EUROPEAN DATA PROTECTION SUPERVISOR

Atzinums Nr. 4/2015

Virzībā uz jaunu digitālo ētiku —

dati, cieņa un tehnoloģija

2015. gada 11. septembrī

Eiropas Datu aizsardzības uzraudzītājs (EDAU) ir neatkarīga ES iestāde, kas saskaņā ar 41. panta 2. punktu Regulā (EK) Nr. 45/2001 "attiecībā uz personas datu apstrādi ... nodrošina to, ka Kopienas iestādes un struktūras ievēro fizisku personu pamattiesības un brīvības un jo īpaši viņu tiesības uz privāto dzīvi" un ir atbildīga "... par padomu sniegšanu Kopienas iestādēm un struktūrām un datu subjektiem visās lietās, kas attiecas uz personas datu apstrādi". Uzraudzītāju un uzraudzītāja palīgu iecēla amatā 2014. gada decembrī, saņemot konkrētu uzdevumu būt konstruktīvākiem un aktīvākiem. EDAU 2015. gada martā publicēja piecu gadu stratēģiju, kurā izklāstīja, kā viņš plāno šo uzdevumu īstenot, nodrošinot pārskatatbildību.

Šis atzinums izriet no EDAU iepriekšējā Atzinuma par Vispārīgo datu aizsardzības regulu, kura mērķis bija palīdzēt ES galvenajām iestādēm panākt pienācīgu vienprātību par praksē īstenojamu un nākotnē vērstu noteikumu kopumu, kas veicinātu fizisku personu tiesību un brīvību ievērošanu. EDAU šajā atzinumā (tāpat kā 2015. gada sākumā pieņemtajā Atzinumā par mobilo veselību) pievēršas uzdevumam nodrošināt datu digitālu aizsardzību — tas ir trešais EDAU stratēģijas mērķis, proti, "pielāgot pašreizējos datu aizsardzības principus pasaules digitālajai telpai", ņemot vērā arī ES plānus par digitālo vienoto tirgu. Tas atbilst 29. panta darba grupas pieejai attiecībā uz datu aizsardzības aspektiem, kas saistīti ar jauno tehnoloģiju (piemēram, lietiskā interneta) izmantošanu; EDAU tās izstrādē piedalījās kā pilntiesīgs grupas loceklis.

Dignity	Cieņa
Future-oriented rules and enforcement	Nākotnē vērsti noteikumi un izpilde
Accountable controllers	Pārskatatbildīgi datu pārziņi
Empowered individuals	Plašākas iespējas fiziskām personām
Innovative privacy engineering	Inovatīva privātuma inženierija
Ethics	Ētika

“Cilvēka cieņa ir neaizskarama. Tā ir jārespektē un jāaizsargā.”

ES Pamattiesību hartas **1. pants**

Pamattiesībām uz privātumu un personas datu aizsardzību saistībā ar cilvēka cieņas aizsardzību mūsdienās ir daudz lielāka nozīme nekā līdz šim. Šīs tiesības ir nostiprinātas ES līgumos un ES Pamattiesību hartā. Tās sniedz fiziskām personām iespēju izkopt personību, dzīvot neatkarīgu dzīvi, nodoties jaunradei, kā arī izmantot citas tiesības un brīvības. ES hartā noteiktie datu aizsardzības principi, t. i., nepieciešamība, samērīgums, godprātīgums, datu minimizēšana, mērķa ierobežošana, piekrišana un pārredzamība, attiecas uz datu apstrādes procesu kopumā — ne tikai uz datu vākšanu, bet arī uz to izmantošanu.

Tehnoloģijai nav jānosaka, kādas vērtības un tiesības ir jāievēro, tomēr to saikni arī nevajadzētu nonivelēt līdz maldīgai dihotomijai. Digitālā revolūcija varētu nodrošināt ieguvumus veselības aprūpes, vides, starptautiskās attīstības un ekonomikas efektivitātes jomā. ES plānos attiecībā uz digitālo vienoto tirgu par svarīgākajiem konkurētspējas un izaugsmes resursiem ir atzīta mākoņdatošana, lietiskais internets, lielie dati un citi tehnoloģijas risinājumi. Uzņēmējdarbības modeļi apzina jaunas iespējas personas informācijas masveida vākšanai, tūlītējai pārsūtīšanai, kombinēšanai un atkārtotai izmantošanai iepriekš neparedzētiem mērķiem, pamatojot to ar gari izklāstītu un neizprotamu privātuma politiku. Šāda rīcība ir radījusi jaunas problēmas saistībā ar datu aizsardzības principu ievērošanu, tāpēc ir vajadzīgs jauns skatpunkts attiecībā uz to piemērošanu.

Mūsdienu digitālajā vidē nepietiek tikai ar to, ka tiek ievēroti tiesību akti; mums ir jāņem vērā arī datu apstrādes ētiskā dimensija. ES tiesiskajā regulējumā jau ir sniegta iespēja pieņemt elastīgus un individuālus lēmumus un garantijas saistībā ar personas informācijas apstrādi. Tiesiskā regulējuma reforma būs vērtīgs solis uz priekšu. Tomēr pastāv dziļāki jautājumi, kā uz datu iegūšanu vērstas sabiedrības tendences ietekmē cieņu, fizisku personu brīvību un demokrātijas darbību.

Šiem jautājumiem ir inženiertehniski, filozofiski, juridiski un morāli aspekti. Atzinumā ir uzsvērtas vairākas svarīgākās tehnoloģijas tendences, kas var ietvert nepieņemamu personas datu apstrādi vai aizskart cilvēku tiesības uz privātumu. Tajā izklāstīta četru pīlāru veidota “lielo datu aizsardzības ekosistēma”, ar kuras palīdzību iespējams reaģēt uz digitālajām grūtībām. Tie ir kolektīvi centieni, kuru pamatā ir ētiski apsvērumi:

(1) nākotnē vērsta datu apstrādes reglamentēšana un tiesību uz privātumu un datu aizsardzību ievērošana;

(2) pārskatatbildīgi datu pārziņi, kas nosaka personas datu apstrādes procesu;

(3) privātuma ievērošana datu apstrādes produktu un pakalpojumu izstrādē un plānošanā;

(4) plašākas tiesības fiziskām personām.

Eiropas Datu aizsardzības uzraudzītājs vēlas veicināt atklātu, ar informāciju pamatotu diskusiju ES un ārpus tās, iesaistot pilsonisko sabiedrību, izstrādātājus, uzņēmumus, akadēmisko aprindu pārstāvjus, publiskās iestādes un regulatorus. Pie EDAU iestādes tiks izveidota jauna ES datu aizsardzības ētikas padome, kas palīdzēs formulēt jaunus digitālās ētikas principus un tādējādi sniegs iespēju labāk izmantot ieguvumus, ko tehnoloģija nodrošina sabiedrībai un ekonomikai, vienlaikus pastiprinot fizisku personu tiesības un brīvības.

SATURS

1. Dati it visur — tendences, iespējas un izaicinājumi

Arvien lielāku daudzumu personas datu apkopo nepārredzami un komplicētā veidā. Pagājušā gadsimta astoņdesmitajos gados pakāpeniski pieaugot datoru lietojumam uzņēmumos un valsts pārvaldes iestādēs, bija plaši izplatīts uzskats, ka ietekmīgu valdību un korporāciju izmantotā personas datu apstrādes prakse padara indivīdu par vienkāršu datu subjektu un apdraud personu pamattiesības un brīvības. Integrētu informācijas un komunikācijas tehnoloģiju pašreizējās straujās attīstības īpašā iezīme ir šīs tehnoloģijas visuresme un ietekme.

Aizvadītajā gadā tika ziņots, ka uz planētas ir vairāk internetam pieslēdzamu ierīču nekā cilvēku[1]. Procesoru jaudas pieaugums[2], krātuvju un pārraides joslu platuma palielināšanās nozīmē, ka personas datu apstrādi ierobežo arvien mazāk tehnisku šķēršļu. Gaidāms, ka lietiskais internets un lielo datu analīze tiks apvienota ar mākslīgo intelektu, dabiskās valodas apstrādes un biometriskajām sistēmām, lai uzlabotu ar datormācīšanās funkciju aprīkoto lietojumprogrammu spēju attīstīt intelektu. Valdības un uzņēmumi var pāriet no "datizraces" uz "realitātes izraci", kas ielūkojas ikdienas pieredzē, saziņā un pat domāšanā[3]. Sabiedrībai pielāgojoties digitālā tirgus prasībām, ir atjaunoti centieni mācīt programmēšanu maziem bērniem[4]. Šo tendenču izmantošana nozarē, kurā ES ir vadošā patērētāja, tomēr kūtra pakalpojumu sniedzēja, ir tēma, kas ir regulāri minēta Komisijas Digitālā vienotā tirgus stratēģijā[5].

Šīs tendences un daudzi mūsdienās izmantotie jēdzieni, lai gan plaši izplatīti, tomēr ir nekonkrēti un savstarpēji pārklājas. Lai palīdzētu veicināt debates, vēlamies uzsvērt atsevišķas tendences, kas gan neaptver visus aspektus, tomēr, mūsuprāt, izraisa svarīgākos ar datu aizsardzības principu piemērošanu saistītos ētiskos un praktiskos jautājumus.

1.1 Lielie dati

"Lielie dati"[6] attiecas uz milzīga, no dažādiem avotiem iegūtas informācijas apjoma apkopošanu un analizēšanu, kurā tiek izmantoti pašapmācoši algoritmi, lai iegūtu informāciju lēmumu pieņemšanai. Šī informācija ne vienmēr ir personiska. Sensoru ģenerēti dati dabas vai atmosfēras parādību, piemēram, laikapstākļu vai piesārņojuma, pārraudzībai vai ražošanas procesu tehnisko aspektu uzraudzībai nav saistīti ar "identificētu vai identificējamu fizisku personu"[7]. Tomēr viena no lielākajām vērtībām, ko lielie dati sniedz uzņēmumiem un valdībām, ir iespēja uzraudzīt *cilvēku* uzvedību kolektīvā un individuālā līmenī un ir saistīta ar to prognostisko potenciālu[8].

