https://doi.org/10.22364/juzk.78.10

# NEBEIDZAMĀ CĪŅA PRET MASVEIDA UZRAUDZĪBU: EST LĪDZSVARA MEKLĒJUMI STARP PRIVĀTUMU UN DROŠĪBU

# THE NEVER-ENDING BATTLE AGAINST MASS SURVEILLANCE: THE CJEU IN SEARCH FOR THE RIGHT BALANCE BETWEEN PRIVACY AND SECURITY

**Irēna Ņesterova, *Dr. iur*.**
Latvijas Universitātes Juridiskās fakultātes
Juridiskās zinātnes institūta pētniece

**Summary**

States all around the world are rapidly deploying new surveillance technologies, raising serious challenges to fundamental rights and the values of democratic society. The findings of the Court of Justice of the European Union (the CJEU) are an important source for the development of criteria for lawful surveillance practices. On December 2019, Advocate General of the CJEU issued his Opinion in *Schrems II* case challenging data transfer mechanisms between the EU and the US considering the latest national security rules. On January 2020, three more opinions were issued in the cases concerning data retention laws. The article aims to evaluate these recent Advocate General's opinions in the light of exposing mass surveillance measures emphasising the paramount importance of compliance with the fundamental rights, the rule of law and democratic principles.

**Atslēgvārdi:** datu saglabāšana, drošība, masveida uzraudzība, privātums, Šrems II

**Keywords:** security, data retention, mass surveillance, privacy, Schrems II

## Ievads[1]

Visā pasaulē valstis arvien vairāk piemēro dažādus masveida uzraudzības pasākumus, radot pamatotas bažas par to ietekmi uz pamattiesībām, kā arī demokrātiskām vērtībām un tiesiskumu. Plašas diskusijas ir radījušas mākslīgā intelekta tehnoloģijas, jo īpaši sejas atpazīšanas tehnoloģijas, kas tiek ieviestas un arvien vairāk izmantotas ASV, Ķīnā, Singapūrā, Krievijā, Japānā, kā

[1] Darbs izstrādāts ERAF specifiskā atbalsta mērķa 1.1.1.2. pasākuma "Pēcdoktorantūras pētniecības atbalsts" projekta 1.1.1.2./VIAA1/1/16/001 pētniecības pieteikuma Nr. 1.1.1.2./VIAA/1/16/196 "Taisnīgs līdzsvars starp privātumu un drošību kibertelpā: stingru datu aizsardzības standartu izveide Eiropā" ietvaros.

arī daudzviet Eiropā, piemēram, Francijā, Vācijā, Apvienotajā Karalistē.[2] Gan Eiropas Savienībā (turpmāk – ES), gan citviet pasaulē tiek meklēti risinājumi, kā regulēt šīs jaunās tehnoloģijas, lai tās atbilstu pamattiesībām un tiesiskas valsts prasībām.[3] Lai cīnītos ar Covid-19 globālās pandēmijas radīto apdraudējumu, valstis visā pasaulē, kā arī ES, tostarp Latvijā un Igaunijā, strauji ievieš jaunus masveida uzraudzības pasākumus, izmantojot tehnoloģiju radītās iespējas, piemēram, kontaktu izsekošanas lietotnes. Tajā pašā laikā pastāv bažas, ka valsts iestādes, kā arī privātie uzņēmumi nevēlēsies atteikties no šādu pamattiesības būtiski ierobežojošu pasākumu piemērošanas arī pēc ārkārtas situācijas beigām.

