, bet sevišķi bīstami tas kļūst, ja mērķis ir ietekmēt cilvēka vai sabiedrības politisko nostāju un tai sekojošo politisko rīcību. Tas rada jautājumu par šāda biznesa modeļa savietojamību ar demokrātisko valsts iekārtu un tiesiskas valsts principiem.¹⁶ Tas ir liels izaicinājums datu aizsardzības sistēmām, kas faktiski nespēj šo problēmu efektīvi risināt.¹⁷

2. Vārda brīvības apdraudējums sociālajos medijos

Globālā digitālā vide ir radījusi jaunas iespējas vietējām, nacionālām, reģionālām un globālām aktivitātēm, ieskaitot jauna veida politisko aktīvismu, kultūras apmaiņu un cilvēktiesību īstenošanu. Globālie interneta koncerni ir radījuši

¹⁴ Zubov, S. (2019). *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*. New York, Public Affairs.

¹⁵ Reaģējot uz ES Vispārīgās datu aizsardzības regulas prasībām un Eiropas Savienības tiesas spriedumu (2019. gada 1. oktobra spriedums lietā Nr. C-673/17, Planet 49), vietnes, kuras cilvēks internetā apmeklē, tagad "lūdz" viņa piekrišanu izvietot viņa datorā sīkdatnes, kas izseko viņa rīcībai. Piekrišanas definīcija ir sniegta Vispārīgās Datu aizsardzības regulas 4. panta 11. punktā: "Datu subjekta "piekrišana" ir jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstipriņošanas darbības veidā sniedz piekrišanu savu personas datu apstrādei."

No civiltiesību viedokļa tomēr var tikt diskutēts jautājums, vai piekrišana bez reālas izvēles alternatīvas vispār var tikt uzskatīta par tiesiski vēra ņemamu, vismaz tad, ja ir runa par tādām vietnēm, kuras cilvēks *de facto* ir spiests izmantot (piemēram, valsts iestādes vai privāti monopoluzņēmumi). Jebkurā gadījumā šeit būtu jāprasa lietotāja kvalificēta piekrišana ("meaningfull consent"), ar parasto klikšķi uz "es piekrītu" pogu nepietiek. Collection, Targeting and Profiling of Consumers Online. BEUC Discussion paper, 2020. Pieejams: <https://www.beuc.eu/publications/2010-00101-01-e.pdf>

¹⁶ Sal: Bennett, C. J., Smith, O.-M. (2019). *Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities*. Pieejams: https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf

¹⁷ Witzleb, N., Paterson, M. *Micro-targeting in Political Campaigns: Political Promise and Democratic Risk*. Pieejams: https://www.researchgate.net/publication/344839124_Micro-targeting_in_Political_Campaigns_Political_Promise_and_Democratic_Risk

cilvēkiem savstarpējās komunikācijas vidi, un gan liela daļa cilvēku, gan valsts iestādes un uzņēmumi savu komunikāciju ir pārvietojuši šajā interneta vidē. Tam, ka globālie koncerni šo globālo komunikācijas vidi pārvalda pamatā saskaņā ar savu īpašnieku noteiktajiem iekšējiem noteikumiem, līdz šim ir pievērsta nepietiekama uzmanība.

Šī digitālā vide ir radījusi iespējas prettiesiskai tās lietošanai: naida runas vai bērnu pornogrāfijas izplatīšanai, kūdīšanai uz vardarbību utt. Reālajā vidē šādas darbības ir aizliegtas, un valsts iestādes par tām var sodīt ar administratīvo vai kriminālsodu, taču digitālajā vidē pieļautās vārda un informācijas aprites brīvības un privātuma robežas paliek neskaidras, izplūdušas un pakļautas dažādām interpretācijām.

Demokrātiska un tiesiska valsts garantē informācijas un vārda brīvību. Latvijā to garantē Satversmes 100. pants. Tā ir viena no galvenajām pilsoņa tiesībām, to ievērošana ir priekšnoteikums, lai demokrātiskā valsts iekārta varētu funkcionēt. Taču šī brīvība, tāpat kā lielākā daļa cilvēktiesību, nav neierobežota. Tai ir robežas, kuras nosaka Satversmes 116. pants. To var ierobežot ar samērīgu likumu, lai nodrošinātu citu personu tiesības un novērstu nepārprotamus un tiešus draudus sabiedrībai.¹⁸

