Eiropas Ekonomikas un sociālo lietu komitejas atzinums par tematu "Priekšlikums Eiropas Parlamenta un Padomes regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula)"

(COM(2017) 10 final – 2017/0003 (COD))

(2017/C 345/23)

Ziņotāja: **Laure BATUT**

Apspriešanās	Eiropas Parlaments, 16.2.2017.
	Eiropas Savienības Padome, 9.3.2017.
Juridiskais pamats	Līguma par Eiropas Savienības darbību 16. un 114. pants.
Atbildīgā specializētā nodaļa	Transporta, enerģētikas, infrastruktūras un informācijas sabiedrības specializētā nodaļa
Pieņemts specializētās nodaļas sanāksmē	14.6.2017.
Pieņemts plenārsesijā	5.7.2017.
Plenārsesija Nr.	527
Balsojuma rezultāts	155/0/5
(par/pret/atturas)	

1. **Secinājumi un ieteikumi**

1.1. EESK pauž dziļu nožēlu, ka tiesību aktu par datu aizsardzību pārklāšanās, to apjoms un sarežģītība, nepieciešamība pāriet no viena teksta uz otru un atpakaļ, lai tos būtu iespējams saprast, ir cēlonis tam, ka tos lasīt un īstenot var tikai to personu loks, kurām ir īpašas zināšanas, un ka to pievienotā vērtība – šis jēdziens netiek ietverts nevienā regulas priekšlikumā – pilsoņiem nav izprotama. Iesaka publicēt tiešsaistē apkopojošu brošūru, kurā šie tiesību akti būtu aprakstīti sabiedrībai un kas nodrošinātu to pieejamību visiem.

1.2. EESK uzsver, ka no ietekmes novērtējumā piedāvātajiem variantiem Komisija ir izvēlējusies to, kas privātumu stiprinās "samērīgi". Vai tā nolūks ir nodrošināt līdzsvaru ar ražotāju interesēm? Komisija neprecizē, kuri no "vērienīgas" privātuma stiprināšanas elementiem varētu kaitēt ražotāju interesēm. Šāda pozīcija vājina tiesību aktu jau pašā saknē.

1.3. EESK iesaka Komisijai:

1) ņemt vērā, ka pašlaik jebkas var kļūt par datiem un par elektroniskas saziņas priekšmetu, atstājot sekas uz fizisku un juridisku personu privātumu;

2) precizēt Eiropas Savienības Pamattiesību hartas un cilvēktiesību piemērošanu priekšlikumā (5., 8. un 11. pants), kā arī iespējas ar valstu tiesību aktiem noteikt ierobežojumus (26. apsvērums);

3) pārskatīt priekšlikuma 5. un 6. pantu. Internets un mobilie sakari ir vispārējas nozīmes pakalpojumi un to piekļuvei ir jābūt universālai, pieejamai un par pieņemamām cenām, un patērētājiem nav jābūt spiestiem pēc operatora prasības piekrist viņu datu apstrādei, lai šos pakalpojumus varētu izmantot. Tāpēc ir jāparedz pienākums sistemātiski piedāvāt lietotājam iespēju no tās atteikties, balstoties uz saprotamu informāciju (sīkdatnes, "pārraudzības siena" u. c.);

4) skaidri noteikt, ka *lex specialis*, kas ierosināts, lai papildinātu Vispārīgo datu aizsardzības regulu (VDAR), atbilst minētā tiesību akta vispārīgajiem principiem un nemazina tajā noteiktos aizsardzības pasākumus un ka jebkāda apstrāde, tostarp tīmekļa mērķauditorijas mērīšana (*web audience measuring*), notiek saskaņā ar VDAR principiem (8. pants);

5) nodrošināt regulatīvo stabilitāti iedzīvotājiem un uzņēmumiem un šajā nolūkā precizēt regulas tekstu un īstenošanas pasākumu saturu, lai neradītu pārāk daudz deleģēto aktu;

6) izstrādāt stratēģiju, kas dotu iespēju informēt visus patērētājus par to, ka Savienība nav atteikusies no cilvēktiesību ievērošanas principiem un ka tā vēlas panākt, lai privātās dzīves neaizskaramību ievērotu ne tikai elektronisko sakaru operatori, bet arī *OTT* (*over-the-top*) pakalpojumu sniedzēji;

