

EUROPEAN DATA PROTECTION SUPERVISOR

Nuomonė Nr. 4/2015

Naujos skaitmeninės etikos link

Duomenys, orumas ir technologijos



EDPS

2015 m. rugsėjo 11 d.

Europos duomenų apsaugos priežiūros pareigūnas (EDAPP) yra nepriklausoma ES institucija, kuri pagal Reglamento Nr. 45/2001 41 straipsnio 2 dalį atsako už tai, „kad būtų užtikrinta, jog Bendrijos institucijos ir įstaigos, tvarkydamos asmens duomenis, gerbia fizinių asmenų pagrindines teises ir laisves, svarbiausia – jų teisę į privataus gyvenimo neliečiamumą“, ir „už [...] Bendrijos institucijų, įstaigų ir duomenų subjektų konsultavimą visais su asmens duomenų tvarkymu susijusiais klausimais“. Priežiūros pareigūnui ir jo pavaduotojui 2014 m. gruodžio mėnesį paskirta speciali užduotis veikti konstruktyviau ir aktyviau. 2015 m. kovo mėn. EDAPP pateikė penkerių metų strategiją, kurioje numatyta, kaip jis ketina įgyvendinti šią užduotį ir būti atskaitingas už jos įgyvendinimą.

Šia nuomone tęsiama anksčiau EDAPP pateikta nuomonė dėl Bendrojo duomenų apsaugos reglamento, kuriuo buvo siekiama padėti pagrindinėms ES institucijoms pasiekti reikiamą sutarimą dėl veiksmingų, į ateitį orientuotų taisyklių, kuriomis grindžiamos individų teisės ir laisvės. Kaip ir 2015 m. pradžioje pateiktoje nuomonėje dėl mobiliosios sveikatos priežiūros, šioje nuomonėje sprendžiamas duomenų apsaugos „skaitmeninimo“ klausimas (trečiasis EDAPP strategijos tikslas) – „globaliai skaitmeninei erdvei pritaikant esamus duomenų apsaugos principus“ ir atsižvelgiant į ES planus dėl bendrosios skaitmeninės rinkos. Ši nuomonė atitinka 29 straipsnio darbo grupės, prie kurios EDAPP prisidėjo visaverčio nario teisėmis, požiūrį į duomenų apsaugos aspektus naudojant naujas technologijas, tokias kaip daiktų internetas.



Dignity	Orumas
Future-oriented rules and enforcement	Į ateitį orientuotos taisyklės ir teisių vykdymo užtikrinimas
Accountable controllers	Atskaitingi valdytojai
Empowered individuals	Įtakos įgiję individai
Innovative privacy engineering	Naujoviška privatumo inžinerija
Ethics	Etika

„Žmogaus orumas yra neliečiamas. Jį reikia gerbti ir saugoti.“

1 straipsnis, ES pagrindinių teisių chartija

Pagrindinės teisės į privatumą ir asmens duomenų apsaugą šiuo metu kaip niekada svarbios siekiant apsaugoti žmogaus orumą. Šios teisės įtvirtintos ES sutartyse ir ES pagrindinių teisių chartijoje. Jos leidžia individams ugdyti savo asmenybę, gyventi nepriklausomą gyvenimą, kurti naujoves ir naudotis kitomis teisėmis ir laisvėmis. ES chartijoje apibrėžti duomenų apsaugos principai – reikalingumo, proporcingumo, sąžiningumo, duomenų kiekio mažinimo, tikslų apribojimo, sutikimo ir skaidrumo – taikomi visam duomenų tvarkymui, jų rinkimui ir naudojimui.

Technologijos neturėtų diktuoti vertybių ir teisių, tačiau šių dviejų sričių negalima ir visiškai atskirti. Numatoma, kad skaitmeninė revoliucija suteiks naudos sveikatos, aplinkos sritims, tarptautinei plėtrai ir ekonominiam efektyvumui. ES planuose dėl bendrosios skaitmeninės rinkos, debesijos kompiuterijos, daiktų interneto dideli duomenų kiekiai ir technologijos yra traktuojami kaip konkurencingumo ir augimo pamatas. Verslo modeliuose išnaudojamos naujos galimybės masiškai rinkti, akimirksniu perduoti, derinti ir pakartotinai naudoti asmeninę informaciją. Šie veiksmai dažnai atliekami iš anksto nenumatytais tikslais ir pagrįsti ilga, sunkiai suprantama privatumo politika. Tokia padėtis sukėlė naują įtampą dėl duomenų apsaugos principų, todėl reikia iš naujo apgalvoti jų taikymą.

Nūdienos skaitmeninėje aplinkoje vien laikytis įstatymų nepakanka; turime apsvarstyti etinį duomenų tvarkymo aspektą. ES reguliavimo sistema jau dabar leidžia tvarkant asmeninę informaciją priimti lankstesnius, konkrečiam atvejui pritaikytus sprendimus ir naudoti apsaugos priemones. Geras žingsnis į priekį bus reguliavimo sistemos reforma. Tačiau esama sudėtingesnių klausimų, kuriuos reikia permąstyti: kokią poveikį duomenų tvarkymo tendencijos turi visuomenės orumui, asmens laisvei ir demokratijos funkcionavimui.