Sabiedrības interesēs ir nepieļaut naida runu, tomēr tikpat nozīmīgi ir, lai digitālajā vidē netiktu ierobežotas tiesības uz vārda brīvību. Šāds ierobežojums pieļaujams tikai ekstrēmā gadījumā. Kā atzinusi Eiropas Cilvēktiesību tiesa vienā no saviem pamatspriedumiem, vārda brīvība ietver arī tādas informācijas un viedokļus, “kas apvaino, uztrauc vai šokē valsti vai kādu sabiedrības daļu”.¹⁹ Tātad jebkurš vārda brīvības ierobežojums, kas nenodara kaitējumu citu personu tiesībām, ir pilsoņa tiesību uz vārda brīvību pārkāpums.

Lielās tiešsaistes platformas, globālie interneta koncerni ir privāti uzņēmumi, to galvenās mītnes atrodas ASV, un tie ir pakļauti ASV likumiem. Tie spēj kontrolēt un dzēst lietotāja augšuplādētu saturu, pamatojoties uz šo tiešsaistes platformu interpretāciju par to, vai saturs ir, piemēram, medicīniska dezinformācija, naida runa vai vardarbības veicināšana.

Taču šajās vietnēs izvietotais, lietotāju ģenerētais saturs vienlaikus ir arī Latvijas sabiedrības diskursa telpas, tātad demokrātiskā politiskā procesa, sastāvdaļa.²⁰ Tās robežu noteikšana – nelikumīga satura definēšana – ir pilsoņu demokrātiski leģitīmētā likumdevēja uzdevums. Katrā valstī tas var būt atšķirīgs. Latvijā,

¹⁸ Satversmes tiesas spriedums lietā Nr. 2003-05-09, 22. punkts.

¹⁹ Eiropas Cilvēktiesību tiesas spriedums lietā *Handyside v. United Kingdom*, C-5493/72, 49. punkts.

²⁰ Sal.: Levits, E. (2016, 1. marts). Nacionālā informācijas un demokrātiskā diskursa telpa kā demokrātiskas valsts iekārtas elements. *Jurista Vārds*, Nr. 9.

ņemot vērā vēsturisko pieredzi padomju okupācijas laikā, vārda brīvībai sabiedrības izpratnē ir īpaši svarīga nozīme.

Globālie interneta koncerni ir izveidojuši digitālo komunikācijas vidi, kas ir kļuvusi par cilvēku galveno saziņas vietu, bez tās cilvēks faktiski vairs nevar pilnvērtīgi piedalīties sabiedrības dzīvē, tādējādi šie koncerni ievērojamā mērā “pārvalda” mūsu sociālo dzīvi.²¹ Demokrātiskas valsts tiesības ietekmēt savu iedzīvotāju vārda brīvību ir skaidri noteiktas konstitūcijā, pieļaujot to tikai ekstrēmās gadījumos, un šī ietekme ir pakļauta neatkarīgas tiesas kontrolei.²² Turpretim globālo interneta koncernu, šo privāto uzņēmumu, iespējas ietekmēt vārda brīvību ir daudz lielākas, jo tie darbojas tiesiski neregulētā vidē vai “pelēkajā zonā”. Taču to atklātā un vēl jo vairāk slēptā ietekme uz cilvēku, uz demokrātiskas sabiedrības publisko diskursu un privāto komunikāciju ir ievērojama. Globālie interneta koncerni ir koncentrējuši lielu varas potenciālu – un šis varas potenciāls atrodas ārpus demokrātiskās ietekmes un kontroles.

Tāpēc pats fakts, ka globāls interneta koncerns, dzēšot, nepieļaujot vai citādi regulējot vārda brīvību tam privāttiesiski piederošās vietnēs, kuras – apzināti ar mērķi radīt peļņu – ir izveidotas par galveno demokrātiskas sabiedrības diskursa vietu, ir problemātisks.²³ Tas ir sabiedrības pamatvērtību un demokrātiskas un tiesiskas valsts iekārtas apdraudējums.