7) nepieļaut iespēju, ka, pateicoties elektroniskajiem sakariem, veselības jomu varētu izmantot kā plaši atvērtas durvis privātuma un personas datu izmantošanai peļņas nolūkos;

8) risināt problēmas, kas saistītas ar sadarbīgo ekonomiku, datu nosūtīšanu un lietošanu, izmantojot elektroniskos sakarus ar tādu platformu starpniecību, kuras nereti atrodas ārpus ES;

9) ņemt vērā lietu internetu (*IoT*), kas ir ļoti nediskrēts un, kad dati tiek nosūtīti, izmantojot elektroniskos sakarus, var izraisīt privātuma apdraudējumu;

10) ņemt vērā datu pārsūtīšanas sekas un aizsargāt personu glabātos datus, jo lielākā daļa no tiem ir privāti (neatkarīgi no saskarnes, tostarp mākoņdatošanā);

11) precizēt aizsardzību datu mašīnas-mašīnas (*M2M*) pārsūtīšanā un šim jautājumam veltīt atsevišķu pantu, nevis tikai vienu apsvērumu (12);

12) lai palīdzētu iedzīvotājiem orientēties daudzajos dokumentos un izmantot savas tiesības, izveidot Eiropas portālu (Tieslietu ģenerāldirektorāts), kas būtu visiem pieejams un dotu iespēju piekļūt Eiropas un valstu dokumentiem, tiesiskās aizsardzības līdzekļiem un tiesu praksei (piemērs: izskaidrot 25. apsvērumu un 12. un 13. pantu);

13) dot uzraudzības iestādēm līdzekļus uzdevumu izpildei (Eiropas Datu aizsardzības uzraudzītājam, valstu iestādēm);

14) dot iespēju patērētājiem Eiropas līmenī iesniegt kolektīvās prasības, lai panāktu savu tiesību ievērošanu, ejot tālāk ar jaunu direktīvu nekā ar ieteikumu C(2013)401&3539 ([1]).

2. **Tiesiskā regulējuma elementi**

2.1. Elektronisko sakaru tīkli ir būtiski mainījušies kopš stājusies spēkā Direktīva 95/46/EK un Direktīva 2002/58/EK ([2]) par privātās dzīves aizsardzību elektronisko komunikāciju nozarē.

2.2. **Vispārīgā datu aizsardzības regula (VDAR), kas pieņemta 2016. gadā**, (Regula (ES) 2016/679) ir kļuvusi par pamatu darbībām, tajā ir noteikti galvenie principi, tostarp attiecībā uz tiesu datiem un krimināltiesiskajiem datiem. Saskaņā ar šo regulu personas datus var vākt tikai stingri noteiktos apstākļos un likumīgos nolūkos, ievērojot konfidencialitāti (VDAR 5. pants).

2.2.1. Komisija **2016. gada oktobrī** iesniedza priekšlikumu direktīvai par Eiropas Elektronisko sakaru kodeksa ([3]) izveidi (300 lappušu apjomā), kas vēl nav pieņemta, taču Komisija uz to atsaucas saistībā ar atsevišķām definīcijām, kas nav minētas ne VDAR, ne izskatāmajā dokumentā.

2.2.2. Divos 2017. gada janvāra priekšlikumos precizēti atsevišķi aspekti, pamatojoties uz VDAR; šie priekšlikumi ir šādi: Priekšlikums Regulai par personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un šādu datu brīvu apriti (**COM(2017) 8 final**, ziņotājs: J. PEGADO LIZ) un izskatāmais dokuments (**COM(2017) 10 final**) par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā.

2.3. Visi trīs iepriekš minētie dokumenti būs **jāpiemēro, sākot no viena un tā paša datuma: 2018. gada 25. maija**, un to mērķis ir saskaņot tiesības un kontroles procedūras.

2.4. Jāpiezīmē, ka nolūkā sekmēt šādu pieeju tika pieņemts lēmums privātuma aizsardzības nolūkā izmantot ES regulu, nevis direktīvu.

([1]) 11.06.2013. – IP/13/525; Memo13/531 – Tieslietu ĢD.

([2]) Ar Direktīvu 2002/58/EK, piemēram, tika aizliegtas mēstules (13. pants), pēc 2009. gadā veiktā grozījuma ieviešot tā dēvēto *opt-in* principu, saskaņā ar kuru operatoram ir jāsaņem adresāta piekrišana, lai varētu viņam sūtīt komerciņojumus.