Atsakymai į šiuos klausimus turės inžinerinių, filosofinių, teisinių ir moralinių pasekmių. Šioje nuomonėje akcentuojamos kai kurios svarbiausios technologijų tendencijos, galinčios apimti nepriimtinius asmens informacijos tvarkymo būdus arba pažeisti teisę į privatumą. Joje bendrais bruožais nusakoma keturių pakopų „didelių duomenų apsaugos ekosistema“ – atsakas į skaitmeninį iššūkį, etiniais svarstymais grindžiamos kolektyvinės pastangos.

- (1) Į ateitį orientuotas duomenų tvarkymo reguliavimas, pagarba teisėms į privatumą ir duomenų apsaugą.
- (2) Atskaitingi duomenų valdytojai, kurie nustato asmeninės informacijos tvarkymą.
- (3) Privatumą apsauganti inžinerija ir duomenų tvarkymo produktų ir paslaugų projektavimas.
- (4) Įtakos įgiję individai.

Europos duomenų apsaugos priežiūros pareigūnas siekia skatinti tiek ES, tiek už jos ribų atviras ir informatyvias diskusijas, kuriose dalyvautų pilietinė visuomenė, kūrėjai, įmonės, mokslininkai, valdžios ir reguliavimo institucijos. EDAPP tarnyboje įsteigsime ES duomenų apsaugos etikos tarybą. Ji padės sukurti naują skaitmeninę etiką, leisiančią geriau

suvokti, kokią naudą technologijos turės visuomenei ir ekonomikai, ir ją naudoti taip, kad būtų stiprinamos individų teisės ir laisvės.

TURINYS

1. Duomenys visur: tendencijos, galimybės ir iššūkiai.....	7
1.1 DIDELI DUOMENŲ RINKINIAI.....	7
1.2 DAIKTŲ INTERNETAS.....	8
1.3 APLINKOS DUOMENŲ TVARKYMAS.....	8
1.4 DEBESIJOS KOMPIUTERIJA.....	8
1.5 NUO ASMENS DUOMENŲ PRIKLAUSOMI VERSLO MODELIAI.....	9
1.6 BEPILOČIAI ORLAIVIAI IR AUTONOMINĖS TRANSPORTO PRIEMONĖS.....	9
1.7 TENDENCIJOS, GALINČIOS TURĖTI PLATESNIO MASTO IR LABIAU ILGALAIKĘ ĮTAKĄ	10
2. Didelių duomenų rinkinių apsaugos ekosistema.....	10
2.1 Į ATEITĮ ORIENTUOTAS REGULIAVIMAS.....	11
2.2 ATSKAITINGI VALDYTOJAI.....	11
2.3 PRIVATUMĄ SAUGANTI INŽINERIJA.....	12
2.4 ĮTAKOS ĮGIJĘ INDIVIDAI.....	12
„Profesionalių vartotojų“ aplinka.....	12
Sutikimas.....	12
Valdymas ir duomenų „nuosavybė“.....	13
3. Orumas – naujosios skaitmeninės etikos šerdis.....	13
3.1 ORUMAS IR DUOMENYS.....	13
3.2 EUROPOS PATARIAMOJI ETIKOS TARYBA.....	15
4. Išvada: laikas skatinti gilesnes diskusijas.....	15
Pastabos.....	17

1. Duomenys visur: tendencijos, galimybės ir iššūkiai

Vis gausesnė asmeninės informacijos kiekiai surenkami ir tvarkomi taikant vis neskaidresnius ir sudėtingesnius metodus. XX a. devintajame dešimtmetyje įmonėms ir viešojo administravimo institucijoms pradėjus labai aktyviai naudoti kompiuterius, plačiai įsivyravo nuomonė, kad galingų vyriausybės ir įmonių taikoma asmens duomenų tvarkymo praktika individus pavers paprasčiausiais duomenų subjektais ir sukels grėsmę pagrindinėms teisėms ir laisvėms. Dabartinė integruotos informacijos ir ryšio technologijų banga nuo minėtos situacijos skiriasi savo aprėptimi ir įtaka.

Pernai paskelbta, kad planetoje įrenginių, kuriuose naudojamas interneto ryšys, yra daugiau nei žmonių¹. Išaugus tvarkymo gebai², saugykloms ir perdavimo spartai, lieka vis mažiau asmeninės informacijos tvarkymo techninių kliūčių. Numatoma, kad daiktų internetas ir didelių duomenų rinkinių analizės susilies su dirbtiniu intelektu, natūralios kalbos apdorojimu ir biometrinėmis sistemomis – tai leistų dar labiau padidinti mašininio mokymosi gebėjimu pasižyminčių įrenginių intelektą. Vyriausybės ir įmonės gali vykdyti ne tik „duomenų gavybą“, bet ir „realybės gavybą“ – įsiskverbti į kasdienius potyrius, komunikaciją ir netgi mintis³. Visuomenei prisitaikant prie skaitmeninės rinkos poreikių, vėl atnaujintos pastangos programavimo mokytį mažus vaikus⁴. ES yra didžiausia šio sektoriaus vartotoja, bet stokoja paslaugų teikimo. Šio sektoriaus tendencijų panaudojimas – pasikartojanti Komisijos bendrosios skaitmeninės rinkos strategijos tema⁵.