Jautājums, kādos gadījumos masveida uzraudzības pasākumi ir pieļaujami un kādos ne, kādas prasības ir jāievēro, tos piemērojot, un kā panākt līdzsvaru starp privātuma aizsardzību un drošības interesēm, jau ilgstoši nodarbina arī Eiropas Savienības Tiesas (turpmāk – EST) tiesnešu prātus, un tā turpina saņemt arvien jaunus lūgumus sniegt skaidrojumus par ES tiesību piemērošanu lietās, kas saistītas ar masveida uzraudzības pasākumu piemērošanu. 2019. gada 19. decembrī ģenerāladvokāts Henriks Saugmandsgors Ē e (*Henrik Saugmandsgaard Øe*) sniedza savus secinājumus lietā C-311/18 *Schrems II*[4] par datu nosūtīšanas mehānismu no ES uz ASV atbilstību Eiropas Savienības Pamattiesību hartai[5] (turpmāk – Harta), ņemot vērā ASV nacionālo drošības regulējumu. Savukārt 2020. gada 15. janvārī ģenerāladvokāts Manuels Kamposs Sančess-Bordona (*Manuel Campos Sánchez-Bordona*) publicēja vēl trīs secinājumus EST lietās par pienākumu elektronisko pakalpojumu sniedzējiem saglabāt datus – divās Francijas apvienotajās lietās C-511/18 *La Quadrature du Net u. c.* un C-512/18 *French Data Network u. c.*[6], Beļģijas lietā C-520/18 *Ordre des barreaux francophones un germanophone u. c.*[7] un Apvienotās Karalistes lietā C-623/17 *Privacy International*[8].

Raksta mērķis ir aplūkot iepriekš minētos EST lietās sniegtos ģenerāladvokāta secinājumus, lai akcentētu būtiskākās pamattiesību aizsardzības prasības attiecībā uz masveida uzraudzības pasākumu piemērošanu un to nozīmi, ieviešot jaunas uzraudzības metodes un tehnoloģijas.

## Ģenerāladvokāta secinājumi Eiropas Savienības Tiesas *Schrems II* lietā

EST *Schrems II* lieta ir turpinājums *Schrems I* lietai, kas aizsākās 2013. gadā, kad Maksimiliāns Šrems (*Maximilian Schrems*) iesniedza sūdzību Īrijas datu aizsardzības iestādē par *Facebook* veikto datu nodošanu uz ASV, uzskatot, ka

---

[2] Feldstein S. The Global Expansion of AI surveillance. 17.09.2019. Pieejams: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 [aplūkots 10.03.2020.].

[3] Khan M. EU plans sweeping regulation of facial recognision. 22.08.2019. Pieejams: https://www.ft.com/content/90ce2dce-c413-11e9-a8e9-296ca66511c9 [aplūkots 11.03.2020.].

[4] Ģenerāladvokāta Henrik Saugmandsgaard Øe 19.12.2019. secinājumi EST lietā C-311/18 Data Protection Commissioner pret Facebook Ireland un Schrems.

[5] Eiropas Savienības Pamattiesību harta. Pieņemta 12.12.2007. [12.03.2020. red.].

[6] Ģenerāladvokāta Manuel Campos Sánchez-Bordona 15.01.2019. secinājumi EST apvienotajās lietās C-511/18 La Quadrature du Net u. c. un C-512/18 French Data Network u. c.

[7] Ģenerāladvokāta Manuel Campos Sánchez-Bordona 15.01.2019. secinājumi EST lietā 520/18 Ordre des barreaux francophones un germanophone u. c.

[8] Ģenerāladvokāta Manuel Campos Sánchez-Bordona 15.01.2019. secinājumi EST lietā C-623/17 Privacy International.

ASV nacionālās drošības regulējums ES pilsoņu personas datiem nenodrošina pietiekamu aizsardzību. Pēc sūdzības noraidīšanas viņš pārsūdzēja lēmumu Augstākajā tiesā, kas savukārt iesniedza prejudiciāla nolēmuma lūgumu EST. 2015. gadā EST pieņēma spriedumu *Schrems* lietā,[9] atzīstot par spēkā neesošu Eiropas Komisijas lēmumu par aizsardzības līmeņa pietiekamību datu nodošanai uz ASV kā trešo valsti[10] jeb tā saukto drošās zonas lēmumu, ņemot vērā, ka ASV prakse attiecībā uz datu iegūšanu no privātiem uzņēmumiem nacionālās drošības nolūkos nav atbilstoša Hartai.