([3]) COM(2016) 590 final, 12.10.2016., Priekšlikums Eiropas Parlamenta un Padomes Direktīvai par Eiropas Elektronisko sakaru kodeksa izveidi, 2. lpp. (OV C 125, 21.4.2017., 56. lpp.);

3. **Ievads**

3.1. Pilsoniskā sabiedrība vēlas zināt, vai pilnīgi digitālā pasaulē, kuras aprises veidojas, ES nodrošina pievienoto vērtību, kas garantē privātās dzīves telpu, kurā var justies brīvi un būt bez bažām.

3.2. Pastāvīgi ģenerētie dati visus lietotājus padara izsekojamus un identificējamus it visur. Fiziski eksistējošos centros, kuri lielākoties atrodas ārpus Eiropas, veiktā datu apstrāde rada bažas.

3.3. Lielie dati (*Big Data*) ir kļuvuši par valūtu – to viedā apstrāde ļauj "profilēt" un padarīt par preci fiziskas un juridiskas personas un tā pelnīt naudu, pašiem lietotājiem par to bieži nemaz nezinot.

3.4. Taču papildus interneta piekļuves sniedzējiem datu apstrādes nozarē ir iesaistījušies arī jauni dalībnieki, un tāpēc būtu īpaši svarīgi tiesību aktus pārskatīt.

4. **Priekšlikuma kopsavilkums**

4.1. Ar šo tiesību aktu Komisija vēlētos izveidot līdzsvaru starp patērētājiem un ražotājiem:

— operatoriem atļauts izmantot datus, taču galalietotājs var saglabāt kontroli ar skaidri paustas piekrišanas palīdzību,

— operatoriem noteikta prasība norādīt, ko viņi ar šiem datiem darīs,

— izvēlēts ir trešais ietekmes novērtējumā ietvertais variants, kurā priekšroka dota samērīgai privātuma stiprināšana, bet ne ceturtais variants, kurā tika piedāvāta vērienīga stiprināšana.

4.2. Priekšlikuma nolūks ir izvērst VDAR, kas ir vispārēji piemērojama tieši tāpat kā privāto datu konfidencialitāte un tiesības uz datu dzēšanu, un tas attiecas konkrēti uz privātās dzīves neaizskaramības un personas datu aizsardzības aspektu telesakaru nozarē; tajā ierosināts ieviest stingrākus noteikumus privātuma aizsardzības jomā, kā arī koordinētas pārbaudes un sankcijas.

4.3. Tajā nav noteikti konkrēti pasākumi attiecībā uz pašu lietotāju radītām personas datu "plaisām", taču jau pirmajos pantos (5. pantā) ir apstiprināts elektronisko sakaru konfidencialitātes princips.

4.4. Pakalpojumu sniedzēji drīkst apstrādāt elektronisko sakaru saturu:

— lai sniegtu pakalpojumu galalietotājam, kurš ir devis savu piekrišanu,

— attiecīgajiem galalietotājiem, kas ir devuši piekrišanu (6. panta 3. punkta a) un b) apakšpunkts).

4.5. Viņiem ir pienākums dzēst saturu pēc tam, kad adresāti to ir saņēmuši, vai padarīt šādu saturu anonīmu.

4.6. Saskaņā ar VDAR 4. panta 11. punktu "piekrišana" ir jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei.

4.7. Projektā saglabāta **skaidri paustas piekrišanas** prasība, kas definēta VDAR, pierādīšanas pienākumu nosakot operatoriem.

4.8. "Apstrāde" balstīta uz piekrišanu. Pārzinim ir jāspēj "uzskatāmi parādīt, ka datu subjekts ir piekritis savu personas datu apstrādei" (VDAR 7. panta 1. punkts).

4.9. Ar ES vai valstu tiesību aktiem varētu radīt atsevišķus konfidencialitātes ierobežojumus (pienākumus un tiesības), lai aizstāvētu sabiedrības intereses vai nodrošinātu pārbaudes.

4.10. Fiziskām personām ir jābūt devušām savu piekrišanu par iekļaušanu publiski pieejamā elektroniskā sarakstā un viņām jābūt iespējai savus datus pārbaudīt un labot (15. pants).