Šios tendencijos ir daugybė šiuo metu naudojamų koncepcijų, nepaisant jų populiarumo, yra miglotos ir sutartinės. Kad paskatintume debatus, norime atkreipti dėmesį į konkrečias tendencijas (žinoma, sąrašas nėra baigtinis), kurios, mūsų manymu, kelia svarbiausius etinius ir praktinius klausimus dėl duomenų apsaugos principų taikymo.

1.1 Dideli duomenų rinkiniai

Sąvoka „dideli duomenų rinkiniai“⁶ apibrėžiamas milžiniškos apimties, iš skirtingų šaltinių surinktos informacijos derinimas ir analizė, dažnai naudojant automatinio mokymosi algoritmus. Remiantis gautais rezultatais priimami sprendimai. Ši informacija ne visuomet yra asmeninė: duomenys, kuriuos jutikliai generuoja gamtos ar atmosferos reiškinių (tokių kaip oras ar tarša) stebėsenai arba gamybos proceso techninių aspektų stebėsenai, nėra susiję su „asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta“⁷. Tačiau vieni iš vertingiausių duomenų, kuriuos įmonės ir vyriausybės gauna iš didelių duomenų rinkinių, renkami stebint žmonių elgesį – bendrą arba individualų. Šie duomenys suteikia galimybę prognozuoti⁸.

Vienas iš rezultatų – interneto įmonių pajamų modelio susiformavimas. Šios įmonės stebi internetinę veiklą, kad galėtų optimizuoti paslaugų teikėjų operacijų ekonominę vertę – ne tik taikydamos tikslingą reklamą, bet ir keisdamos draudimo sutarčių bei paskolų sąlygas ir normas bei kitus sutartimis grįstus santykius. Rinkoje jaučiama didžiulė konkurencija dėl naudotojų dėmesio ir daugelis žmonių nežino, koks platus yra tokio stebėjimo mastas⁹. Tokie „didelių duomenų rinkiniai“ laikytini asmeniniais net ir tada, kai pritaikyti anonimiškumo metodai: tampa vis lengviau nustatyti asmens tapatybę tariamai anoniminius duomenis suderinus su kitais duomenų rinkiniais, įskaitant viešai prieinamą (pvz., socialiniuose tinkluose) informaciją¹⁰. Kai duomenimis prekiaujama, ypač tarp valstybių ir skirtingų jurisdikcijų, atskaitomybė už informacijos tvarkymą tampa miglota, ją sunku užtikrinti arba priverstinai taikyti pagal duomenų apsaugos teisės aktus (ypač tada, kai nėra jokių tarptautinių standartų).

1.2 Daiktų internetas

Jau įprasta naudoti įvairiausių įrenginius, kuriuose naudojamas interneto ryšys – išmaniuosius telefonus, planšetinius kompiuterius ir grynųjų pinigų išdavimo ar registracijos į skrydį įrenginius. Numatoma, kad 2020 m. ryšio galimybė taps standartine funkcija: interneto ryšį naudos 25 mlrd. objektų (plg. su 4,8 mlrd. 2015 m.) – nuo nuotolinės medicinos įrenginių iki transporto priemonių, nuo išmaniųjų skaitiklių iki įvairiausių naujų stacionarių ir mobiliųjų įrenginių, leidžiančių kurti pažangius miestus¹¹.

Šie jutikliai akimirksniu suteiks fragmentuotos informacijos, kuri statistikos biurams ir tyrimams šiuo metu yra neprieinama – tačiau tai nereiškia, kad informacija bus tikslesnė. Gali būti, kad ji bus netgi klaidinanti¹². Numatyta, kad 2022 m. bus sukurta maždaug 1,8 mlrd. automobilių tarpusavio sąveikos jungčių. Jos galės sumažinti avarijų skaičių ir taršos lygį, pagerinti vyresnio amžiaus žmonių ir neįgaliųjų produktyvumą ir savarankiškumą¹³. „Dėvimieji“ įrenginiai (pvz., drabužiai ir laikrodžiai) tvarkys asmeninę informaciją kaip ir kiti internetą naudojančius įrenginius. Jie galės aptikti kraujo krešulius, stebėti fizinę būklę ir žaizdų gijimą. Interneto ryšį naudojančius audiniai galės apsaugoti nuo pavojingos aplinkos (pvz., gėsinant gaisrus). Šie įrenginiai asmens duomenis nusiųs tiesiai į debesijos kompiuterijos laikmenas, turinčias ryšį su socialiniais tinklais. Duomenys galės būti paviešinti, suteikti galimybę nustatyti naudotojų tapatybę ir stebėti individų bei minios elgesį ir judėjimą¹⁴.

Informacijos tvarkymo pobūdis gali paveikti ne tik įrenginių (įskaitant naudojamus darbo vietoje) naudotojų privatumą, bet ir kitų asmenų, kuriuos stebi ir kurių duomenis įrenginys įrašo, teises. Nors įrodymų apie realią diskriminaciją yra nedaug, akivaizdu, kad daiktų interneto surinkti milžiniški asmeninės informacijos kiekiai sulaukia didelio susidomėjimo – jie gali tapti pajamų gausinimo priemonėmis, nes leidžia atsižvelgiant į stebėtą elgesį labiau suasmeninti kainų pasiūlymus (ypač – sveikatos draudimo sektoriuje)¹⁵. Problemų gali kilti ir dėl kitoms konkrečioms sritims skirtų taisyklių (pvz., kai sveikatos duomenis tvarkantys įrenginiai techniškai nepriskiriami medicinos prietaisų kategorijai ir nepatenka į reglamento aprėptį)¹⁶.