Valsts prezidents Egils Levits ir uzsvēris, ka sociālo tīklu algoritmi vai kādi mums nezināmi anonīmi cilvēki nav tiesīgi pieņemt lēmumus, kas ierobežo Satversmē garantēto vārda brīvību Latvijā. Demokrātiskā un tiesiskā valstī vārda brīvības robežas likumos nosaka demokrātiski pilnvarotais likumdevējs, un to, vai šīs robežas ir pārkāptas, var lemt tikai tiesa.²⁴

Tas ir iemesls, kādēļ Eiropā diskusijas par interneta vides un it sevišķi globālo interneta koncernu – tāpat lielo tiešsaistes platformu – darbības regulēšanas

²¹ Suzor, N. P. (2019). *Lawless: the secret rules that govern our digital lives and why we need new digital constitutions that protect our rights*. Cambridge University Press. Pieejams: file:///C:/Users/konto-2/Downloads/Suzor%202019%20Lawless-2018-11-19T13_55_25.098Z.pdf

²² Skat.: Šņepste, I. (2021, 5. janvāris). Vārda brīvības iepriekšēji ierobežojumi internetā: jēdziens un pieļaujamība. *Jurista Vārds*, Nr. 1.

²³ Sal.: Stjernfelt, F., Lauritzen, A. M. (2020). *Your Post has been Removed*. Springer Open, p. 83. Pieejams: <https://link.springer.com/content/pdf/10.1007%2F978-3-030-25968-6.pdf>

²⁴ Valsts prezidents: Vārda un mākslas brīvība nedrīkst tikt sašaurināta. Pieejams: <https://www.president.lv/lv/jaunumi/zinas/valsts-prezidents-varda-un-makslas-briviba-nedrikst-tikt-sasaurinata-26622#gsc.tab=0>

nepieciešamību²⁵ pārtop rīcībā. Ir skaidrs, ka klasiskā datu aizsardzība, arī datu aizsardzības sistēmas līdz šim augstākais sasniegums – Vispārīgā datu aizsardzības regula, ir absolūti nepietiekama, lai aizsargātu cilvēka privātumu, vārda brīvību un – līdz ar to arī demokrātiju.

3. Digitālo pakalpojumu akta un Digitālo tirgu akta projekti

2020. gada 15. decembrī Eiropas Komisija nāca klajā ar diviem jaunu regulu priekšlikumiem – Digitālo pakalpojumu tiesību aktu un Digitālo tirgu tiesību aktu.

Digitālo pakalpojumu akta projekts noteic virkni pamatnoteikumu un principu attiecībā uz to, kā tiešsaistes platformas piedalās satura publicēšanā un izplatīšanā. Digitālo pakalpojumu akta priekšlikumi satur noteikumus, kas ne tikai paredz šo platformu nosacīto atbildību par lietotāju izvietoto saturu šajās platformās, bet arī nosaka to “satura moderēšanas” (šis labāk skanīgais jēdziens tiek lietots “cenzēšanas” vietā²⁶) politikas pamatnoteikumus un to izpildi.²⁷ Priekšlikumi cita starpā paredz:

- pasākumus pret lietotāju izvietoto “nelikumīgu saturu”, tostarp mehānismu, kas ļauj citiem lietotājiem tādu saturu iezīmēt un platformām sadarboties ar īpašiem “uzticamiem signalizētājiem”;
- lietotāju aizsardzības pasākumus, tostarp iespēju apstrīdēt platformu lēmumus ierobežot to saturu;
- pienākumu tiešsaistes platformām nodrošināt to algoritmu daļēju caurskatāmību.

Būtisks jauninājums ir tas, ka īpaši tiek definēti un stingrāk nekā citi interneta uzņēmumi regulēti tieši visiem zināmie lielie globālie interneta koncerni, kuri ir galvenie cilvēku izsekošanas, profilēšanas, rīcības paredzēšanas un

²⁵ Dobber, T., Ó Fathaigh, R., Zuiderveen Borgesius, F. J. (2019, 31. decembris). The regulation of online political micro-targeting in Europe. Internet Policy Review. Vol. 8, Issue 4. Pieejams: <https://policyreview.info/articles/analysis/regulation-online-political-micro-targeting-europe>

Priekšlikums Eiropas Parlamenta un Padomes Regulai par digitālo pakalpojumu vienoto tirgu (Digitālo pakalpojumu tiesību akts), ar ko groza Direktīvu 2000/31/EK, 15.12.2020. Pieejams: <https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020PC0825&from=en>

Priekšlikums Eiropas Parlamenta un Padomes Regulai par sāncensīgiem un godīgiem tirgiem digitālajā nozarē (Digitālo tirgu tiesību akts), 15.12.2020. Pieejams: <https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52020PC0842&from=en>