4.11. Tiesības iebilst visiem lietotājiem ļauj bloķēt tādu savu datu izmantošanu, kuri uzticēti trešai pusei (piemēram, tirgotājam), kā arī katra ziņojuma nosūtīšanas laikā (16. pants). Jaunie noteikumi uzlabos lietotāju iespējas pārvaldīt savus uzstādījumus (sīkdatnes, identifikatori), un nepasūtīti paziņojumi (mēstules, ziņojumi, SMS, zvani) lietotāja piekrišanas neesamības gadījumā varēs tikt bloķēti.

4.12. Attiecībā uz zvanu identifikāciju un nevēlamu zvanu bloķēšanu (12. un 14. pants) regulā ir uzsvērts, ka šādas tiesības ir arī juridiskām personām.

4.13. Kontroles sistēmas uzbūve atbilst VDAR (VI nodaļa par uzraudzības iestādēm un VII nodaļa par sadarbību starp uzraudzības iestādēm).

4.13.1. Tieši dalībvalstīm un to valsts iestādēm, kuras ir atbildīgas par datu aizsardzību, būs jāievēro konfidencialitātes noteikumi. Citas uzraudzības iestādes varēs savstarpējās palīdzības ietvaros sagatavot iebildumus, ko iesniegt valstu uzraudzības iestādēm. Tās sadarbojas ar valstu uzraudzības iestādēm un ar Eiropas Komisiju konsekvences mehānisma ietvaros (VDAR 63. pants).

4.13.2. Savukārt Eiropas Datu aizsardzības kolēģijas uzdevums ir gādāt par šīs regulas konsekventu piemērošanu (VDAR 68. un 70. pants).

Tās uzdevums varētu būt publicēt pamatnostādnes, ieteikumus un paraugpraksi, lai sekmētu regulas piemērošanu.

4.14. Fiziskām un juridiskām personām, kuras ir galalietotāji, ir pieejami tiesiskās aizsardzības līdzekļi, lai aizstāvētu savas intereses, pret kurām ir izdarīti pārkāpumi; tās varēs saņemt kompensāciju par nodarīto kaitējumu.

4.15. Iecerētās administratīvo naudas sodu summas būs atturošas, jo to apmērs jebkuram pārkāpējam var sasniegt 10 miljonus euro, savukārt uzņēmumiem – līdz 2 % no kopējā visā pasaulē iepriekšējā finanšu gadā sasniegtā gada apgrozījuma atkarībā no tā, kuras summas apmērs ir lielāks (23. pants). Dalībvalstis nosaka sankcijas gadījumos, kad administratīvais naudas sods netiek piemērots, un attiecīgi informē Komisiju

4.16. Jaunais tiesību akts par privātās dzīves neaizskaramību un personas datu izmantošanu būs **piemērojams no 2018. gada 25. maija** – tā paša datuma, no kura būs piemērojama arī 2016. gada VDAR, Regula par personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un projekts direktīvai par Eiropas Elektronisko sakaru kodeksa izveidi (COM(2016) 590 final), ja šie dokumenti tiks pieņemti.

4.17. *Lex specialis*, ar ko īsteno VDAR, piemērošanas joma:

— ***ratione jure*: juridiskais pamats**

Pamatā ir LESD 16. pants (datu aizsardzība) un 114. pants (vienotais tirgus), kā arī Pamattiesību hartas 7. un 8. pants. Regula papildinās VDAR attiecībā uz datiem, kurus var uzskatīt par personas datiem.

— ***ratione personae*: dalībnieki**

Tie ir galalietotāji, fiziskas un juridiskas personas, kas definētas Eiropas Elektronisko sakaru kodeksā iepretim visiem sakaru pakalpojumu sniedzējiem, ne tikai tradicionālajiem pakalpojumu sniedzējiem, bet jo īpaši jaunajiem dalībniekiem, kuru jaunie pakalpojumi lietotājiem nesniedz garantijas. Tā dēvētie *OTT* "apiešanas" paņēmieni (tūlītējā ziņapmaiņa, SMS, paņēmieni ar interneta protokolu, daudzfaktoru saskarnes u. c.) šobrīd nav pašreizējo tekstu piemērošanas jomā.