EST spriedums bija liels satricinājums datu aizsardzības pasaulei. Uzņēmumiem, lai nodotu datus no ES uz ASV, vajadzēja sākt izmantot citu datu nosūtīšanas pamatu. Kā to paredz Vispārīgā datu aizsardzības regula[11] (turpmāk – Regula), personas datus var nosūtīt uz trešo valsti, pamatojoties uz Eiropas Komisijas pieņemtu lēmumu par aizsardzības līmeņa pietiekamību (45. pants). Savukārt, ja šāda lēmuma nav, datus var nodot arī, pamatojoties uz atbilstošām garantijām, kas cita starpā var būt līgums starp datu nosūtītāju un saņēmēju, kurā ietvertas ar Komisijas lēmumu 2010/87/ES[12] apstiprinātās datu aizsardzības standartklauzulas (46. pants).

Pēc EST sprieduma, kad prasību atkārtoti izskatīja Īrijas uzraudzības iestāde, *Facebook Ireland* norādīja, ka dati tiek pārsūtīti uz ASV, pamatojoties uz Komisijas apstiprinātām standartklauzulām. Augstākā tiesa atkārtoti vērsās EST ar prejudiciālu jautājumu, lūdzot izvērtēt šī Komisijas lēmuma spēkā esamību. Pa to laiku 2016. gada 12. jūlijā Komisija pieņēma jaunu atbilstības lēmumu 2016/1250 jeb tā saukto ASV un ES "Privātuma vairogu".[13]

Ģenerāladvokāts secinājumos uzsver, ka pamatlieta ir vērsta vienīgi uz Komisijas lēmuma 2010/87/ES izvērtēšanu. Vispirms viņš norāda, ka ES tiesības ir piemērojamas personas datu pārsūtīšanai uz trešajām valstīm, kad šie dati atbilst komerciāliem mērķiem, pat ja šīs trešās valsts iestādes pārsūtītos datus var apstrādāt valsts drošības mērķiem (110. punkts). Turklāt augsts personas datu aizsardzības līmenis ir jānodrošina neatkarīgi no datu nosūtīšanas pamata.

Tālāk ģenerāladvokāts izvērtē Komisijas Lēmuma 2010/87/ES atbilstību Hartai un secina, ka nav atklājušies apstākļi, kas varētu ietekmēt tā spēkā esamību. Apstāklis, ka lēmums nav saistošs trešo valstu iestādēm, nav pamats, lai atzītu to par spēkā neesošu. Datu nosūtītājam un saņēmējam ir pienākums ievērot līguma nosacījumus un izvērtēt, vai nosūtīšanas gadījumā datu subjektu tiesības tiek ievērotas un vai ir pieejami efektīvi tiesiskās aizsardzības līdzekļi. Savukārt uzraudzības iestādēm ir pienākums apturēt vai aizliegt datu pārsūtīšanu, kad no līguma standartklauzulām izrietošie pienākumi nevar tikt ievēroti, ņemot

[9] EST 06.10.2015. spriedums lietā C-362/14 Maximillian Schrems pret Data Protection Commissioner.

[10] Komisijas Lēmums 2000/520/EK atbilstīgi Direktīvai 95/46 par pienācīgu aizsardzību, kas noteikta ar privātuma "drošības zonas" principiem un attiecīgajiem visbiežāk uzdotajiem jautājumiem, kurus izdevusi ASV Tirdzniecības ministrija. Pieņemts 26.07.2000. OV, 25.08.2020., L 215.

[11] Eiropas Parlamenta un Padomes Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula). Pieņemta 04.27.2016. [12.03.2020. red.].

[12] Komisijas Lēmums 2010/87 par līguma standartklauzulām attiecībā uz personas datu pārsūtīšanu trešās valstīs reģistrētiem apstrādātājiem saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK. Pieņemts 05.02.2010. [12.03.2020. red.].