Dobber, T., Ó Fathaigh, R., Zuiderveen Borgesius, F. J. (2019, 31. decembris). The regulation of online political micro-targeting in Europe. Internet Policy Review. Vol. 8, Issue 4. Pieejams: <https://policyreview.info/articles/analysis/regulation-online-political-micro-targeting-europe>

²⁶ Skat. arī: Stjernefelt, F., Lauritzen, A. M. (2020). Facebook and Google as Offices of Censorship. Pieejams: file:///C:/Users/konto-2/Downloads/Facebook_and_Google_as_Offices_of_Censorship.pdf

²⁷ Barata, J. (2021, 2. marts). The Digital Services Act and the Reproduction of Old Confusions. Pieejams: <https://verfassungsblog.de/dsa-confusions/>

ietekmēšanas mehānisma darbinātāji. Tie tiek apzīmēti par “ļoti lielām tiešsaistes platformām” un definēti kā “tiešsaistes platformas, kuru pakalpojumi sasniedz vismaz 10% no Eiropas Savienības iedzīvotāju skaita” (25. pants).

Digitālo tirgu akts cita starpā paredz definēt kritēriju kopumu, pēc kuriem liela tiešsaistes platforma kvalificējama par piekļuves kontrolieri. Tie ir:

- spēcīga ekonomiskā pozīcija, būtiska ietekme iekšējā tirgū, un tas darbojas vairākās ES valstīs;
- spēcīga starpniecības pozīcija, kas nozīmē, ka tas saista lielu lietotāju skaitu;
- ir (vai drīzumā būs) nostiprināta un ilgtspējīga pozīcija tirgū, kas nozīmē, ka tas laika gaitā ir stabils.

Šādam par “piekļuves kontrolieri” definētam uzņēmumam – faktiski runa ir galvenokārt par globālajiem interneta koncerniem – ir jāpilda noteikti pienākumi, lai nodrošinātu taisnīgāku komercvidi, it sevišķi maziem un vidējiem uzņēmumiem, jaunuzņēmumiem. Piemēram, interneta meklētājplatforma (piemēram, *Google*) vairs nedrīkstēs savus vai tai piederošu uzņēmumu vai sadarbības partneru produktus meklēšanas rezultātu sarakstā “izbīdīt” priekšgalā.

4. Projektu problemātiskie punkti

Par šiem jaunajiem Eiropas Komisijas regulējumu priekšlikumiem Eiropā jau ir sākusies diskusija (Latviju pagaidām tā vēl nav sasniegusi), un netrūkst arī kritikas. Sistēmiski būtiskākie kritikas punkti ir divi.

Pirmkārt, Digitālo pakalpojumu akts lielu vērību pievērš “nelikumīga saturs” izskaušanai, uzliekot interneta uzņēmumiem pienākumu to vispirms darīt pašiem. Tas nozīmē, ka viņiem ir jāatrod lietotāju tur izvietotais “nelikumīgs saturs”. Uzņēmums to var darīt ar citu lietotāju ziņojumu, īpašu “uzticamu signalizētāju” palīdzību, kā arī pēc savas iniciatīvas. Tas automātiski rada jautājumus – vai šiem uzņēmumiem tagad ir deleģētas tiesības cenzēt tur izvietoto saturu? Kā tas ir savietojams ar vārda brīvības nodrošināšanu, kuras robežas demokrātiskā un tiesiskā valstī nosaka demokrātiski leģitīms likumdevējs? Jāņem vērā, ka praktiski jebkura par nelikumīgu uzskatīta saturs dzēšana var radīt domstarpības par to, vai tas patiešām ir bijis nelikumīgs. Vai tiešām šos jautājumus no tiesību viedokļa drīkst izšķirt ar algoritmu palīdzību?²⁸ Kā praksē varētu darboties apstrīdēšanas mehānisms, ņemot vērā šādu strīdu iespējamo lielo skaitu? Vai patlaban

²⁸ Par algoritmu lietošanas robežām lēmumu pieņemšanā tiesiskā procedūrā sal.: Kucina, I. (2021). Algorithms in Courts and Predictive Justice. In: Julia Iliopoulos-Strangas, Egils Levits, Michael Potacs, Jacques Ziller (Hrsg.): Die Herausforderungen der digitalen Kommunikation für den Staat und seine demokratische Staatsform. The Challenges of Digital Communication for the State and its Democratic State Form. Nomos, Baden-Baden; Stämpfli, Bern; Sakkoulas, Athens.