Viens no rezultātiem ir tāda interneta uzņēmumu peļņas modeļa rašanās, kura pamatā ir tiešsaistes aktivitātes izsekošana, lai pakalpojumu sniedzēju interesēs optimizētu darbību ekonomisko vērtību ne tikai saistībā ar mērķorientētu reklāmu, bet arī apdrošināšanas polišu nosacījumiem un likmēm, aizdevumiem un citām līgumattiecībām. Tirgū, ko raksturo konkurence cīņā par lietotāju uzmanību, vairums cilvēku neapzinās šīs izsekošanas plašo mērogu[9]. Šādi "lielie dati" ir jāuzskata par personas datiem pat tad, ja tiem ir piemērotas anonimizēšanas metodes. Kļūst arvien vienkāršāk izsecināt personas identitāti, apvienojot it kā "anonīmus" datus ar citām datu kopām, tostarp publiski pieejamu informāciju, piemēram, sociālajos plašsaziņas līdzekļos[10]. Gadījumos, kad šie dati tiek pārdoti starp valstīm vai jurisdikcijām, atbildība par informācijas apstrādi ir neskaidra un to ir grūti pārbaudīt vai piemērot atbilstīgi datu aizsardzības tiesiskajam regulējumam, jo īpaši, situācijā, kad nav starptautisku standartu.

1.2 Lietiskais internets

Daudzas ar internetu savienotas ierīces, piemēram, viedtālruņi, planšetdatori, kā arī ierīces skaidras naudas izņemšanai un lidojumu reģistrācijai, jau ir plaši izplatītas. Paredzams, ka laikposmā līdz 2020. gadam savienojamība kļūs par standarta iezīmi, internetam pieslēdzamu ierīču skaitam sasniedzot 25 miljardus (salīdzinājumā ar 4,8 miljardiem 2015. gadā) — no telemedicīnas līdz transportlīdzekļiem, no viedajiem skaitītājiem līdz jaunu stacionāro un mobilo iekārtu klāstam viedo pilsētu darbības nodrošināšanai[11].

Šie sensori nodrošinās tūlītēju un sīku informāciju, kurai statistikas biroji un apsekojumu veicēji pašlaik nevar piekļūt, bet kura ne vienmēr ir precīzāka un var būt pat maldinoša[12]. Prognozēts, ka laikposmā līdz 2022. gadam automobiļu starpdatoru savienojumu skaits sasniegs 1,8 miljardus. Tie varētu mazināt negadījumu skaitu un piesārņojumu, palielināt produktivitāti un uzlabot vecāka gada gājuma cilvēku un cilvēku ar invaliditāti autonomiju[13]. Apģērbi un aksesuāri, piemēram, rokas pulksteņi, apstrādās personas informāciju tāpat kā citas ar internetu savienojamas ierīces. Tie spēs konstatēt trombus un pārraudzīt fizisko stāvokli un brūču dzīšanas procesu. Internetam pieslēdzami materiāli varētu aizsargāt pret ekstremāliem vides apstākļiem, piemēram, ugunsdzēsības jomā. Šīs ierīces augšupielādēs personas datus tieši mākoņkrātuvē, kas ir savienota ar sociālajiem tīkliem, un, iespējams, pārraidīs tos publiski, sniedzot iespēju identificēt lietotājus un izsekot indivīdu un grupu rīcību un pārvietošanos[14].

Tas, kā šī informācija tiek apstrādāta, varētu ietekmēt ne tikai ierīču lietotāju privātumu, tostarp, ja ierīces tiek lietotas darbavietā, bet arī tādu citu personu tiesības, kuras tiek novērotas ar ierīces palīdzību un kuru darbības tiek ierakstītas. Lai gan ir maz pierādījumu par faktisku diskrimināciju, tomēr nav šaubu par to, ka lielais personas datu daudzums, ko apkopo lietiskais internets, ir ļoti pievilcīgs instruments peļņas maksimālai palielināšanai, lai noteiktu individualizētas cenas saskaņā ar izsekoto rīcību, jo īpaši veselības aprūpes nozarē[15]. Tiks radīts izaicinājums arī citiem konkrētu jomu noteikumiem, piemēram, saistībā ar ierīcēm, kas apstrādā veselības datus, bet nav tehniski iekļautas medicīnas ierīču kategorijā un neietilpst regulējuma darbības jomā[16].

1.3 Ambientā skaitļošana

Ambientā jeb neredzamā skaitļošana ir svarīga tehnoloģija, kas veido lietiskā interneta pamatu. Viens no tās acīmredzamākajiem lietojuma veidiem ir "viedie mājokļi" un "viedie biroji", kurus veido ierīces ar iebūvētu sarežģītu informācijas apstrādes funkciju, kas piedāvā lielāku energoefektivitāti un informētāku cilvēku spēju attālināti ietekmēt enerģijas patēriņu (lai gan tas būtu atkarīgs no mājokļa iemītnieka neatkarības no namīpašnieka vai ēkas pārvaldnieka). Būs skaidri jānorāda, kurš ir atbildīgs par ambientās skaitļošanas lietojumprogrammu veiktās personas datu apstrādes mērķi un līdzekļiem — ne tikai tāpēc, lai aizsargātu personu pamattiesības, bet arī pienācīgai atbildības noteikšanai par vispārējo sistēmas drošības prasību ievērošanu.

1.4. Mākoņdatošana

Mākoņdatošana ir zināma kā centrālā pamattehnoloģija gan sīki izstrādātas analīzes un izraces iespēju nodrošināšanai, lielo datu vākšanai un analīzei, gan datu plūsmas no lietiskā interneta nodrošināšanai, ko pašlaik izmanto aptuveni piektdaļa ES iedzīvotāju un uzņēmumu[17]. Tā ļauj koncentrēt datus, kas iegūti no virknes lietiskā interneta ierīču, un

pamatojas uz to, ka dati, kas milzīgā apjomā tiek uzglabāti lielās glabāšanas un apstrādes iekārtās visā pasaulē, ir pieejami un savienojami[18]. Tiek prognozēts, ka, privātajam un valsts sektoram plašāk ieviešot mākoņdatošanu[19], ES28 IKP pieaugs kopumā par EUR 449 miljardiem (0,71 % no kopējā ES IKP).

Kontrole pār personas datiem bieži vien tiek dalīta starp klientu un mākoņpakalpojuma sniedzēju, un atbildība par datu aizsardzības pienākuma ievērošanu ne vienmēr ir skaidri noteikta. Tas varētu nozīmēt, ka praksē tiek nodrošināta nepietiekama aizsardzība. Šie pienākumi nav atkarīgi no **datu glabātuves fiziskās atrašanās vietas. Turklāt,** lai gan tā ir tikai bāzes tehnoloģija, kas atbalsta uzņēmējdarbības lietojumprogrammas, pati mākoņdatošanas infrastruktūra var kļūt par kritisku infrastruktūru un palielināt nelīdzsvarotību tirgus ietekmes jomā, ņemot vērā apstākli, ka 30 % uzņēmumu nesen ir ziņojuši par grūtībām anulēt abonementu vai mainīt piegādātājus[20].

1.5. No personas datiem atkarīgi uzņēmējdarbības modeļi

Šīs tehnoloģijas ir ļāvušas rasties jauniem uzņēmējdarbības modeļiem, kuru pamatā ir informācija, kas ir iegūta ne tikai pakalpojumu sniegšanas rezultātā, bet arī no citiem avotiem, piemēram, sociālajiem plašsaziņas līdzekļiem, un tā tiek izmantota, lai novērtētu risku un kredītspēju, kā arī maksimāli palielinātu ieņēmumus. Mūsdienās svarīgu uzņēmējdarbības modeli veido platformas, kas savieno pārdevējus un pircējus, sniedzot iespēju koplietot un pārdalīt produktus, pakalpojumus, prasmes un aktīvus. Šīs platformas bieži tiek dēvētas par "sadarbīgo patēriņu" vai tiešsaistes un mobilajām vienādranga uzņēmējdarbības platformām,[21] un tās var nodrošināt klasisku ekonomisko efektivitāti, radīt tirgos konkurētspēju un mazināt izšķērdēšanu. Tiek lēsts, ka turpmākajos gados to globālā vērtība četrkāršosies, no USD 26 miljardiem pieaugot līdz USD 110 miljardiem[22]. Šādi uz datiem pamatoti uzņēmējdarbības modeļi jau rada milzīgu peļņu automobiļu koplietošanas un mājokļu izīrēšanas, kā arī finanšu tehnoloģiju un sociālo aizdevumu jomā. Apsekojumi liecina, ka patērētāji novērtē to, ka šie modeļi cenu ziņā ir šķietami pieejamāki un ērtāki[23].

Šādu platformu "valūta" parasti ir lietotāju reputācija, salīdzinoši novērtējumi un identitātes pārbaude. Tos, iespējams, var uzskatīt par pārredzamību un pārskatatbildību veicinošiem elementiem, tomēr ne vienmēr saistībā ar pašu platformas nodrošinātāju. Lieli šo tirgu dalībnieki ir kritizēti par to, ka, iespējams, ar reputāciju saistīta informācija netiek sniegta tieši tiem atsevišķajiem lietotājiem, uz kuriem šī informācija attiecas. Pastāv liels risks, ka personām var tikt liegti pakalpojumi, pamatojoties uz reputāciju, ko radījuši nepareizi dati, kurus šīs personas nevar apstrīdēt vai kuru dzēšanu tās nevar pieprasīt. Paļaušanās uz datiem, kas iegūti no daudziem avotiem, arī rada šaubas par ES tiesisko regulējumu attiecībā uz datu apjoma samazināšanu. Ir vērts rūpīgi izvērtēt, kāda būs šo un turpmāko uz tehnoloģijām pamatoto uzņēmējdarbības modeļu radītā ietekme uz personām un sabiedrību nākotnē[24].