[13] Komisijas Īstenošanas lēmums (ES) 2016/1250 saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK par pienācīgu aizsardzību, ko nodrošina ES un ASV privātuma vairogs. Pieņemts 12.07.2016. [12.03.2020. red.].

vērā trešās valsts tiesībās noteiktos pienākumus (128. punkts). Neatbildēts paliek jautājums, cik efektīvi praksē datu pārziņi un uzraudzības iestādes var izpildīt minētos pienākumus un vai personas tiesības var tikt efektīvi aizsargātas.[14]

Ģenerāladvokāts secinājumos norāda, ka par ASV un ES "Privātuma vairoga" lēmumu lemt nav nepieciešams, bet uzreiz pēc tam sniedz desmit lapas garu analīzi, pamatojot, kāpēc EST, ja tā tomēr lemtu par "Privātuma vairoga" spēkā esamību, būtu jāatzīst, ka tas ir pretrunā Hartas 7. pantā noteiktajām tiesībām uz privātās dzīves neaizskaramību, 8. pantā noteiktajām tiesībām uz personas datu aizsardzību, kā arī 47. pantā noteiktajām tiesībām uz efektīvu tiesību aizsardzību.

Atbilstoši Hartas 52. pantā[15] noteiktajam proporcionalitātes testam ģenerāladvokāts tālāk izvērtē tiesību uz privātās dzīves neaizskaramību un tiesību uz personas datu aizsardzību ierobežojumus, ASV regulējumā paredzot valsts iestādēm iespēju piekļūt no ES nosūtītajiem datiem un izmantot tos nacionālās drošības nolūkos. Vispirms ir konstatēts, ka nosacījums – ierobežojumiem ir jābūt "noteiktiem ar tiesību aktu" – neizpildās, jo tiesību aktos nav paredzēti skaidri un precīzi noteikumi, kā arī juridiski īstenojamas tiesības (266.–277. punkts). Lai gan ierobežojumiem ir leģitīms mērķis, proti, nodrošināt valsts drošību, tomēr tie nav samērīgi. Tiek norādīts, ka piekļuves pieprasījumi ir jāpārbauda tiesai vai citai neatkarīgai iestādei (293. punkts). Tiek vērsta uzmanība uz Regulas 23. panta 2. punktu, kas paredz, ka leģislatīvos pasākumos, kas ierobežo personas tiesības, ir jābūt ietvertiem konkrētiem noteikumiem, jo īpaši attiecībā uz apstrādes nolūkiem, personas datu kategorijām, ieviesto ierobežojumu darbības jomu, garantijām, lai novērstu ļaunprātīgu izmantošanu vai nelikumīgu piekļuvi vai nosūtīšanu, glabāšanas ilgumu, kā arī datu subjektu tiesībām saņemt informāciju par ierobežojumiem, izņemot tad, ja tas var kaitēt ierobežojuma mērķiem (294. punkts). Tiek secināts, ka konkrētajā gadījumā nav skaidrs, vai pastāv aizsardzības garantijas, kas ierobežotu personu loku, kurām tiek piemēroti uzraudzības pasākumi, vai nolūkus, kādiem dati var tikt vākti, tādējādi nodrošinot aizsardzības līmeni, kas ir atbilstošs Regulā un Hartas 7. un 8. pantā noteiktajam (301. punkts). Ģenerāladvokāts uzsver, ka ierobežojumiem ir jābūt nevis "cik vien iespējams piemērotiem", bet gan "stingri nepieciešamiem" (300. punkts).

Ģenerāladvokāts secinājumos arī konstatē, ka "Privātuma vairogs" neatbilst Hartas 47. pantā noteiktajām tiesībām uz efektīvu tiesību aizsardzību, jo nepastāv tiesas vai neatkarīgas valsts iestādes kontrole, ņemot vērā, ka izveidotais ombuda mehānisms nav noregulēts ar tiesību aktu, nav neatkarīgs, kā arī nav pakļauts neatkarīgai tiesas kontrolei (340 punkts).