— ***ratione materiae*: dati**

Priekšlikums neietver noteikumu par datu saglabāšanu mākoņdatošanā un ļauj dalībvalstīm rīkoties saskaņā ar VDAR 23. pantu par iebilduma tiesību ierobežojumiem un Tiesas jurisdikciju (sk. pamatojuma 1.3. punktu).

Lietotājam būs jādod sava piekrišana sistēmās ģenerēto datu un metadatu (datuma, laika, vietas u. c.) saglabāšanai, pretējā gadījumā dati būs jāpadara anonīmi vai jādzēš.

— ***ratione loci*: kur?**

Iestādes veic apstrādes darbības dalībvalstīs, vai arī viena no iestādēm, kas atrodas kādā dalībvalstī, tiek uzskatīta par vadošo uzraudzības iestādi. Valstu uzraudzības iestādes pildīs savus uzdevumus, un Eiropas Datu aizsardzības uzraudzītājs (EDAU) pārraudzīs visu procesu.

4.18. ES mērķi: digitālais vienotais tirgus

— Viens no digitālā vienotā tirgus mērķiem ir radīt digitālajiem pakalpojumiem drošus apstākļus un panākt lietotāju uzticēšanos, lai būtu iespējams attīstīt, piemēram, tiešsaistes tirdzniecību, inovāciju un pastarpināti radīt darbvietas un izaugsmi (pamatojums, 1.1. punkts).

— Izskatāmajā regulas projektā ir skatīts arī jauns veids tiesību aktu saskaņošanai un konsekvences nodrošināšanai starp dalībvalstīm.

— Reizi trijos gados Komisija veiks regulas īstenošanas izvērtēšanu un par to ziņos Eiropas Parlamentam, Padomei un EESK (28. pants).

5. **Vispārīgas piezīmes**

5.1. Komiteja atzinīgi vērtē to, ka vienlaikus visā ES tiek ieviests konsekvents noteikumu kopums, kuru nolūks ir aizsargāt fizisku un juridisku personu tiesības, kas saistītas ar digitālo datu izmantošanu ar elektronisko sakaru palīdzību.

5.1.1. Atzinīgi vērtē faktu, ka Savienība pilda savu pilsoņu un patērētāju tiesību aizstāves lomu.

5.1.2. Lai arī nolūks ir saskaņošana, Komiteja uzsver, ka daudzu koncepciju interpretācija ir dalībvalstu ziņā, tādējādi šī regula kļūst par sava veida direktīvu, kas atstāj plašas iespējas personas datus padarīt par preci. Īpaši veselības nozare ir kā atvērtas durvis personas datu ievākšanai milzīgos apjomos.

5.1.3. Priekšlikuma 11. panta 1. punkts, 13. panta 2. punkts, 16. panta 4. un 5. punkts un 24. pants vairāk ir vērtējami kā "transponēšanas" noteikumi, kas būtu piemēroti direktīvai, taču ne regulai. Ar mērķi uzlabot pakalpojumu kvalitāti, operatoriem ir sniegta pārāk plaša rīcības brīvība (5. un 6. pants). Šai regulai vajadzētu būt neatņemamai tā sauktā Eiropas Elektronisko sakaru kodeksa direktīvas priekšlikuma (COM(2016) 590 final) daļai.

5.1.4. EESK pauž dziļu nožēlu, ka šo tiesību aktu pārklāšanās, to apjoms un sarežģītība, ir cēlonis tam, ka tos lasīt var tikai to personu loks, kurām ir īpašas zināšanas. Realitātē pastāvīgi ir nepieciešams pāriet no viena teksta uz otru un atpakaļ. Turklāt pilsoņi nevar saskatīt pievienoto vērtību. Šī apgrūtinātā lasīšana un priekšlikuma sarežģītība ir pretrunā Normatīvās atbilstības un izpildes programmas (REFIT) garam un mērķim uzlabot likumdošanas procesu, to būs grūti interpretēt un radīsies plaisas aizsardzībā.