1.6. Bezpilota gaisa kuģi (droni) un autonomie transportlīdzekļi

Droni jeb daļēji autonomi gaisa kuģi pašlaik tiek izmantoti galvenokārt militāriem mērķiem, tomēr arvien biežāk to izmantojums ir saistīts ar uzraudzības, kartēšanas, transporta, loģistikas un sabiedrības drošības mērķiem, piemēram, mežu ugunsgrēku ierobežošanai[25]. Fotoattēlus, videomateriālus un citus personas datus, kas ir apkopoti, izmantojot dronus, iespējams nosūtīt, izmantojot telekomunikāciju tīklus. To izmantošana rada nopietnu risku saistībā ar privātās dzīves aizskārumu un negatīvu ietekmi uz vārda brīvību. Rodas jautājums, kā efektīvi reglamentēt to projektēšanu un lietošanu, lai datu subjekti varētu izmantot savas tiesības piekļūt datiem, kas iegūti ar šo mašīnu palīdzību.

Autonomie transportlīdzekļi jeb bezvadītāja automašīnas mainīs individuālās pārvietošanās izmantošanas un organizēšanas veidu uz uz sauszemes, un tie var nonivelēt atšķirību starp privāto un sabiedrisko transportu. Tiek lēsts, ka 2035. gadā lietošanā būs 12 miljoni pilnīgi autonomu un 18 miljoni daļēji autonomu transportlīdzekļu un Eiropa būs viena no šīs tehnoloģijas pirmajām ieviesējām[26]. Algoritmi, kas nodrošinās automašīnu vadīšanu, noteiks lēmumus, kas var tieši attiekties uz personu fizisko veselību un pat dzīvību vai nāvi, piemēram, saistībā ar ieprogrammēto izvēli nenovēršama trieciena gadījumā. Ir acīmredzams, ka ir skaidri jāprecizē, kurš šajā gadījumā ir atbildīgs par datu kontroli un datu drošību, turklāt šie lietojumi rada vairākus ētiskus jautājumus.

1.7. Tendences ar iespējami plašāku ietekmi ilgākā termiņā

Tiek prognozēts, ka drīzumā būs viegli pieejama organisku materiālu **3D biodrukāšana**, kurai izmanto pacienta šūnu kopijas un kolagēna "bio pārsējus" (tas ir, sensitīvus datus saskaņā ar ES tiesisko regulējumu), lai izveidotu secīgas dzīvu šūnu rindas[27]. Tā atvieglotu individuāli pielāgotu cilvēka anatomisko daļu nodrošināšanu un būtu īpaši noderīga nabadzīgākos reģionos un pēckonflikta zonās visā pasaulē. Biodrukāšana nepārprotami izraisa jautājumus par medicīnisko ētiku, intelektuālā īpašuma tiesību aizsardzību un patērētāju aizsardzību, kā arī datu aizsardzības noteikumu piemērošanu, jo tā ir saistīta ar intīmu un sensitīvu datu apstrādi personu veselības kontekstā.

Mākslīgais intelekts, tāpat kā robotika, ir saistīts ar tehnoloģisko pieprasījumu pēc autonomām mašīnām — gan stacionārām, gan mobilām ierīcēm. To attīstība radīs milzīgas iespējas, kas pārsniegs to pašreizējā lietojuma robežas. Padziļinātās apmācības datori sevi apmāca, saspiežot lielas datu kopas un izmantojot (cita starpā) neironu tīklus, kas, domājams, imitē smadzenes. Pētnieku un uzņēmumu mērķis ir pilnveidot nekontrolēto apmācību. Algoritmi jau spēj saprast un tulkot valodas, atpazīt attēlus, rakstīt ziņu rakstus un analizēt medicīniskus datus[28]. Sociālie plašsaziņas līdzekļi sniedz lielu personas datu daudzumu, kuru faktiski ir iepriekš marķējušas pašas personas. Tas varētu būt jaunākais sasniegums cilvēka smadzeņu spējas palielinošu kognitīvo uzlabojumu virknē (kā papīrs, skaitāmie kauliņi, autonomās mašīnas, roboti), bet tagad ir īstais brīdis, lai izsvērtu plašākas sekas iedzīvotāju un sabiedrības dzīvē[29].

2. Lielo datu aizsardzības ekosistēma

ES tagad ir iespēja uzņemties līderību, lai demonstrētu, kā valdības, regulatori, pārziņi, noformētāji, izstrādātāji un fiziskas personas var labāk sadarboties, lai stiprinātu tiesības un virzītu, nevis bloķētu tehnoloģiskās inovācijas. Otrajā sadaļā aprakstītās tendences saskaņā ar kāda komentētāja pausto ir "paplašinājušas plaisu starp to, kas ir iespējams, un to, kas ir likumīgi atļauts"[30]. Pretēji dažiem apgalvojumiem privātums un datu aizsardzība ir platforma, nevis šķērslis ilgtspējīgai un dinamiskai digitālajai videi. Tādas neatkarīgas datu aizsardzības iestādes kā EDAU ir būtiski svarīgas, lai kliedētu šādus mītus un reaģētu uz patiesām personu bažām par kontroles zaudēšanu pār saviem personas datiem[31].

Domājams, ka nākamā personas datu paaudze būs vēl mazāk pieejama personām, uz kurām šie dati attiecas. Atbildība par ilgtspējīga vienotā digitālā tirgus izveidi ir nenovēršami izkliedēta, bet tas, tāpat kā ekosistēma, ir arī savstarpēji atkarīgs, tāpēc ir nepieciešama izstrādātāju, uzņēmumu un regulatoru efektīva sadarbība privātpersonu interesēs. Šajā sadaļā mēs aplūkojam, kādu ieguldījumu var sniegt šīs četras svarīgās puses.

2.1. Nākotnē vērsta reglamentēšana

Mēs nesen mudinājām ES izmanot tās vēsturisko iespēju, lai pieņemtu vienkāršākus noteikumus attiecībā uz tādu personas datu apstrādi, kas būs aktuāli paaudzes laikā[32]. Sarunas par Vispārīgo datu aizsardzības regulu un direktīvu par datu aizsardzību policijas un tieslietu jomā ir sasniegušas noslēguma posmus, un uzmanība drīz tiks pievērsta E-privātuma direktīvas par elektronisko komunikāciju nākotnei un jaunai regulai, ar kuru reglamentē, kā pašas ES iestādes un struktūras apstrādā personas datus. Tā kā datu vākšanas un uzglabāšanas ekonomiskās izmaksas ir visai niecīgas, pienākums nodrošināt šo noteikumu konsekventu ievērošanu būs datu aizsardzības iestādēm, lai novērstu pārmērīgas datu apstrādes radītus "morālos draudus"[33].

Digitālā vienotā tirgus stratēģijā ir atzīta saikne starp lielu datu apjomu kontroli un ietekmi tirgū. Tajā ir pausts atbalsts mūsu 2014. gada sākotnējā atzinumā "Privātums un konkurētspēja lielo datu laikmetā" paustajai pārliecībai par to, ka starp regulatoriem ir jānodrošina lielāka saskaņotība. ES rīcībā jau ir instrumenti nevienlīdzīgā spēku samēra novēršanai digitālajā tirgū. Piemēram, Eiropas Komisijas sāktie pretmonopola procesi ir apliecinājums mobilo ierīču izmantojuma pārsvaram, lai piekļūtu internetam. Saistībā ar spēkā esošo tiesisko regulējumu ir iespējama visaptverošāka īstenošana, piemēram, izmantojot ES koordinācijas mehānismu attiecībā uz uzraudzības iestādēm, lai izvērtētu, vai atsevišķi gadījumi var radīt jautājumus par atbilstību konkurences, patērētāju un datu aizsardzības noteikumiem. Piemēram:

- lielākas pārredzamības pieprasīšana attiecībā uz pakalpojuma cenu (skaidrā naudā vai citādi) var sniegt informāciju un veicināt konkurences lietu analīzi[34], un
- negodīgas cenu diskriminācijas noteikšana, pamatojoties uz sliktu datu kvalitāti, kā arī netaisnīgu profilēšanu un saistībām[35].

Ciešāks dialogs starp dažādu nozaru regulatoriem varētu nodrošināt atbildi uz aizvien aktīvākajiem aicinājumiem izveidot globālas partnerības, kas varētu radīt atklāto datu "masīvu", kurā var plūst un būt pieejami dati un idejas, piemēram, statistika un kartes, un kurā ar tiem iespējams apmainīties sabiedrības interesēs, saskaroties ar mazāku uzraudzības risku, lai sniegtu fiziskām personām lielāku ietekmi attiecībā uz lēmumiem, kas tās ietekmē[36].

2.2. Pārskatatbildīgi datu pārziņi

Lai nodrošinātu pārskatatbildību, ir jāievieš iekšējās politikas programmas un kontroles sistēmas, kas nodrošina atbilstību un sniedz pienācīgus pierādījumus, jo īpaši neatkarīgām uzraudzības iestādēm.

Mēs esam strīdējušies par birokrātijas novēršanu datu aizsardzības tiesību aktos, ierobežojot liekas dokumentācijas prasības un atstājot pēc iespējas plašāku telpu atbildīgai uzņēmumu iniciatīvai, ko ar pamatnostādnēm atbalsta datu aizsardzības iestādes. Princips, ar kuru paredz, ka personas dati ir apstrādājami tikai tādos veidos, kas ir saderīgi ar konkrēto(-iem) nolūku(-iem), kādiem tie tika vākti, ir būtisks, lai respektētu privātpersonu tiesisko paļāvību. Piemēram, rīcības kodeksi, revīzijas, sertifikācija un jaunas līgumu klauzulas un saistoši korporatīvie noteikumi var palīdzēt radīt stabilu uzticēšanos digitālajam tirgum. Pusēm, kas atbildīgas par personas datu apstrādi, jābūt daudz dinamiskākām un aktīvākām un jāatsakās no tā dēvētās "melnās kastes" slepenības tendences un uzņēmējdarbības prakses nepārredzamības, vienlaikus pieprasot arvien lielāku klientu pārredzamību[37].