1.3 Aplinkos duomenų tvarkymas

Aplinkos duomenų tvarkymas arba nematomas duomenų tvarkymas – tai pagrindinė technologija, kuria grindžiamas daiktų internetas. Vienas iš akivaizdžiausių naudojimo pavyzdžių – „išmanieji namai“ arba „išmanieji biurai“. Juos sudaro įrenginiai, pasižymintys sudėtinės informacijos tvarkymo pajėgumu, leidžiančiu pagerinti energijos vartojimo efektyvumą. Daugiau asmenų yra gerai informuoti ir gali energijos suvartojimą valdyti nuotoliniu būdu (nors tai priklauso nuo gyventojų nepriklausomybės nuo nuomotojo arba pastato valdytojo). Reikės aiškiai nustatyti, kas yra atsakingas už aplinkos duomenų tvarkymo programomis atliekamo asmens duomenų tvarkymo tikslą ir priemones. Tai svarbu ne tik dėl asmens pagrindinių teisių apsaugos, bet ir dėl klausimo, kam priskirti atsakomybę užtikrinti atitiktį visos sistemos saugos reikalavimams.

1.4 Debesijos kompiuterija

Debesijos kompiuterija vadinama pagrindinė technologija, leidžianti atlikti išsamias analizes ir išplėsti gavybos galimybes, sudaryti didelius duomenų rinkinius ir juos analizuoti. Ji taip pat naudojama daiktų interneto duomenų srautui. Šiuo metu debesijos kompiuterijos

paslaugomis naudojasi maždaug penktadalis ES individų ir įmonių¹⁷. Debesijos kompiuterija leidžia sutelkti duomenis iš galybės daiktų interneto įrenginių. Jos pamatas – milžiniškos apimties duomenų, kaupiamų didelėse saugyklose ir tvarkymo infrastruktūrose visame pasaulyje, prieinamumas ir ryšys¹⁸. Apskaičiuota, kad plačiau naudodami debesijos kompiuterijos paslaugas¹⁹ privatusis ir viešasis sektoriai ES-28 BVP gali papildyti 449 mlrd. eurų (0,71 proc. bendro ES BVP).

Asmeninės informacijos kontrolė dažnai priklauso ir naudotojui, ir debesijos kompiuterijos paslaugų teikėjui. Atsakomybė dėl duomenų apsaugos įsipareigojimų ne visada yra aiški. Tai reiškia, kad praktiškai nėra suteikiama pakankamai apsaugos. Šie įsipareigojimai nepriklauso nuo **fizinės duomenų laikymo vietos. Be to**, nors debesijos kompiuterijos infrastruktūra yra tik pagalbinė technologija, padedanti plėtoti verslo veiklą, ji gali įgyti ypatingą svarbą ir padidinti įtakos rinkoje disbalansą: 30 proc. įmonių pastaruoju metu teigė susiduriančios su problemomis, kai nori atsisakyti tiekėjų paslaugų arba juos pakeisti²⁰.

1.5 Nuo asmens duomenų priklausomi verslo modeliai

Šios technologijos leido sukurti naujus verslo modelius, kurie riziką ir kreditingumą vertina ir pajamas didina remdamiesi informacija, gaunama ne tik teikiant paslaugas, bet ir iš kitų šaltinių, tokių kaip socialiniai tinklai. Dabartinis sėkmingo verslo modelio pavyzdys – platformos, jungiančios pardavėjus ir pirkėjus ir leidžiančios dalytis ir paskirstyti produktus, paslaugas, įgūdžius ir turtą. Šios platformos dažnai vadinamos „dalijimosi ekonomika“, „bendradarbiavimu grįsta ekonomika“ arba internetinėmis ir mobiliosiomis tarpusavio sąveikos platformomis.²¹ Jos dažnai gali pasiūlyti tradicinių ekonominių privalumų, paskatinti rinkų konkurencingumą ir sumažinti atliekų kiekį. Numatyta, kad pasaulinė jų vertė per ateinančius metus išaugs keturis kartus – nuo 26 iki 110 mlrd. JAV dolerių²². Tokie duomenimis grįsti verslo modeliai jau kuria milžiniškas pajamas automobilių dalijimosi, namų nuomos, finansinių technologijų ir tarpusavio skolinimo srityse. Apklaustos atskleidžia, kad vartotojai vertina geresnį jų įperkumą ir prieinamumą²³.