5.1.5. Piemērs: regulas priekšlikumā nav ietverta "operatora" definīcija; tā ir jāmeklē Eiropas Elektronisko sakaru kodeksa projektā ([4]), kurš vēl nav stājies spēkā un ar kuru tiks grozīti nozares noteikumi saistībā ar digitālo vienoto tirgu, t. i., grozītā Pamatdirektīva 2002/21/EK, grozītā Atļauju izsniegšanas direktīva 2002/20/EK, grozītā Universālā pakalpojuma direktīva 2002/22/EK, grozītā Piekļuves direktīva 2002/19/EK, Regula (EK) Nr. 1211/2009, ar ko izveido *BEREC*, Radiofrekvenču spektra lēmums 676/2002/EK, Lēmums 2002/622/EK, ar ko izveido radiofrekvenču spektra politikas grupu un Lēmums 243/2012/ES, ar ko izveido radiofrekvenču spektra daudzgadu politikas programmu. Galvenais atsauces dokuments, protams, paliek VDAR (sk. 2.2. punktu), ko ierosināts papildināt ar šo priekšlikumu un tas tātad ir pakārtots.

5.2. EESK īpaši izceļ 8. panta saturu, kurā ir runa par galalietotāja galiekārtā glabātās informācijas aizsardzību un iespējamiem izņēmumiem – šis pants ir ārkārtīgi svarīgs, jo tas dod informācijas sabiedrībai iespēju piekļūt privātai informācijai. Izceļ arī 12. panta saturu, kas saistīts ar izsaucošā numura un savienotā numura uzrādīšanas ierobežošanu, jo šie punkti lasītājam bez īpašas sagatavotības ir grūti uztverami.

5.2.1. 1995. gada direktīvā (2. pantā) "personas dati" ir definēti kā "jebkura informācija attiecībā uz identificētu vai identificējamu fizisku personu ("datu subjektu")". Ar izskatāmo regulu datu aizsardzība tiek attiecināta arī uz metadatiem un turpmāk tā tiks piemērota gan fiziskām, gan juridiskām personām. No jauna jāuzsver, ka projekta mērķi ir divi: no vienas puses, aizsargāt personas datus un, no otras puses, nodrošināt elektronisko sakaru datu un elektronisko sakaru pakalpojumu brīvu apriti Savienībā (1. pants).

([4]) COM(2016) 590 un 1. līdz 11. pielikums (12.10.2016.) (OV C 125, 21.4.2017., 56. lpp.).

5.2.2. EESK uzsver, ka vēlme aizsargāt juridisku personu datus (1. panta 2. punkts) būs pretrunā citiem tekstiem, kuros tā nav minēta, jo tajos nav skaidri pateikts, ka tie ir piemērojami arī juridisko personu gadījumā (VDAR, datu apstrāde ES iestādēs).

5.3. EESK apsver, vai patiesais šā priekšlikuma mērķis nav vairāk uzsvērt tā 1. panta 2. punktu, t. i., nodrošināt "elektronisko sakaru datu un elektronisko sakaru pakalpojumu brīvu apriti Savienībā", kas tajā nav nedz ierobežota, nedz aizliegta tādu iemeslu dēļ, kuri saistīti ar fizisku personu privātās dzīves un sakaru neaizskaramību, nevis patiešām nodrošināt to, kas ir paziņots 1. panta 1. punktā, t. i., tiesības "uz privātās dzīves un sakaru neaizskaramību un (..) fizisku personu aizsardzību saistībā ar personas datu apstrādi".

5.4. Visa pamatā ir fiziskās vai juridiskās personas piekrišana. Attiecīgi EESK izpratnē lietotājiem jābūt informētiem, apmācītiem un piesardzīgiem, jo, tiklīdz piekrišana ir sniegta, piegādātājs varēs apstrādāt vairāk satura un metadatu, lai no tiem gūtu pēc iespējas lielāku labumu. Cik daudzi pirms apstiprināšanas zina, ka sīkdatne nodrošina izsekošanu? Ar šo regulu saistītām prioritātēm vajadzētu būt lietotāju izglītošanai par to, kā izmantot savas tiesības, un anonimitātes nodrošināšanai un šifrēšanai.

6. **Īpašas piezīmes**

6.1. Privātie dati būtu jāpārbauda tikai struktūrām, kas pašas ievēro ļoti stingrus nosacījumus un tiecas uz atzītiem un leģitīmiem mērķiem (VDAR).