2.3. Privātumu respektējoša inženierija

Cilvēces panāktā inovācija vienmēr ir bijusi konkrētu sociālo grupu darbību un īpašu situāciju produkts, parasti atspoguļojot attiecīgā laikmeta normas[38]. Tomēr atr tehniskās projektēšanas lēmumiem nav jādiktē sabiedrības saskarsmes veidi un mūsu kopienu struktūra, bet gan jāsniedz atbalsts mūsu vērtībām un pamattiesībām.

ES ir jāizstrādā un jāatbalsta inženierijas paņēmieni un metodikas, kas sniedz iespēju ieviest tādas datu apstrādes tehnoloģijas, kuru darbā tiek pilnīgi ievērota fiziskās personas cieņa un tiesības. Sistēmām un programmatūras izstrādātājiem ir jāizprot un jaunajos produktos un pakalpojumos labāk jāizmanto integrētas privātuma aizsardzības principi visos izstrādes posmos un tehnoloģijās. Pārskatatbildība ir jāatbalsta ar plašāku pētniecību un izstrādi metožu un rīku jomā, lai nodrošinātu precīzas revīzijas un noteiktu datu pārziņu un apstrādātāju atbilstību noteikumiem, piemēram, atzīmējot katru personas datu vienību ar metadatiem, kas atbilst datu aizsardzības prasībām.

Ar inženiertehniskajiem risinājumiem ir jāstiprina to fizisko personu tiesības, kuras ar anonimitātes starpniecību vēlas saglabāt savu privātumu un brīvību. ES ir jāatbalsta tādu algoritmu izstrāde un ieviešana, kas slēpj identitāti un apkopo datus, lai aizsargātu privātpersonu, un vienlaikus jāizmanto datu sniegtās prognozēšanas iespējas[39].

Mums šodien ir jāliek pamati šo uzdevumu izpildei, apvienojot izstrādātājus un dažādu jomu datu aizsardzības ekspertus plašos tīklos, piemēram, Interneta privātuma inženierijas tīklā (*IPEN*), kas veicina starpnozaru ideju un pieeju apmaiņu.

2.4. Plašākas iespējas fiziskām personām

Ražojoša patērētāja vide

Fiziskas personas nav tikai pasīvi objekti, kam ir vajadzīga likuma aizsardzība pret ļaunprātīgu izmantošanu. Iepriekš raksturotās digitālās tendences sniedz atzinīgi vērtējamas iespējas fiziskās personas ietekmes stiprināšanai. Piemēram, cilvēki mūsdienās gan rada, gan patērē saturu un pakalpojumus, un arvien biežāk var uzskatīt, ka viņi kopā ar pakalpojumu sniedzējiem ir atbildīgi par personas datu apstrādi, izņemot gadījumus, kad tā tiek veikta tikai "mājsaimniecības" nolūkos[40] (lai raksturotu šo norisi, ir radies jēdziens "ražojošs patērētājs"[41]). Tomēr virtuālā valūta sniedz lietotājiem anonimitāti un iespēju apiet trešās puses veiktu darījumu pārbaudi un tādējādi pazemina darījumu izmaksas, kad tiek veikta preču un pakalpojumu pārrobežu samaksa. No otras puses, šo virtuālo valūtu anonimitāte un pārrobežu jurisdikcija (vai, iespējams, to varētu apzīmēt kā *jurisdikcijas trūkums*) pakļauj fiziskas personas krāpniecības un kriminālu tirgu radītajam riskam, ko ir grūti atklāt un izmeklēt. Regulatoriem, uzņēmumiem un inženieriem ir jāveic savi pienākumi, tomēr arī iedzīvotājiem ir jābūt pienākumam būt zinošiem, uzmanīgiem, kritiskiem un informētiem, pieņemot lēmumus gan tiešsaistē, gan bezsaistē[42].

Piekrišana

Turklāt atšķirībā no tradicionālajiem pieņēmumiem ne visu cilvēku uzvedību iespējams skaidrot ar ekonomiskiem principiem, kas paredz, ka visi cilvēki ir pilnīgi racionāli un reaģē uz ekonomiskiem stimuliem[43]. Tas ir svarīgi, ņemot vērā nozīmi, kāda turpmāk būs fiziskas personas sniegtajai piekrišanai par tās personas datu apstrādi. Saskaņā ar ES tiesisko regulējumu vairumā apstrādes gadījumu piekrišana nav vienīgais likumīgais apstrādes pamatojums. Pat gadījumos, kad piekrišanai ir svarīga nozīme, tā neatbrīvo datu pārziņus no

atbildības par to, ko tie dara ar datiem, jo īpaši tad, ja ir iegūta vispārīga piekrišana apstrādei vairākos nolūkos.

Kontrole un datu "īpašumtiesības"

Fiziskām personām ir jābūt iespējai apstrīdēt kļūdas un netaisnīgu neobjektivitāti, kas izriet no algoritmu izmantotās loģikas, lai noteiktu pieņēmumus un prognozes. Piemēram, ASV veiktā pētījumā, kurā tika aplūkoti gandrīz 3000 ziņojumu par kredītiem, kas pieder 1000 patērētāju, tika konstatēts, ka 26 % gadījumu bija pieļautas "būtiskas" kļūdas — problēmas, kas ir pietiekami nopietnas, lai ietekmētu patērētāju kredītvērtējumu un tādējādi kredīta saņemšanas izmaksas[44].

Datus bieži vien uzskata par resursu (piemēram, kā naftu), kuru iespējams pārdot — ideālā gadījumā slēdzot darījumu starp vienlīdz labi informētām darījuma pusēm[45]. Patērētājiem netiek sniegta taisnīga atlīdzība par viņu datiem, kas tiek pārdoti, un dažas puses ir paudušas atbalstu datu īpašumtiesību modelim. Tomēr ir grūti garantēt pilnīgu kontroli pār personas datiem — to ietekmēs citi jautājumi, piemēram, sabiedrības intereses un citu personu tiesības un brīvības. Kontrole ir vajadzīga, bet tā nav pietiekama[46]. Tomēr cilvēka cieņa ir vienmēr nemainīga vērtība, un saskaņā ar ES tiesisko regulējumu īpašumtiesību analoģiju nav iespējams piemērot attiecībā uz personas datiem, kas ir cieši saistīti ar individuālām personībām. ES datu aizsardzības tiesiskajā regulējumā nav noteikumu, kas paredzētu, ka fiziskai personai jāatsakās no savām pamattiesībām.

Viena alternatīva metode, lai piešķirtu fiziskām personām efektīvāku kontroli pār to datiem un to, kurš un kādos nolūkos tiem var piekļūt, varētu būt personas datu glabātuvju jeb datu seifu izmantošana[47]. Šāda personīgās glabātuves koncepcija ietver vajadzību pēc drošības mehānismiem, kas nodrošina, ka datiem var piekļūt tikai datu subjekta pilnvarotas struktūras un ka minētās struktūras var piekļūt tikai tām datu daļām, uz kurām attiecas šis pilnvarojums. Personīgās datu glabātuves būtu visefektīvākais risinājums gadījumos, kad tās būtu saistītas ar aktuālu un pastāvīgi atjauninātu informāciju, piemēram, ģeotelpisku informāciju vai dzīvības pazīmēm. Papildus tehniskām garantijām datu lietotājiem būtu pienākums ievērot noteikumus par datu koplietošanu un izmantošanu. Konkurence un iespēja mainīt izmantoto pakalpojumu sniedzēju ir efektīvākais patērētāja rīcībā esošais instruments, ar kura palīdzību tas var ietekmēt patērētājiem pieejamo pakalpojumu tirgu. Savienojumu, tostarp identifikatoru un kontaktinformācijas pārnesamība, ir izrādījusies efektīvs konkurences veicinātājs, un telekomunikāciju tirgus liberalizācijas laikā tā efektīvi samazināja patēriņa cenas. Datu pārnesamība, kas ir faktiskā un praktiskā iespēja pārnest personas datus no viena pakalpojumu sniedzēja pie cita pakalpojumu sniedzēja, ir efektīvs izejas punkts patiesas izvēles apstākļu nodrošināšanai patērētājiem.

3. Jaunās digitālās ētikas centrā — cieņa

Šīs digitālās ekosistēmas elementu pamatā ir jābūt ētiskiem aspektiem. EDAU uzskata, ka efektīvāka cilvēka cieņas ievērošana un aizsardzība varētu būt labāks pretsvars plaši izplatītajai uzraudzībai un spēka asimetrijai, ar ko pašlaik saskaras fiziskās personas. Tai ir jābūt jaunās digitālās ētikas centrā.

3.1. Cieņa un dati

Pēc rūpnieciskās revolūcijas 18. un 19. gadsimtā cilvēktiesību kustība centās nodrošināt plašāku sabiedrisko labumu, mazinot šķēršļus cieņai pret personu. ES, pateicoties

Pamattiesību hartai, kā arī pēc Vispārējās cilvēktiesību deklarācijas un Eiropas Cilvēktiesību konvencijas pieņemšanas par savu izejas punktu ir pieņēmusi cilvēka cieņas neaizskaramību. Cilvēka cieņa pati par sevi ir ne tikai daļa no pamattiesībām, bet arī pamats pārējām brīvībām un tiesībām, tostarp tiesībām uz privātumu un personas datu aizsardzību[48]. Cieņas aizskārumi var ietvert "lietiskošanu" — situācijas, kad persona tiek uzskatīta par instrumentu, kas kalpo kāda cita interesēm[49]. Privātums ir neatņemama cilvēka cieņas daļa, un tiesības uz datu aizsardzību sākotnēji tika formulētas 20. gadsimta septiņdesmitajos un astoņdesmitajos gados kā veids, kādā kompensēt plaša mēroga personas datu apstrādes izraisīto situācijas pasliktināšanos privātuma un cieņas jomā. Vācijā tiesības uz informācijas privātumu tika pamatotas ar tiesībām uz personas cieņu un brīvu personības attīstību, kas noteiktas Vācijas Konstitūcijas 1. un 2. pantā[50].