Šobrīd EST izskatīšanā atrodas jauna tiešā lieta T738/16 *La Quadrature du Net u. c. pret Komisiju*[16] par "Privātuma vairoga" spēkā esamību, līdz ar to

[14] Kuner C. International data transfers, standard contractual clauses, and the Privacy Shield: the AG Opinion in Schrems II. 07.01.2020. Pieejams: https://europeanlawblog.eu/2020/01/07/international-data-transfers-standard-contractual-clauses-and-the-privacy-shield-the-ag-opinion-in-schrems-ii/ [aplūkots 11.03.2020.].

[15] Eiropas Savienības Pamattiesību hartas 52. panta pirmā daļa paredz, ka tiesību un brīvību izmantošanas ierobežojumiem ir: – jābūt noteiktiem tiesību aktos; – jārespektē tiesību un brīvību būtība; – jāatbilst vispārējas nozīmes mērķiem, ko atzinusi ES, vai vajadzībai aizsargāt citu personu tiesības un brīvības; – jābūt nepieciešamiem; – jābūt samērīgiem.

[16] Sk.: EST 25.10.2016. prasība EST lietā T-738/16 La Quadrature du Net u. c. pret Komisiju.

EST izskatīs šo jautājumu arī tad, ja, sekojot ģenerāladvokāta secinājumiem, tas netiks izvērtēts *Schrems II* lietā.

Ģenerāladvokāta secinājumos norādītie apsvērumi ir būtiski, izvērtējot jaunu uzraudzības tehnoloģiju, piemēram, sejas atpazīšanas tehnoloģiju ieviešanu un izmantošanu. Pirms šādu tehnoloģiju ieviešanas ir jāizvērtē, vai tās ir vajadzīgas, jo "var palīdzēt" un "ir piemērotas", lai sasniegtu konkrēto mērķi, piemēram, lai garantētu valsts vai sabiedrības drošību, kā arī vai tās ir "stingri nepieciešamas" un nepastāv citi mazāk tiesības ierobežojoši veidi un līdzekļi, kā šo mērķi sasniegt. Tikai pēdējā gadījumā ierobežojumi var tikt atzīti par tiesiskiem. Turklāt ir jābūt izveidotam neatkarīgam uzraudzības mehānismam, lai kontrolētu šādu pasākumu piemērošanu. Atbilstoši Regulas 23. panta 2. punktam šādiem ierobežojumiem ir jābūt noregulētiem nacionālajā tiesiskajā regulējumā, paredzot konkrētus nosacījumus attiecībā uz datu apstrādi, lai nodrošinātu to samērīgumu un tiesiskumu.

EST izskatīšanā līdzās lietām par datu nodošanu no ES uz ASV, ievērojot ASV iestāžu praksi tālāk iegūt datus no privātiem uzņēmumiem drošības apsvērumu dēļ, ir arī vairākas lietas par ES dalībvalstu regulējumu, kas uzliek pienākumu elektronisko pakalpojumu sniedzējiem saglabāt datus valsts drošības nolūkā, tās tiks aplūkotas darba turpinājumā.

## Ģenerāladvokāta secinājumi Eiropas Savienības Tiesas lietās par valstu datu saglabāšanas regulējumu

EST ir jau izskatījusi vairākas lietas, izvērtējot masveida uzraudzības pasākumu piemērošanu. 2014. gadā EST pieņēma spriedumu *Digital rights Ireland* lietā,[17] atzīstot par spēkā neesošu tā saukto Datu saglabāšanas direktīvu,[18] kas paredzēja pienākumu elektronisko komunikāciju pakalpojumu sniedzējiem saglabāt datus drošības iestāžu vajadzībām. Savukārt 2016. gada spriedumā *Tele2 Sverige* un *Watson* apvienotajās lietās[19] EST atzina, ka E-privātuma direktīva[20] neaizliedz dalībvalstīm pieņemt tiesību aktus, kas atvieglotu mērķtiecīgu datu plūsmas un atrašanās vietas datu saglabāšanu smagu noziegumu apkarošanai, tajā pašā laikā tā aizliedz nacionālajās tiesībās paredzēt normas, kas uzliek elektronisko sakaru pakalpojumu sniedzējiem visaptverošu un nediferencētu datu saglabāšanas pienākumu.