6.2. Komiteja atkārtoti pauž nožēlu par pārāk daudziem izņēmumiem un ierobežojumiem, kas ietekmē apstiprinātos personas datu aizsardzības tiesību principus ([5]). ES raksturiezīmei arī turpmāk ir jābūt līdzsvaram starp brīvību un drošību, nevis līdzsvaram starp cilvēku pamattiesībām un ražošanu. 29. panta darba grupa, analizējot regulas projektu (WP247, 4.4.2017., atzinums 1/2017), ir asi aizrādījusi, ka ar to tiek pazemināts VDAR noteiktais aizsardzības līmenis, to īpaši attiecinot uz galiekārtas atrašanās vietu, vācamo datu lauka ierobežojumu neesamību (17. punkts), un faktu, ka netiek ieviesta privātās dzīves aizsardzība pēc noklusējuma principa (19. punkts).

6.3. Dati ir kā personas turpinājums, tās "ēnu identitāte", *Shadow-ID*. Dati pieder personai, kas tos pārvalda, taču pēc to apstrādes, tie izslīd no šīs personas ietekmes. Datu saglabāšana un pārsūtīšana: katra valsts paliek atbildīga, un saskaņošana netiek veikta ar tiesību akta projektu noteikto tiesību iespējamo ierobežojumu dēļ. Komiteja uzsver atšķirīgas attieksmes risku, jo tiesību ierobežojumi paliek dalībvalstu ziņā.

6.4. Tomēr ir jāuzdod jautājums īpaši par uzņēmumos strādājošajām personām – kam pieder dati, ko šīs personas ģenerē darbā? Kā tie tiek aizsargāti?

6.5. Kontroles struktūra nav īpaši skaidra ([6]). Neraugoties uz EDAU īstenoto pārraudzību, garantijas pret patvaļību šķiet nepietiekamas, un procedūrām nepieciešamais laiks līdz sankciju piemērošanai nav novērtēts.

6.6. EESK atbalsta Eiropas portāla izveidi, kurā tiktu apkopoti un atjaunināti visi ES un valstu dokumenti, visas tiesības, tiesiskās aizsardzības līdzekļi, tiesu spriedumi un praktiski elementi, lai iedzīvotāji un patērētāji savu tiesību izmantošanas nolūkā varētu orientēties daudzajos dokumentos un īstenošanā. Šā portāla izveidē vajadzētu iedvesmoties no norādēm, kas ietvertas 2016. gada 26. oktobra Direktīvā (ES) 2016/2102 par publiskā sektora struktūru tīmekļvietņu un mobilo lietotņu piekļūstamību un no tās 12., 15. un 21. apsvērumā minētajiem principiem, kā arī no priekšlikuma tā sauktajai direktīvai "Eiropas Pieejamības akts" (2015/0278(COD)) un piedāvāt visiem galalietotājiem pieejamu un saprotamu saturu. EESK varētu piedalīties šā portāla izstrādes posmos.

6.7. Kā EESK jau norādījusi savā atzinumā par Eiropas Elektronisko sakaru kodeksu, 22. pantā nav atsauces uz "kolektīvām prasībām".

([5]) OV C 125, 21.4.2017., 56. lpp., kā arī OV C 110, 9.5.2006., 83. lpp.

([6]) Izskatāmās regulas IV nodaļā ir atsauce uz VIII nodaļas noteikumiem, īpaši uz VDAR 68. pantu.

6.8. Arī materiālās piemērošanas jomas ierobežošana (2. panta 2. punkts), datu apstrādes pilnvaru paplašināšana bez īpašnieka piekrišanas (6. panta 1. un 2. punkts) un maz ticamā iespēja saņemt *visu* attiecīgo lietotāju piekrišanu (6.panta 3. punkta b) apakšpunkts un 8. panta 1., 2. un 3. punkts), tiesību ierobežojumi, ko dalībvalstis var noteikt, ja tās uzskata, ka tie ir "nepieciešami, piemēroti un proporcionāli" pasākumi, ir noteikumi, kuru saturs ir tik plaši interpretējams, ka nonāk pretrunā patiesai privātās dzīves neaizskaramības aizsardzībai. Īpaša uzmanība ir jāpievērš arī ar nepilngadīgām personām saistītu datu aizsardzībai.

6.9. EESK atzinīgi vērtē 12. pantā minētās kontroles tiesības, taču vērš uzmanību uz grūti saprotamo formulējumu, kurā var secināt, ka priekšroka tiek dota "nezināmiem" vai "slēptiem" zvaniem – it kā tiktu ieteikta anonimitāte, lai gan zvaniem pēc principa vajadzētu būt identificētiem.