Tomēr 21. gadsimta sākumā fiziskām personām internetā tiek prasīts atklāt arvien vairāk personas datu, lai tās varētu piedalīties sociālajās, administratīvajās un komerciālajās aktivitātēs, un aizvien vairāk ierobežotas iespējas no šīs prasības atteikties. Tā kā visa darbība potenciāli tiek veikta tiešsaistē, brīvas un apzinātas piekrišanas jēdziens tiek pakļauts arvien lielākam spiedienam. "Digitālās drupatas" tiek radītas ik brīdi, un tās tiek apvienotas, lai klasificētu fiziskās personas reālajā laikā un radītu vairākus un dažkārt pretrunīgus profilus. Šos profilus iespējams izplatīt mikrosekundēs, fiziskajai personai par to nezinot, un izmantot kā pamatu svarīgu lēmumu pieņemšanā, kas skar minētās personas.

Pastāv risks, ka profili, kas tiek izmantoti cilvēku rīcības prognozēšanai, rada stigmatizāciju, stiprina pastāvošos stereotipus, sociālo un kulturālo nošķiršanu un izslēgšanu[51], šādai "kolektīvai inteliģencei" iznīcinot individuālo izvēli un līdzvērtīgas iespējas. Šādi "filtra burbuļi" un "personīgās atbalss kameras" galu galā varētu apturēt radošumu, inovācijas, kā arī vārda un biedrošanās brīvību, kas ir veicinājušas digitālo tehnoloģiju uzplaukumu.

Vienlaikus, pamatojoties uz "drošību", pastāvīgi tiek piemērota izņēmuma pieeja, lai attaisnotu daudzās iejaukšanās metodes, ko izmanto fizisku personu darbības uzraudzībai[52]. Lai izprastu šo "uzraudzības sprūdratu", ir vajadzīga ilgākā termiņa perspektīvas piemērošana vispārējai ietekmei uz sabiedrību un rīcību.

ES kopā ar trešām valstīm ir rūpīgi jāizvērtē, kā nodrošināt, ka šīs vērtības netiek ievērotas tikai "uz papīra", kibertelpā tās faktiski neitralizējot. Tagadpirms šo tehnoloģiju masveida pieņemšanas ES ir būtiska iespēja iebūvēt vērtības digitālajās struktūrās, kas definēs mūsu sabiedrību[53]. Lai to paveiktu, ir jāveic jauns novērtējums par to, vai jauno tehnoloģiju sniegtie iespējamie ieguvumi patiešām ir atkarīgi no miljardiem fizisku personu personiski identificējamu datu vākšanas un analīzes. Šāds novērtējums varētu mudināt izstrādātājus radīt produktus, kas reālajā laikā depersonalizē milzīgus neorganizētas informācijas apjomus, apgrūtinot vai padarot par neiespējamu atsevišķas fiziskās personas izcelšanu.

Mēs jau atzīstam, ka atsevišķu datu, piemēram, ģenētiskās informācijas, apstrāde ir ne tikai jāreglamentē, bet arī jāizvērtē, piemēram, ētikas komisijām, ņemot vērā plašākas sabiedrības bažas. Ģenētiskie dati pēc savas būtības ir saistīti ne tikai ar vienu fizisku personu, bet arī ar to priekštečiem un pēcnācējiem. Šādi dati izmantojami ne tikai ģimenes radniecības saišu noteikšanai, bet vienas fiziskas personas gēnos atrastie elementi var sniegt informāciju arī par šīs personas vecākiem un bērniem, un no tās var izrietēt datu pārziņu lēmumi, kas ietekmē bērnu izredzes dzīvē pat pirms viņu piedzimšanas. Personas ģenētisko datu iespējamā koncentrācija dažu milzīgu tirgus dalībnieku rokās ietekmē gan tirgus ekonomiku, gan datu subjektus. Pieaugoša atkarība no pastāvīgas datu plūsmas globāla mēroga vākšanas un

analīzes sistēmas varētu palielināt sabiedrības un ekonomikas neaizsargātību pret nepieredzētiem trūkumiem drošības jomā un ļaunprātīgiem uzbrukumiem.

Ja nedomāsim par nākotni inovatīvi, pašreizējā sistēma varētu ciest neveiksmi. Pastiprinās prasības un vajadzība uzskatīt datu subjektus par fizisku personu, nevis vienkārši patērētāju vai lietotāju. Patiesi neatkarīgām datu aizsardzības iestādēm ir būtiska nozīme tādas nākotnes novēršanā, kurā fizisku personu dzīvi nosaka algoritmi un to nebeidzamās variācijas. Šīm iestādēm ir jāspēj īstenot rūpības pienākumu attiecībā uz fiziskām personām un to cieņu tiešsaistē. Tradicionālie privātuma un datu aizsardzības jēdzieni un principi jau ietvēra ētiskas nianses cieņas aizsardzībai, piemēram, saistībā ar nodarbinātību un veselību. Tomēr mūsdienās vērojamās tendences ir sākušas pavisam jaunu vēstures periodu, un ir jāpārbauda, vai principi ir pietiekami stingri digitālajam laikmetam[54]. Domājams, ka pati izpratne par personas datiem radikāli mainīsies, jo tehnoloģijas sniedz arvien lielākas iespējas atkārtoti identificēt fiziskās personas, pamatojoties uz šķietami anonīmiem datiem. Turklāt mašīnmācīšanās, kā arī cilvēku un mākslīgā intelekta apvienošana vājinās fiziskas personas tiesību un atbildības koncepcijas.

3.2. Eiropas Ētikas konsultatīvā padome

Mēs necenšamies radīt trauksmi veicinošu distopisku ainu. Tiesību, politikas, ekonomikas, sociālajā, zinātniskajā un pat reliģiskajā kontekstā jau norit diskusijas[55]. Domājams, ka pārmērīgi vienkāršotas pieejas, kas uz drošības rēķina sniedz vienpusējas priekšrocības ekonomiskajai peļņai vai uzraudzībai, ir tikpat nelietderīgas kā pārmērīgi ierobežojoša pašreizējā tiesiskā regulējuma piemērošana, kas kavē inovācijas un progresu. Tāpēc EDAU ierosina padziļinātu, plašu un starpnozaru analīzi, lai sniegtu ieteikumus un informāciju sabiedrības diskusijām, kā brīvai un demokrātiskai sabiedrībai jārisina tehnoloģiju radītās problēmas.

EDAU stratēģijā [56] tika pausta apņēmība izstrādāt ētisku pieeju datu aizsardzībai. Ar to tika atzīts, ka "īstenojamība, lietderība vai rentabilitāte automātiski nenozīmē ilgtspējību", un uzsvērts, ka "pārskatatbildība ir svarīgāka par mehānisku likuma burta ievērošanu". Mēs plānojam uzrunāt ES ierēdņu aprindas, juristus un IT speciālistus, ievērojamas personas, kuras spēj spriest par tehnoloģisko pārmaiņu radīto ietekmi vidējā un ilgā termiņā un regulatīviem risinājumiem. Turpmākajos mēnešos mēs savā neatkarīgajā iestādē izveidosim ārēju konsultatīvu grupu datu aizsardzības ētisko jautājumu jomā, lai pētītu attiecības starp cilvēktiesībām, 21. gadsimta tehnoloģijām, tirgiem un uzņēmējdarbības modeļiem.

Mūsu Ētikas konsultatīvo padomi veidos izcilu personu grupa, kas pārstāv ētikas un filozofijas, socioloģijas, psiholoģijas, tehnoloģijas un ekonomikas nozares. Tās darbu vajadzības gadījumā atbalstīs papildu eksperti ar zināšanām tādās jomās kā veselības aprūpe, transports un enerģētika, sociālā saskarsme un plašsaziņas līdzekļi, ekonomika un finanses, pārvaldība un demokrātija, kā arī drošība un policijas darbs. Šie eksperti tiks aicināt analizēt plašāka mēroga ētiskās sekas, kas izriet no tā, kā tiek uztverti un izmantoti personas dati. Viņu apsvērumi būs maksimāli pārredzami.

4. Secinājums — pienācis laiks padziļinātām diskusijām

Privātums un datu aizsardzība ir risinājuma daļa, nevis problēma. Patlaban tehnoloģiju kontrolē cilvēki. Tās potenciālo attīstību ir grūti klasificēt kā labu vai sliktu, vēlamu vai kaitīgu, izdevīgu vai neizdevīgu, un situāciju vēl vairāk sarežģī tas, ka vairākas potenciālās tendences ir jāizvērtē plašākā kontekstā. Politikas veidotājiem, tehnoloģijas izstrādātājiem,

uzņēmējiem un visai sabiedrībai ir nopietni jāapsver, vai un kā mēs vēlamies ietekmēt tehnoloģijas attīstību un izmantošanu. Tomēr vienlīdz svarīgi ir panākt, ka ES neatliekami ņem vērā ētikas un cilvēka cieņas aspektu nozīmi saistībā ar nākotnes tehnoloģijām.

Pieredze liecina, ka datu aizsardzības principi var aizsargāt fiziskas personas un to privātumu pret bezatbildīgas datu apstrādes riskiem. Tomēr uz mūsdienu tendencēm, iespējams, jāreaģē, izmantojot pilnīgi jaunu pieeju. Tāpēc mēs sākam jaunas debates par to, ciktāl tādu principu kā godprātība un likumība piemērošana ir pietiekama. Datu aizsardzības kopiena var uzņemties jaunas funkcijas, izmantojot jau pieejamos instrumentus, piemēram, iepriekšējas pārbaudes un atļaujas, jo citām struktūrām nav līdzekļu, ar ko rūpīgi pārbaudīt šādu datu apstrādi. Laikā, kad tehnoloģija, vispasaules inovācija un cilvēku savienotība attīstās galvu reibinošā ātrumā, mums ir iespēja piesaistīt uzmanību, raisīt interesi un panākt vienprātību.

Mēs ceram, ka šis atzinums kļūs par pamatu plašākai un padziļinātai diskusijai, kā ES var izmantot jauno tehnoloģiju sniegtos ieguvumus un vienlaikus nodrošināt savu vērtību neaizskaramību.