Įprasta tokių platformų valiuta – vartotojo reputacija, tarpusavio vertinimas ir tapatybės patvirtinimas. Tai galima vertinti kaip skaidrumo ir atskaitomybės stiprinimą, bet tai nebūtinai galioja pačiam platformos teikėjui. Stambūs šių rinkų veikėjai sulaukė kritikos dėl to, kad reputacijai įtakos turinčių duomenų tariamai neatskleidžia net patiems vartotojams, su kuriais tokia informacija yra susijusi. Kyla milžiniška rizika, kad asmenys nebegalės naudotis paslaugomis dėl reputacijos, grindžiamos netiksliais duomenimis, kurių patys negalėjo pakeisti arba paprašyti pašalinti. Kliovimasis kelių šaltinių duomenimis taip pat skatina apsvaistinti ES duomenų kiekio mažinimo teisės aktų principą. Šių ir ateityje susiformuosiančių verslo modelių, kuriuos įgyvendinti leidžia technologijos, poveikio individams ir visuomenei mastą reikia nuodugniai apsvaistinti²⁴.

1.6 Bepiločiai orlaiviai ir autonominės transporto priemonės

Bepiločiai orlaiviai, dar vadinami pusiau autonomiais orlaiviais, šiuo metu dažniausiai naudojami kariniais tikslais, tačiau vis aktyviau jie pasitelkiami ir stebėsenos, planavimo, gabenimo, logistikos ir visuomenės saugos (pvz., gamtinių teritorijų gaisrų) tikslais²⁵. Bepiločių orlaivių užfiksuotomis nuotraukomis, vaizdo įrašais ir kitais asmens duomenimis galima keistis per telekomunikacijų tinklus. Naudojimo rizika rimtai trikdo privatumą ir kenkia saviraiškos laisvei. Kyla klausimas, kaip efektyviai reguliuoti šių įrenginių projektavimą ir naudojimą, kad duomenų subjektai galėtų pasinaudoti savo teise į prieigą prie duomenų, surinktų juos naudojant.

Autonominės transporto priemonės arba bepiločiai automobiliai pakeis asmeninių kelionių pobūdį ir rengimą. Jos gali sumenkinti skirtumą tarp privataus ir viešojo transporto. Apskaičiuota, kad sulaukus 2035 m. bus naudojama 12 mln. visiškai autonominių ir 18 mln. iš dalies autonominių transporto priemonių, o Europa jas pradės naudoti viena iš pirmųjų²⁶. Automobilių valdymo algoritmai lems sprendimus, kurie gali turėti tiesioginę įtaką individų fizinei gerovei ir netgi gyvybei ar mirčiai – pvz., neišvengiamo susidūrimo atvejui užprogramuotas sprendimas. Kyla akivaizdus poreikis aiškiai nurodyti, kas yra atsakingas ir atskaitingas už duomenų kontrolę ir duomenų saugumą. Be to, kyla įvairių etinių klausimų.

1.7 Tendencijos, galinčios turėti platesnio masto ir labiau ilgalaikę įtaką

Organinių dalių **trimatis biospausdinimas**, atliekamas naudojant pacientų ląsteles ir kolageno „biologines jungtis“ (pagal ES įstatymus laikomas neskelbtiniais duomenimis), siekiant sukurti tolesnes gyvų ląstelių sekas. Manoma, kad ši paslauga netrukus bus prieinama²⁷. Ji leis lengvai tiekti individualiai pritaikytas žmogaus anatomines dalis – tai bus ypač naudinga vargingesnėms ir po konfliktų atsigaunančioms pasaulio teritorijoms. Biospausdinimas kelia akivaizdžių klausimų dėl medicinos etikos, intelektinės nuosavybės apsaugos ir vartotojų apsaugos. Tačiau šis procesas grindžiamas intymiais ir neskelbtiniais duomenimis, susijusiais su asmenų sveikata, todėl reikia apsvarstyti ir duomenų apsaugos taisyklių taikymą.

Dirbtinis intelektas (pvz., robotika) – tai technologiniai reikalavimai, taikomi autonominiams įrenginiams, tiek stacionariems, tiek mobiliems. Jų pažanga leis gerokai išplėsti dabartines taikymo ribas. Išsamaus mokymosi kompiuterių mokymosi procesas vyksta tvarkant didelius duomenų rinkinius, kuriems naudojami (be kita ko) neuroniniai tinklai, atkartojantys smegenų veiklą. Tyrėjai ir įmonės siekia patobulinti nestebimą mokymąsi. Algoritmai jau gali suprasti kalbas, atlikti vertimus, atpažinti atvaizdus, kurti naujus straipsnius ir analizuoti medicinos duomenis²⁸. Socialiniai tinklai pateikia daugybę asmeninės informacijos, kurią veiksmingai pažymi patys individai. Galbūt tai naujausi kognityviniai patobulinimai, skirti žmogaus smegenų gebėjimams padidinti – kaip popierius, skaitytuvai ar autonominiuose įrenginiuose, robotuose, įdiegtos technologijos, tačiau dabar pats metas apsvarstyti platesnes jų pasekmes individams ir visuomenei²⁹.

2. Didelių duomenų rinkinių apsaugos ekosistema

ES dabar turi galimybę imtis lyderės vaidmens ir parodyti, kaip vyriausybės, reguliavimo institucijos, valdytojai, projektuotojai, kūrėjai ir individualūs asmenys gali sėkmingiau bendradarbiauti, kad sustiprintų teises ir paskatintų technologines inovacijas, užuot užkirtę joms kelią. Antroje dalyje aprašytos tendencijos, anot vieno komentatoriaus, „išplėtė atskirtį tarp to, kas įmanoma, ir to, kas teisiškai leistina“³⁰. Priešingai kaip kurioms nuomonėms, privatumo ir duomenų apsauga yra ne kliūtis, o tvariai ir dinamiškai skaitmeninei aplinkai skirta platforma. Nepriklausomoms duomenų apsaugos institucijoms, tokioms kaip EDAPP, tenka pagrindinis vaidmuo siekiant išsklaidyti tokius mitus ir atsakyti į pagrįstą individų nerimą dėl savo asmens duomenų kontrolės praradimo³¹.