6.10. Nepasūtītu paziņojumu (16. pants) un tiešās tirgvedības jautājumi jau ir risināti direktīvā par negodīgu komercpraksi ([7]). Sistēmai pēc noklusējuma būtu jādarbojas pēc *opt-in* (pieņemšana), nevis pēc *opt-out* principa (atteikums).

6.11. Komisijas novērtējumu plānots veikt reizi trijos gados, taču digitālajā jomā šāds termiņš ir pārāk ilgs. Pēc diviem novērtējumiem digitālā pasaule jau būs pilnīgi mainījusies. Taču deleģēšanai (25. pants), kas var tikt paplašināta, būtu vajadzīgs noteikts termiņš, ko potenciāli varētu atjaunot.

6.12. Tiesību aktos ir jāsaglabā patērētāju tiesības (LES 3. panta), vienlaikus nodrošinot komercdarbībai nepieciešamo tiesisko stabilitāti. EESK pauž nožēlu par to, ka priekšlikumā nav minēta mašīnas-mašīnas (*M2M*) datu aprite: tā jāmeklē Eiropas Elektronisko sakaru kodeksā (direktīvas priekšlikums, 2. un 4. pants).

6.12.1. Lietu internets (*IoT*) ([8]) padarīs lielos datus (*Big Data*) par "milzīgajiem datiem" ("*Huge Data*") un pēc tam par "visaptverošajiem datiem" ("*All Data*"). Tā ir atslēga turpmākajiem inovāciju viļņiem. Un lielas un mazas mašīnas savā starpā sazinās un pārsūta personas datus savā starpā (jūsu pulkstenis ieraksta jūsu sirdspukstus un nosūta uz jūsu ārsta datoru utt.). Daudzi digitālās jomas dalībnieki ir radījuši paši savu platformu, kas īpaši paredzēta savienotajiem objektiem: *Amazon*, *Microsoft*, *Intel* vai Francijā – *Orange* un *La Poste*.

6.12.2. Ikdienas *IoT* var ātri kļūt par kaitnieciskas darbības cēloni, attālināti iegūstamu personas datu daudzums pieaug (atrašanās vietas noteikšana, ar veselību saistītie dati, video un audio plūsmas). Plaisas personas datu aizsardzībā cita starpā interesē apdrošināšanas uzņēmumus, kuri jau sāk piedāvāt saviem klientiem savienotos objektus un veicināt atbildīgu rīcību.

6.13. Vairāki interneta milži tiecas pārveidot savu sākotnējo lietojumprogrammu par platformu – šajā saistībā ir jānošķir *Facebook* lietojumprogramma no *Facebook* platformas, kas ļauj attīstītājiem izstrādāt no lietotāju profiliem pieejamas lietojumprogrammas. Savukārt *Amazon* bija tīmekļa lietojumprogramma, kas specializējusies tiešsaistes pārdošanā. Pašlaik tā ir kļuvusi par platformu, kas dod iespēju trešām pusēm – lielo grupu dalībniekiem – tirgot savus produktus, izmantojot *Amazon* resursus (reputāciju, loģistiku u. c.). Tas viss notiek, veicot personas datu pārsūtīšanu.

6.14. Sadarbīgā ekonomikā izplatās platformas, kas galvenokārt ar elektroniskiem līdzekļiem nodrošina kontaktus starp vairākiem dalībniekiem, kuri piedāvā preces vai pakalpojumus, no vienas puses, un plašu lietotāju loku, no otras puses ([9]). Lai gan tās ir pieprasītas to aktivitātes un radīto darba iespēju dēļ, EESK vēlas zināt, kā varēs kontrolēt to ģenerēto datu pārsūtīšanu gan piemērojot VDAR, gan šo regulu.

Briselē, 2017. gada 5. jūlijā

Eiropas Ekonomikas un sociālo lietu komitejas priekšsēdētājs
Georges DASSIS

([7]) OV L 149, 11.6.2005., 22. lpp., 8. un 9. pants.
([8]) Atzinums WP247/17 (1.4.2017.) (OV C 12, 15.1.2015., 1. lpp.), 19. punkts.
([9]) OV C 125, 21.4.2017., 56. lpp.