Briselē, 2015. gada 11. septembrī

(**paraksts**)

Giovanni BUTTARELLI
Eiropas datu aizsardzības uzraudzītājs

Piezīmes

[1] Avots: *GSMA Intelligence*.

[2] Ir pierādīts, ka Mūra likums par tranzistoru skaitu, ko iespējams ievietot mikroshēmā un kas dubultojas aptuveni 18 mēnešu laikā, kopumā ir pareizs; *Moore, Gordon E.* (19.04.1965.). "Cramming more components onto integrated circuits", *Electronics*. 22.08.2011.

[3] Nathan Eagle, Alex (Sandy) Pentland, "Reality mining: sensing complex social systems", *Journal Personal and Ubiquitous Computing*, 10. sējums, 4. numurs, 2006. gada marts, 255.–268. lpp. *Shoshana Zuboff* rakstā "Big Other: surveillance capitalism and the prospects of an information civilization", kas publicēts *Journal of Information Technology* (2015. gads) 30. sēj., 75.–89. lpp., raksta: "Vispārējas datoru izmantošanas rezultātā pasaule tiek skaidrota jaunā simboliskā dimensijā, jo notikumi, objekti, procesi un cilvēki kļūst redzami, izzināmi un kopīgojami jaunā veidā." *S. Zuboff* paredz "jaunas universālas arhitektūras rašanos", ko viņa dēvē par "Lielo citu" (*Big other*). Tas būs "visuresošs tīklā savienotu iestāžu režīms, kas reģistrē, modificē un komodificē ikdienas pieredzi — no tosteriem līdz ķermeņiem, no saziņas līdz domai, lai izveidotu jaunus ceļus uz monetizāciju un peļņu"; 77., 81. lpp.

[4] "BBC Micro Bit computer's final design revealed" 07.07.2015., http://www.bbc.com/news/technology-33409311(skatīts 10.09.2015.); "No assembler required: How to teach computer science in nursery school", *The Economist*, 01.08.2015.

[5] Saskaņā ar *PWC* sniegto Pasaules desmit vadošo uzņēmumu sarakstu (vērtējot pēc tirgus kapitalizācijas) (2015. gada 31. marta atjauninājums) neviens no tehnoloģiju nozares desmit vadošajiem uzņēmumiem (vērtējot pēc tirgus kapitalizācijas) neatrodas ES (astoņi ir ASV reģistrēti uzņēmumi, viens Taivānā un viens Ķīnā).

[6] "Lielie dati ir saistīti ar eksponenciālo pieaugumu gan attiecībā uz informācijas pieejamību, gan tās automatizētu izmantošanu. Lielie dati ir korporāciju, valdību un citu lielu organizāciju rīcībā esošas gigantiskas digitālo datu kopas, kas tiek plaši analizētas (tādēļ tās sauc par "analītiskām"), izmantojot datora algoritmus"; 29. panta darba grupas atzinums Nr. 3/2013 par mērķa ierobežojumu. Baltā nama 2014. gada ziņojumā lielie dati ir raksturoti kā "augoša tehnoloģiskā spēja tvert, apkopot un apstrādāt arvien lielāku datu apjomu, ātrumu un veidus", skatīt "Big Data: Seizing Opportunities, Preserving Values", prezidenta izpildbirojs ("Podesta-report"), 2014. gada maijs.

[7] Saskaņā ar ES tiesisko regulējumu "personas dati" ir "jebkura informācija attiecībā uz identificētu vai identificējamu fizisku personu ("datu subjektu"); identificējama persona ir tā, kuru var identificēt tieši vai netieši, norādot reģistrācijas numuru vai vienu vai vairākus šai personai raksturīgus fiziskās, fizioloģiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktorus"; Direktīvas 95/46/EK 2. panta a) punkts. Šī definīcija ir lielā mērā salīdzināma ar Eiropas Padomes Konvencijā par indivīda aizsardzību attiecībā uz personas datu automātisko apstrādi (zināma kā konvencija Nr. 108) un ESAO Pamatnostādnēs par privātās dzīves aizsardzību un personas datu pārrobežu plūsmu pieņemtajām definīcijām. Lai iepazītos ar padziļinātu analīzi, skatīt 29. panta darba grupas Atzinumu Nr. 4/2007 par personas datu jēdzienu, WP136.

[8] Skatīt, piemēram, Amerikas Savienoto Valstu Federālās tirdzniecības komisijas priekšsēdētājas runu 2014. gadā "Internetam pieslēdzamu ierīču izplatība, informācijas vākšanas, uzglabāšanas un apstrādes izmaksu pazemināšanās un informācijas brokeru, kā arī citu pušu spēja apvienot bezsaistes un tiešsaistes datus nozīmē, ka uzņēmumi var uzkrāt burtiski neierobežotu patērētāju informācijas daudzumu un uzglabāt to nenoteiktu laiku. Izmantojot prognostisko analīzi, viņi par ikvienu no mums var uzzināt pārsteidzoši daudz"; Federālās tirdzniecības komisijas priekšsēdētājas *Edith Ramirez* atklāšanas runa, "Big Data: A Tool for Inclusion or Exclusion?", Vašingtona, 2014. gada 15. septembris. Saskaņā ar *Sandy Pentland* pausto "sociālā fizika ir kvantitatīva sociālā zinātne, kas aplūko uzticamas, matemātiskas saiknes starp informāciju un ideju plūsmu, no vienas puses, un cilvēku uzvedību, no otras puses (..) Tā mums sniedz iespēju izteikt prognozes par nelielu grupu,

uzņēmumu departamentu vai pat veselu pilsētu produktivitāti". Tas "ir vajadzīgs, lai veidotu labākas sociālās sistēmas" (4., 7. lpp.) un "sniegtu iespēju (valdību ierēdņiem, nozaru uzņēmumu vadītājiem un iedzīvotājiem) izmantot sociālo tīklu stimulu rīkus, lai *radītu jaunas uzvedības normas*" (189. lpp.) (mūsu slīpinājums); Pentland, "Social Physics: How Good Ideas Spread: The Lessons from a New Science".

[9] Speciālais Eirobarometrs 431 par datu aizsardzību, 2015. gada jūnijs, un Pjū Pētniecības centra 2014. gada janvārī veiktais apsekojums par sabiedrības attieksmi pret privātumu un drošību "laikmetā pēc Snoudena". Saskaņā ar vienu pētījumu vidēja atsevišķas tīmekļa vietnes apmeklējuma rezultātā dati tiek vākti 56 reizes, kā norādījusi *Julia Angwin* savā darbā "Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance", 2012. gads. Baltā nama 2014. gada ziņojumā par lielajiem datiem ir apgalvots, ka "nepieredzētā skaitļošanas jauda un augstais attīstības līmenis (..) rada varas asimetriju starp tiem, kuri iegūst datus, un tiem, kuri bez nodoma un nejauši tos sniedz"; "dažas no šā pārskata sagatavošanas laikā atklātajām dziļākajām problēmām ir saistītas ar to, kā lielo datu analīze var (..) radīt tik neskaidru lēmumu pieņemšanas vidi, ka neizprotamu algoritmu kopā tiek zaudēta individuālā autonomija".

[10] Izmantojot 1990. gada tautas skaitīšanas publiski pieejamos anonīmos datus, 87 % ASV iedzīvotāju varētu tikt identificēti, izmantojot viņu piecciparu pasta indeksu kopā ar informāciju par dzimumu un dzimšanas datumu; skatīt *Paul Ohm* "Broken promises of privacy: responding to the surprising failure of anonymisation", *UCLA Law Review*, 2010. gads, kā arī "Record linkage and privacy: issues in creating new federal research and statistical info", 2011. gada aprīlis. DNS ir unikāla (izņemot identisko dvīņu gadījumā) un stabila visā dzīves laikā. Tā ietver informāciju par etnisko izcelsmi un noslieci uz saslimšanām, un, izmantojot DNS, iespējams identificēt pārējos ģimenes locekļus. Pētnieki, izmantojot anonīmus DNS datus, kas pieejami publiski pieejamās ģenealoģijas datubāzēs, 2013. gada janvārī spēja identificēt indivīdus un ģimenes; *Gymrek, M., McGuire, A. L., Golan, D., Halperin, E. & Erlich, Y. Science* 339. sēj., 321.–324. lpp., 2013. gads. Skatīt arī "Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts", 23.06.2014. http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/ (skatīts 10.09.2015.). Skatīt arī 29. panta darba grupas atzinumu Nr. 4/2007 par personas datu jēdzienu, 29. panta darba grupas atzinumu Nr. 3/2013 par mērķa ierobežojumu, 29. panta darba grupas atzinumu Nr. 6/2013 par atklātajiem datiem un PSI atkārtotu izmantošanu un 29. panta darba grupas atzinumu Nr. 5/2014 par anonimizāciju.

[11] Avots: *Gartner*.

[12] Skatīt, piemēram, paneļdiskusiju "Kāda ir oficiālās statistikas nākotne lielo datu laikmetā?" *the Royal Statistical Society*, Londona, 2015. gada 19. janvāris; http://www.odi.org/events/4068-future-official-statistics-big-data-era (piekļūts 10.09.2015).

[13] Desmit tehnoloģijas, kas varētu mainīt mūsu dzīvi: iespējamās sekas un ietekme uz politiku, Zinātnisko prognožu nodaļa, Eiropas Parlamenta Izpētes dienests, 2015. gada janvāris.

[14] ES pamatprogrammas "Apvārsnis 2020" darba programma 2016.–2017. gadam atbalsta šīs norises, tostarp liela mēroga izmēģinājuma projektus, kuros tiks aplūkotas ar privātumu un ētiku saistītās bažas.