Vairākas ES dalībvalstis šādai EST interpretācijai nepiekrita, jo uzskatīja, ka tām tiek atņemts būtisks instruments, kas nepieciešams, lai aizsargātu valsts drošību un cīnītos ar terorismu. Šis pretējais viedoklis ir pamatā četrām jaunām EST prejudiciāla nolēmuma lūguma lietām, kurās 2020. gada 15. decembrī tika publicēti ģenerāladvokāta secinājumi.

---

[17] EST 08.04.2014. spriedums apvienotajās lietās C293/12 Digital Rights Ireland u. c. un C594/12 Seitlinger u. c.

[18] Eiropas Parlamenta un Padomes Direktīva par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK. Pieņemta 15.03.2006. OV, 13.04.2006., L 105.

[19] EST 21.02.2016. spriedums apvienotajās lietās C-203/15 Tele2 Sverige un C-698/15 Watson u. c.

[20] Eiropas Parlamenta un Padomes Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju). Pieņemta 12.07.2002. [11.03.2020. red.].

Atšķirībā no *Tele2 Sverige* un *Watson* lietas, kurā EST izvērtēja dalībvalstu regulējumu, kas paredzēja datu saglabāšanas pienākumu, lai apkarotu smagus noziegumus, jaunajās EST lietās jautājumi ir uzdoti par valsts drošības aizsardzību. EST tiek jautāts, vai gadījumā, ja šādu pasākumu, kuri ierobežo tiesības uz privātumu un datu aizsardzību, mērķis ir valsts drošības garantēšana, interpretācija ir atšķirīga, t. i., vai E-privātuma direktīva ir piemērojama un vai tomēr šādā gadījumā nebūtu pieļaujams paredzēt visaptverošu un nediferencētu datu saglabāšanas pienākumu.

Ģenerāladvokāts secinājumos EST lietā C-511/18 *La Quadrature du Net u. c.*, kā arī pārējos vienlaikus publicētajos secinājumos vispirms noraida argumentu, ka ES tiesības nav attiecināmas uz valsts darbību nacionālās drošības jomā. Viņš norāda, ka E-privātuma direktīva ir piemērojama, kad elektronisko komunikācijas pakalpojumu sniedzējiem ir pienākums saglabāt datus, neatkarīgi no tā, ka mērķis ir garantēt valsts drošību un cīnīties ar terorismu (42. punkts). ES tiesības nebūtu attiecināmas uz darbībām, ko veiktu valsts iestādes pašas, neiesaistot privātus uzņēmumus (79. punkts).

Ģenerāladvokāta secinājumos ir izvērsti analizēts elektronisko komunikāciju pakalpojumu sniedzēju pienākums saglabāt datus "visaptveroši un nediferencēti" valsts drošības apsvērumu dēļ. Vispirms tiek norādīts, ka no šī vispārējā aizlieguma tomēr būtu pieļaujams izņēmums. Proti, patiesi ārkārtējās situācijās, kuras raksturo tūlītēji draudi vai ārkārtīgs risks, kas attaisno oficiālu ārkārtas situācijas pasludināšanu dalībvalstī, uz noteiktu laiku šāds plašs un visaptverošs pienākums tomēr var tikt uzlikts (105. punkts).

Tomēr, atsaucoties uz *Tele2 un Watson* nolēmumu, tika norādīts, ka E-privātuma direktīvai ir pretrunā valsts tiesiskais regulējums, ar ko elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums visaptveroši un nediferencēti saglabāt visu abonentu un lietotāju informāciju par datu plūsmu un atrašanās vietas datus attiecībā uz visiem elektronisko komunikāciju līdzekļiem, neatkarīgi no tā, ka mērķis ir garantēt valsts drošību, teritorijas aizsardzību vai sabiedrības drošību. Tiek vērsta uzmanība, ka šāds pienākums nevar vispārīgi attiekties uz visiem abonentiem un lietotājiem bez jebkādas diferencēšanas, jo tādējādi tas tiek piemērots "pat attiecībā uz personām, par kurām nepastāv nekādas norādes, kas var ļaut uzskatīt, ka to rīcībai varētu būtu kaut netieša vai attālināta saikne ar smagiem noziegumiem" (115. punkts). Proti, šāds tiesiskais regulējums "neprasa nekādu saikni starp datiem, kurus ir paredzēts saglabāt, un draudiem sabiedrības drošībai" (116. punkts).