Tikėtina, kad naujos kartos asmens duomenys bus dar sunkiau prieinami asmenims, su kuriais yra susiję tiesiogiai. Atsakomybė už tvarios skaitmeninės rinkos formavimą yra plačiai paskirstyta, tačiau tarpusavyje susijusi kaip ekosistema. Reikia, kad kūrėjai, įmonės ir reguliavimo institucijos efektyviai bendradarbiautų individo interesų labui. Šiame skyriuje aptariame, kuo šie keturi pagrindiniai veikėjai gali prisidėti.

2.1 Į ateitį orientuotas reguliavimas

Neseniai paraginome ES pasinaudoti istorine galimybe sukurti paprastesnes asmeninės informacijos tvarkymo taisykles. Šios taisyklės būtų pravarčios ištiesai kartai³². Jau pasiekti paskutiniai derybų dėl bendrojo duomenų apsaugos reglamento ir duomenų apsaugos politikos ir teisės sektoriuose etapai. Greitai bus susitelkta į elektroninio privatumo direktyvą dėl elektroninių ryšių ir naująjį reglamentą, kuriuo bus nustatoma, kaip asmens duomenis tvarko pačios ES institucijos. Ekonominiai duomenų rinkimo ir laikymo kaštai yra neesminiai, todėl duomenų apsaugos institucijoms teks nuolat užtikrinti šių taisyklių laikymąsi, kad būtų išvengta perteklinio duomenų tvarkymo keliamo „moralinio pavojaus“³³.

Bendrosios skaitmeninės rinkos strategijoje patvirtinamas ryšys tarp didelės apimties duomenų kontrolės ir įtakos rinkoje. Strategijoje, kaip ir 2014 m. mūsų paskelbtoje pirminėje nuomonėje dėl privatumo ir konkurencingumo didelių duomenų rinkinių amžiuje, pabrėžiamas poreikis didinti reguliavimo institucijų nuoseklumą. ES jau turi priemonių, leidžiančių tvarkyti įtakos skaitmeninėje rinkoje disbalansą: pvz., Europos Komisijos nagrinėjamos antimonopolinės bylos yra patvirtinamas, kad prieigos prie interneto srityje dominuoja mobilieji įrenginiai. Remiantis esama teisine sistema, įmanoma taikyti bendresnes priverstinio vykdymo priemones. Pvz., per ES informacijos koordinavimo mechanizmą priežiūros institucijos gali apsvarstyti, ar konkrečios bylos atveju kyla klausimų dėl atitikties konkurencijos, vartotojų ir duomenų apsaugos taisyklėms. Pavyzdžiui:

- Reikalavimas skaidriau nustatyti kainą (grynaisiais ar kita forma) už paslaugą galėtų suteikti informacijos ir palengvinti konkurencijos bylų analizę³⁴.
- Nesąžiningos diskriminacijos kainomis dėl prastos duomenų kokybės ir nesąžiningo profilių bei korelacijų sudarymo nustatymas³⁵.

Glaudesnis skirtingų sektorių reguliavimo institucijų dialogas galėtų išspręsti augantį pasaulinio lygmens partnerystės poreikį. Tokios partnerystės gali kurti bendras atvirųjų duomenų bazes, kuriose galėtų būti pateikiamas duomenų ir idėjų (tokių kaip statistika ir žemėlapiai) srautas. Šiais duomenimis būtų keičiamasi ir prieiga prie jų naudojamosi remiantis visuomenės interesais, patiriant mažiau rizikos dėl priežiūros, kad individai įgautų daugiau įtakos sprendimams, paveikiantiems juos pačius³⁶.

2.2 Atskaitingi valdytojai

Siekiant atskaitomybės būtina įgyvendinti vidines politikas ir įdiegti kontrolės sistemas, kurios užtikrintų atitiktį ir suteiktų atitinkamų įrodymų, ypač nepriklausomoms priežiūros institucijoms.

Skatinome naikinti duomenų apsaugos teisės aktų biurokratiją – mažinti nereikalingos dokumentacijos reikalavimus, kad būtų sudaromos sąlygos atsakingesnėms įmonių iniciatyvoms, kurioms gaires suteiktų duomenų apsaugos institucijos. Siekiant patenkinti pagrįstus individų lūkesčius, būtina taikyti principą, kad asmens duomenys turi būti tvarkomi tik tais metodais, kurie atitinka konkretų jų rinkimo tikslą. Pvz., pasitikėjimą skaitmeninėje rinkoje gali padėti kurti elgesio kodeksai, auditas, sertifikavimas ir naujos kartos sutarčių sąlygos ir įmonėms privalomos taisyklės. Už asmens informacijos tvarkymą atsakingi asmenys turėtų veikti dinamiškiau, aktyviau ir atsisakyti juodosios dėžės principo, lemiančio verslo praktikų slaptumą ir neskaidrumą, tuo pačiu metu iš vartotojų reikalaujant vis didesnio skaidrumo³⁷.