[15] Apdrošināšana ir raksturota kā "lietiskajam internetam raksturīgais uzņēmējdarbības modelis"; "From fitness trackers to drones, how the 'Internet of Things' is transforming the insurance industry", *Business Insider*, 11.06.2015. Konkurences tiesībās cenu diskriminācijas jēdziens, kas ir atvasināts no LESD 102. panta, kurā uzņēmumam, kam ir dominējošs stāvoklis tirgū, ir aizliegtas tādas darbības kā "tieši vai netieši uzspiestas netaisnīgas iepirkuma vai pārdošanas cenas vai citi netaisnīgi tirdzniecības nosacījumi", ir ļoti strīdīgs, skatīt, piemēram, *Damien Gerardin* un *Nicolas Petit* "Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles" (2005. gada jūlijs), *Global Competition Law Centre Working Paper Series* Nr. 07/05. Saistībā ar lielajiem datiem un to (saskaņā ar vēl nepublicētu autoru viedokli) potenciālu veicināt individualizētu cenu noteikšanu skatīt Amerikas Savienoto Valstu prezidenta izpildbiroja sagatavoto

dokumentu "Big Data and Differential Pricing" (Lielie dati un diferencētas cenas), 2015. gada februāris, un nesen veikto analīzi, kurā secināts, ka individualizēta cenu noteikšana parasti ietver personas datu apstrādi un tāpēc saistībā ar to ir jāievēro datu aizsardzības tiesiskajā regulējumā paredzētais pārredzamības princips, kas paredz, ka uzņēmumiem ir pienākums informēt iedzīvotājus par to personas datu apstrādes mērķi, proti, ja uzņēmumi nosaka individualizētas cenas, viņiem par to ir jāpaziņo. Un, ja uzņēmums izmantot sīkdatni, lai kādu atpazītu, E-privātuma direktīvā noteikts, ka tam ir jāinformē persona par sīkdatnes mērķi; *Frederik Borgesius* darba projekts "Online Price Discrimination and Data Protection Law". Pieejams http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (skatīts 10.09.2015).

[16] ES tiesību aktos medicīnas ierīces ir definētas Padomes Direktīvā 93/42/EEK par medicīnas ierīcēm, kas ir grozīta ar Eiropas Parlamenta un Padomes 2007. gada 5. septembra Direktīvu 2007/47/EK. Saistībā ar "mobilās veselības" ietekmi uz datu aizsardzību skatīt EDAU atzinumu Nr. 1/20015.

[17] Saskaņā ar *Eurostat* datiem 21 % iedzīvotāju un 19 % uzņēmumu ES izmanto mākoņkrātuvju pakalpojumus.

[18] "Ja pasaules internets būtu valsts, tas būtu divpadsmitais lielākais elektrības patērētājs pasaule, ierindojoties aptuveni starp Spāniju un Itāliju. Tas rada aptuveni no 1,1 līdz 1,5 % no globālā elektroenerģijas patēriņa (2010. gadā) un tādu siltumnīcefekta gāzu apjomu, ko gadā rada no 70 līdz 90 lielas (500 megavatu) ogļu elektrostacijas." Dabas resursu aizsardzības padome, Datu centra efektivitātes novērtējums: energoefektivitātes palielināšana datu centru nozarē: galveno stimulu un šķēršļu novērtējums, 2014. gads

[19] Pārskats par pētījumu "SMART 2013/0043 — mākoņpakalpojumu ieviešana Eiropā".

[20] Avots: *Eurostat*.

[21] Termins "sadarbīgais patēriņš" ir kritizēts kā maldinošs: "The Sharing Economy Isn't About Sharing at All", Giana M. Eckhardt and Fleura Bardhi, *Harvard Business Review*, 28.01.2015.

[22] Rachel Botsman and Roo Rogers, "What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live", 2011. gads.

[23] *Future of Privacy Forum*, "User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy", 2015. gada jūnijs.

[24] Skatīt ASV Federālās tirdzniecības komisijas 2015. gada 9. jūnija darbsemināru "Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy" (Sadarbīgā patēriņa radītie jautājumi konkurences, patērētāju aizsardzības un ekonomikas jomā) https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/ (skatīts 10.09.2015.).

[25] Saistībā ar dronu vai tālvadības gaisa kuģu sistēmu ietekmi uz datu aizsardzību skatīt EDAU atzinumu par Komisijas paziņojumu Eiropas Parlamentam un Padomei "Jauna lappuse aviācijas vēsturē. Aviācijas tirgus atvēršana tālvadības gaisa kuģu sistēmu drošai un ilgtspējīgai izmantošanai civiliem mērķiem", 2014. gada novembris.

[26] Avots: *Boston Consulting Group*.

[27] *Gartner*.

[28] Ir ziņots, ka *Facebook DeepFace* seju atpazīšanas algoritms ir bijis sekmīgs 97 % gadījumu, pārspējot cilvēkus; "Deep Face: Closing the Gap to Human-Level Performance in Face Verification", publicēts ziņojumā par *IEEE* konferenci par datoru redzi un attēlu atpazīšanu, 2014. gada jūnijs.

[29] Robo ir definēts kā "mašīna, kas darbojas pasaulē un uztver, domā un rīkojas"; Bekey, G., "Current trends in robotics: technology and ethics, in Robot Ethics - The ethical and social implications of robotics", *The MIT Press2*, 2012. gads, 18. lpp. Tiek lēsts, ka laikposmā starp 2013. un 2016. gadu

būs pārdoti 22 miljoni pakalpojumu robotu; *IRF World Robotics Report*, 2013. gads. Saistībā ar mākslīgo intelektu skatīt "Rise of the Machines", *Economist*, 09.05.15., un Pjū Pētniecības centra interneta projektu, 2014. gads. Mākslīgā intelekta uzņēmums 2014. gadā noteica, ka vadošs tehnoloģiju uzņēmums to varēs iegādāties tad, ja izpildīs priekšnosacījumu par ētikas un drošības valdes izveidi un aizliegs izmantot mākslīgā intelekta darbu militāros vai izlūkošanas nolūkos; *Forbes*, "Inside Google's Mysterious Ethics Board", 03.02.2014.

[30] Pentland, *Social physics*, 147. lpp.

[31] Skatīt iepriekš 9. piezīmi. Pentland, *Social Physics*, 153. lpp.: "Lieli attīstības lēcieni veselības aprūpes, transporta, enerģētikas un drošības jomā ir iespējami (..) galvenie šķēršļi šo mērķu sasniegšanā ir bažas par privātuma aizsardzību un fakts, ka mēs vēl neesam panākuši vienprātību par kompromisiem starp personiskām un sabiedrības vērtībām." Debates saistībā ar 2014. gada Ebolas pandēmiju Rietumāfrikā ilustrē, kā tiek veidots šis nepatiesais dalījums starp personas privātumu un sabiedrības vajadzībām. Bieži vien ar apsekojumu un tautas skaitīšanu palīdzību tiek izsekota slimību izplatība un noteikts to ilgums, tomēr gan apsekojumi, gan tautas skaitīšanas dati ātri zaudē aktualitāti, un tos ir grūti ekstrapolēt, lai prognozētu, kur gaidāms nākamais slimības uzliesmojums. Ir vairāki piemēri lielo datu izmantošanai malārijas uzliesmojumu izsekošanā Namībijā un Kenijā, kā arī efektivitātes izsekošanai attiecībā uz valdības brīdinājumiem par veselības aizsardzību 2009. gadā Meksikas cūku gripas krīzes laikā. Viens datu avots ir mobilo izsaukumu reģistri, kas parāda bāzes staciju, kura atbild uz izsaukumu, un reālajā laikā spēj sniegt aptuvenu aplēsi par cilvēku atrašanās vietu un virzienu, kurā tie dodas. Visu šo datu apkopošana nav mērķtiecīga, jo šādi nav iespējas noteikt, kuri cilvēki ir vai nav slimi ar Ebolas vīrusu. Zviedrijas bezpeļņas organizācija veica iedzīvotāju mobilitātes kartēšanu Rietumāfrikā, bet dati netika izmantoti, jo mobilo telefonsakaru operatori nenodeva datus apstiprinātiem ārējiem pētniekiem, apgalvojot, ka viņiem ir vajadzīgas norādes no valdībām, kas savukārt atsaucās uz bažām par privātuma aizsardzību, kuras mazināšana saskaņā ar ES tiesisko regulējumu nebija attaisnojamahttp://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola. (skatīts 10.09.2015.)

[32] EDAU atzinums Nr. 3/2015.

[33] Lielo datu pieņēmums, ka "N=viss" nozīmē visu datu, nevis tikai parauga aplūkošanu, *Viktor Mayer-Schönberger* un *Kenneth Cukier*, "The Rise of Big Data: How it's changing the way we think about the world", 2013. gads. Lisabonas Padome un Progresīvās politikas institūts ir apgalvojuši, ka pārticība pieaugs, maksimāli palielinot "digitālo blīvumu" — "ekonomikā uz vienu iedzīvotāju izmantoto datu apjomu"http://www.lisboncouncil.net/component/downloads/?id=1178 (skatīts 10.09.2015.). Starptautiskā darba grupa datu aizsardzībai telekomunikāciju jomā (zināma arī kā "Berlīnes grupa") ir ierosinājusi piemērot lielajiem datiem atkāpes no datu aizsardzības principiem:http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf. (skatīts 10.09.2015.). Pasaules Ekonomikas forumā tika pausts aicinājums galveno uzmanību pievērst izmantošanai, nevis vākšanai un atteikties no prasības saņemt atļauju personīgo datu vākšanai; "Unlocking the Value of Personal Data: From Collection to Usage", 2013. gads.

[34] Skatīt EDAU sākotnējo atzinumu "Privātums un konkurētspēja lielo datu laikmetā".

[35] ES Pamattiesību hartas 21. pantā ir "aizliegta jebkāda veida diskriminācija, tostarp diskriminācija dzimuma, rases, ādas krāsas, etniskās vai sociālās izcelsmes, ģenētisko īpatnību, valodas, reliģijas vai pārliecības, politisko vai jebkuru citu uzskatu dēļ, diskriminācija saistībā ar piederību pie nacionālās minoritātes, diskriminācija īpašuma, izcelsmes, invaliditātes, vecuma vai dzimumorientācijas dēļ". Saskaņā ar Direktīvas 95/46/EK 8. pantu daudziem šo kategoriju datiem ("kas atklāj rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībās, kā arī uz veselību vai seksuālo dzīvi attiecināmu datu apstrādi") ir noteikta pastiprināta aizsardzība.