acīmredzot lietotais “aizliegto vārdu” saraksts, kas publiski nav pieejams un kuru lieto šo lielo platformu algoritmi, ir pieļaujams no tiesiskas valsts viedokļa, ņemot vērā, ka tas var radīt brīvai, demokrātiskai sabiedrībai nepieņemamu pašcenzūras efektu?²⁹

Otrkārt, Eiropas Komisijai ir pietrūcis drosmes (visticamāk, ir darbojušies attiecīgie lobiji) nopietni ierobežot vai, vēl labāk, aizliegt izsekošanu, profilēšanu un mikromērķēšanu.³⁰ Kā jau iepriekš minēts, tieši izsekošana un profilēšana mikromērķēšanas nolūkos kā visas cilvēka digitālās izsekošanas infrastruktūras galvenais mērķis ir tas, kas ietekmē cilvēka privātumu un padara viņu mērķtiecīgi manipulējamu. Ja tas notiek tiešās vai netiešās politiskās interesēs, tad ar to tiek skarts pats demokrātijas kodols.

Tomēr pozitīvi ir tas, ka Digitālo tirgu akta 29. pants pirmo reizi, gan visai uzmanīgi, ir pievērsis uzmanību šai izsekošanas, profilēšanas un mikromērķēšanas infrastruktūrai. Pants nosaka, ka lielajām tiešsaistes platformām savos noteikumos jānosaka savās ieteikumu sistēmās izmantotie parametri, kā arī pakalpojuma saņēmēju iespējas ietekmēt šādus galvenos parametrus, kurus tās ir darījušas pieejamus, to starpā vismaz vienu iespēju, kas nav balstīta uz profilēšanu. Tas nodrošinātu lietotājam zināmu transparenci un iespēju ietekmēt to, kā lielās tiešsaistes platformas ietekmē viņu. Un tas jau ir progress ceļā uz šīs problēmas patiesu risināšanu.

Problemātisks ir arī Digitālo pakalpojumu akta tvērums. Saskaņā ar 5. un 14. pantu tas ietver jebkāda veida platformu pakalpojumus – ne tikai sociālos medijus, bet arī e-pastus, mākoņpakalpojumus u. c. Vai tas nozīmēs, ka cenzūra tiks attiecināta arī uz privātajiem e-pastiem un informāciju, ko lietotājs glabā mākonī?³¹

Tāpat neviens no abiem jaunajiem projektiem nepiemin lielo tiešsaistes platformu atbildību par lietotāju uzglabāto datu noplūdi. 2021. gada aprīļa sākumā 533 miljonu *Facebook* lietotāju dati (personīga informācija, telefona numuri) tika izplatīti internetā.³² Kāda ir *Facebook* atbildība? Vai tam jāpaziņo šis fakts attiecīgajiem lietotājiem? Vai lietotāji var no *Facebook* prasīt morālu vai materiālu kompensāciju?

²⁹ Sal.: Benesch, S. (2020). But Facebook's Not a Country. How to Interpret Human Rights Law for Social Media Companies. *Yale Journal on Regulation Online Bulletin*. Pieejams: <https://digitalcommons.law.yale.edu/jregonline/3/>

³⁰ At a Glance: Does the EU Digital Services Act protect freedom of expression? Pieejams: <https://www.article19.org/resources/does-the-digital-services-act-protect-freedom-of-expression/>

³¹ Turpat.

³² 533 million Facebook users' phone numbers and personal data have been leaked online. (2021, 3. aprīlis). *Business Insider*. Pieejams: <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4>

Digitālo pakalpojumu akta un Digitālo tirgu akta projektos, bez šaubām, ir daudz interesantu un novatorisku noteikumu. Daudzos gadījumos tie ir lietotāju tiesību nostiprināšana attiecībā uz tiešsaistes uzņēmumiem. Taču apzinoties, cik svarīgi šajos abos projektos ietvertie regulējumi būs Eiropas digitālās vides veidošanai un līdz ar to cilvēku tiesībām un iespējām izmantot šo vidi, jāreķinās, ka šie projekti tagad tiks uzmanīgi un ilgstoši apspriesti dažādos šo aktu galīgās redakcijas posmos. Šeit sadursies globālo interneta koncernu un citu tiešsaistes uzņēmumu intereses, no vienas puses, un pilsoņu intereses, no otras puses. Un pilsoņu interesēs ir aizstāvēt savu privātumu un vārda brīvību tādās robežās, kā to nosaka valsts likumi, nevis šo uzņēmumu intereses un priekšstati par to, ko drīkst un ko nedrīkst.