2.3 Privatumą sauganti inžinerija

Žmonijos laimėjimai visada buvo tam tikrų socialinių grupių veiklos ir tam tikrų kontekstų rezultatas, dažnai atspindintis laikotarpio socialines normas³⁸. Vis dėlto technologinių projektų sprendimai neturėtų lemti mūsų visuomenės sąveikų ir bendruomenių struktūros – jie veikia turėtų stiprinti mūsų vertybes ir pagrindines teises.

ES turėtų plėtoti ir skatinti inžinerines technikas ir metodus, leidžiančius įgyvendinti duomenų tvarkymo technologijas, kurias naudojant būtų gerbiamas asmenų orumas ir teisės. Sistemų ir programinės įrangos inžinieriai turi suprasti pritaikytosios privatumo apsaugos principus ir juos sėkmingiau taikyti kurdami naujus produktus ir paslaugas – tai aktualu visiems projektavimo etapams ir visoms technologijoms. Atskaitomybę reikia skatinti nuodugniau ištyrinėjant ir plėtojant metodus ir priemones, užtikrinančias audito tikslumą ir leidžiančias nustatyti valdytojų ir tvarkytojų atitiktį taisyklėms, tokioms kaip kiekvieno asmens duomenų vieneto žymėjimas „metaduomenimis“, apibūdinančiais duomenų apsaugos reikalavimus.

Inžineriniai sprendimai turi suteikti galių asmenims, norintiems apsaugoti savo privatumą ir laisvę pasirenkant anonimiškumą. ES turėtų skatinti asmenybę paslepiančių algoritmų kūrimą ir įgyvendinimą, kad galėtų apsaugoti individus ir sykiu išnaudoti šių duomenų teikiamas prognozavimo galimybes³⁹.

Šiuo metu turime sukurti pagrindą šiems tikslams įgyvendinti – programuotojus ir duomenų apsaugos specialistus, dirbančius įvairiose srityse, paskatinti jungtis į plačius tinklus, tokius kaip Interneto privatumo inžinerijos tinklas (IPEN), kurie padeda skirtingų sričių atstovams sėkmingai keistis idėjomis ir požiūriais.

2.4 Įtakos įgiję individai

„Profesionalių vartotojų“ aplinka

Individai nėra paprasčiausi pasyvūs objektai, kuriuos įstatymai turėtų apsaugoti nuo išnaudojimo. Anksčiau aprašytos skaitmeninės tendencijos suteikia galimybių stiprinti individų vaidmenį. Pavyzdžiui, šiuo metu žmonės turinį bei paslaugas ir naudoja, ir kuria. Todėl galima vis tvirčiau teigti, kad jiems tenka bendra atsakomybė (kartu su paslaugų teikėjais) dėl asmens duomenų tvarkymo, nebent jis vykdomas grynai buitiniams tikslais⁴⁰ (profesionalaus vartotojo koncepcija sukurta siekiant apibūdinti šį plėtros reiškinių⁴¹). Virtualios valiutos vartotojams siūlo anonimiškumą ir galimybę apeiti trečiosios šalies patikrinimą dėl sandorio, todėl sumažėja sandorio, per kurį už prekes ir paslaugas mokama tarpvalstybiniu mastu, kaštai. Kita vertus, tokių valiutų pobūdis – anonimiškumas ir skirtingų jurisdikcijų aprėptis (ar, būtų galima ginčytis, jų stoka) – lemia individų pažeidžiamumą dėl sukčiavimo ir nusikalstamų rinkų, kurias sunku aptikti ir iširti. Pareigų turi ne tik reguliavimo institucijos, įmonės ir inžinieriai – atsakomybė tenka ir piliečiams. Jie turi būti informuoti, atidžiai stebėti ir remtis kritiniu vertinimu, kai priima sprendimus tiek naudodamiesi internetu, tiek juo nesinaudodami⁴².

Sutikimas

Be to, priešingai, nei paprastai manoma, ne visą žmonių elgesį galima paaiškinti ekonominiais principais, kuriais vertinant žmonės yra visiškai racionalūs ir jautrūs ekonominėms paskatoms⁴³. Tai svarbu būsimoms sutikimo, kuriuo asmuo leidžia tvarkyti savo asmeninę informaciją, funkcijoms. Remiantis ES teise, daugeliu tvarkymo atvejų

sutikimas nėra vienintelis teisėtas pagrindas. Nors sutikimo funkcija yra svarbi, ji neatleidžia valdytojų nuo atskaitomybės už tai, ką jie daro su duomenimis – ypač tada, kai gaunamas bendras sutikimas dėl duomenų tvarkymo įvairiais tikslais.

Valdymas ir duomenų „nuosavybė“

Individai turi turėti galimybę kreiptis dėl klaidų ir nesąžiningumo, kylančio dėl algoritmų, naudojamų prielaidoms ir prognozėms nustatyti, logikos. Pavyzdys – JAV atliktame tyrime buvo išnagrinėta beveik 3000 kredito ataskaitų, priklausančių 1000 vartotojų. Nustatyta, kad 26 proc. faktinių klaidų buvo pakankamai rimtos, kad paveiktų vartotojų kredito balus – taigi ir kredito gavimo kainą⁴⁴.