[36] Saistībā ar ideju par digitālo datu masīvu skatīt "Ambition numérique: Pour une politique française et européenne de la transition numérique", Francijas Digitālā padome, 2015. gada jūnijs, 276. lpp.; *Bruce Schneier* atbalsta tādu "nevienam nepiederošu publisku telpu" izveidi internetā kā publiskie

parki, *Data and Goliath,* 188.–189. lpp.; *Sandy Pentland* atbalsta "publisko datu masīvu", *Social Physics,* 179. lpp. Saistībā ar apkopotu datu kopu kā atklātu datu publicēšanas drošības novērtējumu skatīt 29. panta darba grupas atzinumu Nr. 6/2013 par atklātajiem datiem un valsts sektora informācijas atkalizmantošanu.

[37] "Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent" http://crackedlabs.org/studie-kommerzielle-ueberwachung/info. Saistībā ar kvalitatīvo pārredzamību skatīt, piemēram, *Frank Pasquale*, "The Black Box Society: The Secret Algorithms that Control Money and Information".

[38] "Aiz tehnoloģijām, kas ietekmē sociālās attiecības, stāv šīs pašas sociālās attiecības," pauž *David Noble*, "Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools", *Case Studies in the Labor Process*, ed. *Andrew Zimbalist*, 1979. gads Skatīt arī *Judy Wacjman*, "Pressed for Time: The Acceleration of Life in Digital Capitalism", 2014. gads, 89., 90. lpp., un *Zuboff*, "Big Other" (citēts iepriekš 3. piezīmē).

[39] Atzinums Nr. 5/2014 par anonimizācijas metodēm (WP 216), ko pieņēma 2014. gada 10. aprīlī.

[40] Saistībā ar šauri izstrādātu atbrīvojumu no datu aizsardzības noteikumiem tikai personiskām vai mājsaimniecības vajadzībām skatīt Eiropas Savienības Tiesas spriedumu lietā C-212/13 *František Ryneš* / *Úřad pro ochranu osobních údajů*.

[41] Terminu "ražojošs patērētājs" (*prosumer*) ieviesa *Alvin Toffler* darbā *The Third Wave*, 1980. gads. Diskusiju par "ražojoša patērētāja vidi" un iespējām to regulēt skatīt *Ian Brown* un *Chris Marsden*, "Regulating Code", 2013. gads

[42] Eiropas grupas par dabaszinātņu ētiku un jaunām tehnoloģijām atzinums Eiropas Komisijai: Drošības un uzraudzības tehnoloģiju ētika, atzinums Nr. 28, 20.05.2015, 74. lpp.

[43]Skatīt, piemēram, *Homer Economicus: The Simpsons and Economics*, ed. *Joshua Hall*, 2014. gads

[44] Saskaņā ar kļūdas konservatīvāko definīciju tas nozīmē, ka 23 miljonu amerikāņu patērētāju kredītinformācijā ir pieļautas būtiskas kļūdas. Attiecībā uz 5 % pētījuma dalībnieku pieļauto kļūdu novēršana uzlaboja viņu kredītvērtējumu tik lielā mērā, ka viņi varēja iegūt kredītu par zemāku cenu; Federālā tirdzniecības komisija, Ziņojums Kongresam saskaņā ar 2003. gada Likuma par godīgiem un precīziem kredīta darījumiem 319. sadaļu, 2012. gada decembris; *Chris Jay Hoofnagle*, "How the Fair Credit Reporting Act Regulates Big Data" (2013. gada 10. septembris). *Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet*, 2013. gads Pieejams *SSRN*: http://ssrn.com/abstract=2432955.

[45] Pasaules Ekonomikas forums uzskata datus par vērtīgu fiziskas personas līdzekli, kura īpašumtiesības, izmantošanas un iznīcināšanas tiesības var tikt piešķirtas uzņēmumiem un valdībām apmaiņā pret pakalpojumiem. Skatīt jaunākās runas, arī Komisijas priekšsēdētāja vietnieka *A. Ansip* runu, piemēram, 2015. gada 7. septembrī *Bruegel* ikgadējā sanāksmē ar nosaukumu "Produktivitāte, inovācija un digitalizācija — kuras ir globālās politikas problēmas?": "Datu plūsmu īpašumtiesības un pārvaldība, datu izmantošana un atkalizmantošana. Datu pārvaldība un uzglabāšana. Šie jautājumi veido pamatu tādām svarīgām jaunām nozarēm kā mākoņdatošana, lietiskais internets un lielie dati."

[46] "Tātad — kuram ir tiesības izmantot informāciju un datus, kas tam pašam īsti nepieder?" Šis ir jautājums, kas pārsniedz tirdzniecības, ētikas un morāles robežas, un no tā izriet ar privātumu un privātuma aizsardzību saistītas problēmas; *Al-Khouri*, 2012. gada novembris, http://www.academia.edu/6726887/Data_Ownership_Who_Owns_My_Data_036. Skatīt arī *Margaret Jane Radin*, "Incomplete Commodification in the Computerized World", *The Commodification of Information* 3, 17, *Niva Elkin-Koren* & *Neil Weinstock Netanel eds.*, 2002. gads: "Ir liela atšķirība starp to, vai privātumu uzskata par cilvēktiesībām, kas ir saistītas ar fiziskām personām to personības dēļ, vai arī to uzskata par īpašumtiesībām, kas fiziskām personām var piederēt un ko tās var kontrolēt. Cilvēktiesības prezumptīvi nav pārdodamas tirgū, savukārt īpašumtiesības prezumptīvi ir pārdodamas tirgū."

[47] *MIT* Datorzinātņu un mākslīgā intelekta laboratorijas *Crosscloud* projektu atbalsta vairāki ES reģistrēti uzņēmumi, un tā mērķi ir "1) panākt vienkāršu vairāklietotāju ("sociālas") programmatūras izstrādi, izmantojot tikai priekšgalsistēmu izstrādi un ievērojot lietotāju tiesības un privātumu, un 2) sniegt lietotājiem iespēju brīvi pārvietoties starp lietojumprogrammām, aparatūras platformām un sociālajiem tīkliem, saglabājot savus datus un sociālos kontaktus"http://openpds.media.mit.edu/#architecture (skatīts 10.09.2015.).

[48] Skatīt Pamattiesību hartas 1. panta skaidrojumu.

[49] *Martha Nussbaum*, "Objectification", *Philopsophy and Public Affairs* 24, 4, 1995. gads.

[50] 1983. gada 15. decembra spriedums, *BVerfGE* 65, 1.–71. lpp., *Volkszählung*.

[51] Skatīt Eiropas grupas par dabaszinātņu ētiku un jaunām tehnoloģijām Atzinumu par ētiku un uzraudzību, 75. lpp. Pētījumā tika norādīts, ka reklāmu mērķgrupu noteikšanas algoritms ir diskriminējošs, jo, salīdzinot sievietes un vīriešus, kuri apmeklēja darba sludinājumu tīmekļa vietnes, attiecībā uz vīriešu veiktajiem meklējumiem vidēji tika uzrādītas reklāmas par augstāk apmaksātām darbvietām. Saistībā ar tendenci ciparasistentiem pēc noklusējuma piešķirt sieviešu balsis skatīt, piemēram, *Judy Wajcman*, "Feminist theories of technology", *Cambridge Journal of Economics*, 34 (1). 143.–152. lpp., 2010. gads.

[52] *Giorgio Agamben, State of Exeption,* 2005. gads.

[53] *Neil Richards, Neil and Jonathan King*, "Big Data Ethics" (2014. gada 19. maijs), *Wake Forest Law Review*, 2014. gads.

[54] BBC, *Information watchdog investigates "charity data sales"*, 01.09.2015.

[55] Skatīt vēstuli no *Future of Life Institute*. Romas pāvesta enciklika *Laudato Si:* "(..) kad plašsaziņas līdzekļi un digitālā pasaule kļūs visuresoša, tās ietekmē var apsīkt cilvēku centieni mācīties, kā viedi dzīvot, kā dziļi domāt un kā nesavtīgi mīlēt. Saistībā ar to pastāv draudi, ka pārmērīgā informācijas daudzuma radītajā troksnī un apjukumā iepriekšējos laikmetos dzīvojušo viedo personību sacītais vairs netiks sadzirdēts. Ir jācenšas panākt, lai šie plašsaziņas līdzekļi kļūtu par jauna cilvēces kultūras progresa avotiem, nevis mūsu dziļāko bagātību apdraudējumu. Patiesa gudrība ir pašanalīzes, dialoga un nesavtīgas personu saskarsmes auglis, un to nav iespējams iegūt, vienkārši uzkrājot datus, kas galu galā rada pārslodzi un apjukumu, sava veida garīgo piesārņojumu. Mūsdienās ir vērojama tendence, ka īstas attiecības ar citiem cilvēkiem un problemātika, ko šādas attiecības ietver, aizvien biežāk tiek aizstāti ar interneta komunikācijas paveids, kas mums sniedz iespēju izvēlēties veidot vai izbeigt attiecības mirkļa iegribas rezultātā, tādējādi radot jaunu izdomātu emociju veidu, kas ir vairāk saistītas ar ierīcēm un izrādīšanos, nevis ar citiem cilvēkiem un ar dabu. Mūsdienās plašsaziņas līdzekļi mums sniedz iespēju sazināties un dalīties ar zināšanām un jūtām. Tomēr nereti tie mūs arī izolē no tiešas saskares ar citu cilvēku sāpēm, bailēm un priekiem, kā arī no viņu personiskās pieredzes daudzslāņainības. Tāpēc mums ir jājūt bažas, ka līdz ar aizraujošajām iespējām, ko piedāvā šie plašsaziņas līdzekļi, var rasties arī dziļa un melanholiska neapmierinātība ar bezpersoniskajām attiecībām vai kaitīga izolācijas sajūta."

[56] Skatīt EDAU stratēģijas 2015.–2020. gadam 4. sadaļu par datu aizsardzības ētiskās dimensijas izstrādi.