Praktiski visas tiesvedībā pārstāvētās valdības, kā arī Komisija vienprātīgi norādīja, ka daļēja un diferencēta personas datu saglabāšana ne tikai radītu tehniskas grūtības, bet arī liegtu valsts izlūkdienestiem iespēju piekļūt informācijai, kas ir vajadzīga, lai identificētu draudus sabiedrības drošībai un valsts aizsardzībai, kā arī veiktu teroristu uzbrukumu organizatoru kriminālvajāšanu (129. punkts). Atbildot uz šo argumentu, ģenerāladvokāts uzsvēra, ka terorisma apkarošanas līdzekļiem un metodēm ir jāatbilst tiesiskas valsts prasībām un, "ja vadītos tikai no efektivitātes apsvērumiem vien, tiesiska valsts zaudētu savas raksturiezīmes un ārkārtas gadījumos, iespējams, pati kļūtu par apdraudējumu pilsoņiem" (130. un 131. punkts). Lai gan ir grūti, tomēr nav neiespējami precīzi un saskaņā ar objektīviem kritērijiem noteikt gan to datu kategorijas, kuru saglabāšana tiek uzskatīta par nepieciešamu, gan attiecīgo personu loku (135. punkts).

Ģenerāladvokāts secinājumos uzsver arī *Tele2 un Watson* lietā noteikto procesuālo garantiju nozīmi, paredzot datu saglabāšanas pienākumu. Tiesību aktos, izņemot atbilstoši pamatotus steidzamības gadījumus, ir jābūt paredzētai iepriekšējai tiesas vai neatkarīgas iestādes piekļuves pieprasījumu kontrolei (147.–152. punkts), kā arī noteiktam pienākumam informēt attiecīgās personas par to, ka kompetentās iestādes veic viņu personas datu apstrādi, ja vien šī informēšana netraucē minēto iestāžu darbību (139. punkts).

Lai gan apskatītajās lietās tiek izvērtēts elektronisko komunikāciju pakalpojumu sniedzēju pienākums saglabāt datus, ģenerāladvokāta secinājumi ir būtiski arī attiecībā uz citām masveida novērošanas metodēm un līdzekļiem, tai skaitā uz jauno uzraudzības tehnoloģiju ieviešanu. Tajos ir uzsvērta nepieciešamība izvērtēt tos līdzekļus un metodes, ko valsts ievieš un izmanto, lai garantētu tādus vispārējo interešu mērķus kā, piemēram, valsts drošība un sabiedrības drošība. Vairāki gadījumi attiecībā uz sejas atpazīšanas tehnoloģiju piemērošanu liecina, ka praksē bieži vien tās tiek ieviestas, neizvērtējot, vai tas ir "stingri" jeb "absolūti" nepieciešams un vai tas ir samērīgi, kā arī tās tiek izmantotas, neinformējot personas un sabiedrību.[21] Minētās tehnoloģijas nevar tikt piemērotas attiecībā uz visām personām, visu laiku un visās vietās, bet ir stingri jāizvērtē, kādos gadījumos tas ir stingri nepieciešams, ierobežojot to piemērošanu. Ir ļoti svarīgi skaidri definēt, vai, kad un kā mākslīgo intelektu var izmantot, lai automātiski identificētu cilvēkus, un nošķirt personas identificēšanu no tās izsekošanas, kā arī mērķtiecīgu uzraudzību no masveida novērošanas.[22]