5. Kas svarīgi Latvijai?

Latvija, tāpat kā citas Eiropas Savienības valstis, gatavojas vērienīgai digitalizācijai. Eiropas Savienība savu dalībvalstu ekonomikas, darba pasaules, komunikācijas un citu jomu pārejā uz digitālo tehnoloģiju ieguldīs lielus līdzekļus.

Kas šajā kontekstā ir svarīgi Latvijai?

Pirmkārt, jāatceras, ka digitalizācijai ir ne vien tehniska, bet arī sociāla un ar to saistīta tiesiska dimensija. Tiesību uzdevums digitalizācijā ir veicināt sabiedrībā pozitīvos efektus un aizsargāt tos no negatīvajiem.

Otrkārt, ieguldot resursus digitalizācijā, jāņem vērā, ka ir sākusies un turpmāk arvien pastiprināsies tendence tiesiski regulēt digitālo vidi tā, lai tā nesaētu indivīda privātumu un līdz ar to viņa patstāvīgo, uz autonomas izvēles balstīto spriestspēju. Līdzšinējie biznesa modeļi, kas balstīti uz cilvēku izsekošanu un viņu rīcības ietekmēšanu ar mikromērķēšanas palīdzību, kurus jau tagad abi šeit apskatītie projekti mēģinājuši pagaidām vēl ļoti saudzīgi ierobežot, pārredzamā nākotnē ar lielu varbūtību nebūs ilgtspējīgi.

Treškārt, Latvijai ir iespēja nevis vienkārši gaidīt, kā viss attīstīsies, kas notiks, bet gan aktīvi piedalīties šajā diskusijā, tostarp pavisam konkrēti – formulēt un aktīvi pārstāvēt savu pozīciju par minētajiem Eiropas Komisijas projektiem. Autores ieskatā Latvijas pozīcijai jābūt tādai, kas aizstāv cilvēku, viņa pamattiesības un brīvību. Savukārt interneta uzņēmumiem jāatrod un Eiropas Savienības regulējumiem mērķtiecīgi jāatbalsta tādi biznesa modeļi, kas to respektē.

Ceturtkārt, Latvijai ir iespēja arī inovatīvi atrast savus nacionālos tiesiskos risinājumus, kas precīzāk nošķir digitalizācijas pozitīvos efektus no negatīvajiem. Tiesiskā vide, juridiskā infrastruktūra ekonomikai ir tikpat svarīga kā kapitāls, darbaspēks un citi ekonomiskie faktori. Latvija var mērķtiecīgi veidot šādu

ilgtspējīgu tiesisku vidi un tādā veidā veicināt digitalizācijas procesu un tā pozitīvos efektus, kas būtu arī papildu stimuls ekonomikai.

Piektkārt, juridiskie mehānismi, kas mums pastāv pilsonisko un politisko tiesību aizsardzībai, globālo interneta koncernu gadījumā nedod labu rezultātu. Eiropai – un Latvijai – ir iespēja attīstīt inovatīvu tiesisku pieeju attiecībā uz šo platformu atbildību un to darbības regulēšanu cilvēku interesēs, nevis vienkārši ļaut tām patverties savā problemātiskajā biznesa modelī un visu tiesisko regulējumu veidot ap to.

Šī arī ir iespēja noteikt konstitucionālos principus, kuriem kopīgi vajadzētu būt par Eiropas kopīgās sociālās telpas pamatu digitālajā laikmetā. Diskusija par “digitālo konstitucionalismu” (*digital constitutionalism*)³³ pēdējā laikā kļūst arvien nozīmīgāka. Tiesiskuma vērtības, labas pārvaldības vērtības ir pamats, kā konstitucionāli konceptualizēt interneta uzņēmumu regulējumu un pārvaldību, pakļaut to darbību un ar to saistītos riskus demokrātiski leģitīmam regulējumam.

³³ De Gregorio, G. (2020). The Rise of Digital Constitutionalism in the European Union. *International Journal of Constitutional Law*. Pieejams: <https://ssrn.com/abstract=3506692>; Celeste, E. (2018). Digital Constitutionalism: Mapping the Constitutional Response to Digital Technology's Challenges. HIIG Discussion Paper Series No. 2018-02. Pieejams: <https://ssrn.com/abstract=3219905> or <http://dx.doi.org/10.2139/ssrn.3219905>