Ne vienmēr mērķis attaisno līdzekļus, proti, ne visas tehnoloģijas, līdzekļi un metodes tikai tāpēc, ka tās ir pieejamas un var būt piemērotas mērķa sasniegšanai, ir arī jāizmanto, bet gan ir nepieciešams rūpīgi izvērtēt, vai to izmantošana ir "stingri nepieciešama" konkrētā mērķa sasniegšanai, ņemot vērā to ietekmi uz pamattiesībām, kā arī uz demokrātiju un tiesiskumu.[23]

## Kopsavilkums

1. Jautājums, cik lielā mērā personas pamattiesības var tikt ierobežotas, lai nodrošinātu tādus vispārējo interešu mērķus kā valsts drošība un sabiedrības drošība, ir aktuālāks kā nekad līdz ar jaunu uzraudzības tehnoloģiju, jo īpaši mākslīgā intelekta tehnoloģiju, arvien plašāku ieviešanu un izmantošanu. Vēl būtiskāks šis jautājums ir kļuvis laikā, kad, lai cīnītos pret Covid-19 globālās pandēmijas radīto apdraudējumu, valstis visā pasaulē, tai skaitā ES, strauji ievieš jaunas uzraudzības tehnoloģijas, kas rada bažas, vai šādi pasākumi netiks saglabāti arī pēc ārkārtas situācijas beigām.
2. Lai gan valstu pasākumi, piemēram, attiecībā uz valsts un sabiedrības drošību, var būt ārpus ES tiesību darbības jomas, tajā pašā laikā EST augstajiem

[21] Sk., piemēram: EDPB. Facial recognition in school renders Sweden's first GDPR fine. 22.08.2019. Pieejams: https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en [aplūkots 11.03.2020.].

[22] AI HLEG. Ethics Guidelines for Trustworthy AI. 2019. Pieejams: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai [aplūkots 11.03.2020.].

[23] Sk.: Council of Europe. Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis. A toolkit for member states. 07.04.2020. Pieejams: https://rm.coe.int/sg-inf-2020-11-respecting-democracy-rule-of-law-and-human-rights-in-th/16809e1f40 [aplūkots 08.04.2020.].

standartiem var būt būtiska nozīme, lai ietekmētu valstu masveida uzraudzības pasākumu piemērošanas praksi un stiprinātu pamattiesību aizsardzību nacionālajā līmenī.

3. 2019. gada decembrī pieņemtajos ģenerāladvokāta secinājumos EST lietā *Schrems II* par datu nodošanas mehānismiem no ES uz ASV, kā arī trijos 2020. gada janvārī publicētajos secinājumos lietās par datu saglabāšanas pienākumu kā būtiskākais nosacījums, piemērojot masveida uzraudzības pasākumus, ir norādīts pienākums izvērtēt, vai piemērotie pasākumi ir "stingri nepieciešami" konkrētā mērķa sasniegšanai un vai tie ir samērīgi jeb proporcionāli ar šo mērķi. Visās lietās ir uzsvērta nepieciešamība tiesību aktos noteikt atbilstošas procesuālās garantijas, jo īpaši tiesas vai neatkarīgas iestādes kontroli un pienākumu informēt personas par šādu pasākumu piemērošanu. Šos nosacījumus ir būtiski ievērot arī pirms jaunu uzraudzības tehnoloģiju ieviešanas.
4. Nav pieļaujams, ka masveida uzraudzības pasākumi, kas būtiski ierobežo personu pamattiesības, tai skaitā jaunās uzraudzības tehnoloģijas, tiek ieviesti un piemēroti, neizvērtējot to proporcionalitāti un nepieciešamību, nenodrošinot atbilstošas procesuālas garantijas, jo īpaši neinformējot personas. Šāda prakse ne tikai ir pretrunā ar personu pamattiesībām, bet arī var apdraudēt tiesiskumu un demokrātiskās vērtības.
5. Gaidāmajiem EST spriedumiem apskatītajās lietās var būt būtiska nozīme, lai liktu valstīm pārvērtēt tendenci arvien plašāk izmantot masveida uzraudzības pasākumus un pirms šādu pasākumu ieviešanas izvērtēt to ietekmi uz pamattiesībām, kā arī demokrātiskām vērtībām un sabiedrību kopumā.