Duomenys dažnai laikomi ištekliais (kaip nafta), kuriais gali būti prekiaujama, pageidautina – tarp vienodai gerai informuotų šalių⁴⁵. Vartotojams nėra sąžiningai atlyginama už jų asmeninę informaciją, kuria prekiaujama, todėl esama duomenų nuosavybės modelio šalininkų. Vis dėlto absoliučią savo asmens duomenų kontrolę užtikrinti sunku – yra ir kitų interesų, pvz., kitų asmenų teisės ir laisvės bei visuomenės interesai. Kontrolė reikalinga, bet jos nepakanka⁴⁶. Vis dėlto žmogaus orumas yra nekintama konstanta. ES teisės aktuose numatyta, kad nuosavybės analogijos negalima taikyti asmeninei informacijai, kuriai būdingas ryšys su konkrečiais asmenimis. ES duomenų apsaugos teisės aktuose nėra nuostatos, leidžiančios asmeniui atsisakyti savo pagrindinių teisių.

Vienas iš alternatyvių metodų, leidžiančių individams geriau valdyti savo duomenis, kitų asmenų prieigą prie jų ir šios prieigos tikslus, galėtų būti asmens duomenų parduotuvės arba „duomenų saugyklos“⁴⁷. Pagal tokios „asmeninės parduotuvės“ koncepciją reikia saugos mechanizmų, užtikrinančių, kad prieiga prie duomenų galėtų pasinaudoti tik duomenų subjekto įgalioti subjektai ir būtų suteikiama tik prieiga prie įgaliojime numatytų dalių. Asmens duomenų parduotuvės būtų efektyviausias sprendimas tais atvejais, kai informacija yra aktuali ir nuolat atnaujinama, pvz., geoerdviniai duomenys ar gyvybiniai požymiai. Taikytinos ne tik techninės apsaugos priemonės – duomenų vartotojai taip pat būtų įpareigoti laikytis duomenų bendrinimo ir naudojimo taisyklių. Konkurencija ir galimybė pakeisti naudojamas paslaugas – pati stipriausia vartotojo galia, galinti paveikti jam prieinamų paslaugų rinką. Ryšio (įskaitant identifikatorius ir kontaktinę informaciją) perkeliavimo užtikrinimas pasirodė esąs galinga paskata konkurencijai. Liberalizavus telekomunikacijų rinką, tai gerokai sumažino vartotojų kainas. Duomenų perkeliavimas – faktinė ir praktinė galimybė didžiąją dalį asmens duomenų perkelti iš vieno paslaugų teikėjo kitam – yra puiki pradžia kurti sąlygas, vartotojui išties suteikiančias galimybę rinktis.

3. Orumas – naujosios skaitmeninės etikos šerdis

Etikos sistema turėtų tapti šios skaitmeninės ekosistemos dalių pamatu. EDAPP manymu, didesnė pagarba žmogaus orumui ir jo apsauga galėtų atsverti įsivyravusią priežiūrą ir įtakos asimetriją, su kuriomis dabar susiduria individas. Tai turėtų būti naujosios skaitmeninės etikos šerdis.

3.1 Orumas ir duomenys

Prasidėjus XVIII ir XIX a. pramonės revoliucijai, judėjimu už žmogaus teises buvo siekiama užtikrinti platesnę socialinę gerovę mažinant pagarbos asmeniui kliūtis. Dabar ES, priėmusi Pagrindinių teisių chartiją ir laikydamosi Visuotinės žmogaus teisių deklaracijos bei Europos žmogaus teisių konvencijos, savo išėities tašku pasirinko žmogaus orumo neliečiamumo

principą. Žmogaus orumas yra ne tik pagrindinė teisė – jis suteikia pagrindą tolesnėms laisvėms ir teisėms, įskaitant teisę į privatumą ir asmens duomenų apsaugą⁴⁸. Vienas iš galimų orumo pažeidimo būdų – žmogų vertinti kaip objektą, įrankį, tarnaujantį kažkieno kito tikslams⁴⁹. Privatumas yra neatsiejama žmogaus orumo dalis. Aštuntajame ir devintajame dešimtmečiuose buvo patvirtinta teisė į duomenų apsaugą kaip galimybė kompensuoti galimus privatumo ir orumo pažeidimus dideliais mastais tvarkant asmens duomenis. Vokietijos konstitucijos 1 ir 2 straipsniuose⁵⁰ išdėstyta teisė į „informacinį apsisprendimą“, pagrįsta teise į asmens orumą ir laisvą asmenybės ugdymą.

Vis dėlto prasidėjus XXI a. asmenims tenka internetu atskleisti vis daugiau asmeninės informacijos, kad galėtų dalyvauti socialiniuose, administraciniuose ir komerciniuose reikaluose. Galimybės išvengti šio atskleidimo dar labiau ribotos. Šiuo metu, kai visa veikla gali vykti internetu, milžiniška reikšmė tenka laisvo ir informuoto sutikimo sąvokai. Kiekvieną minutę nukrenta „skaitmeninių trupinių“, kurie tikroju laiku naudojami individams klasifikuoti ir daugybei (kartais prieštaringų) profilių kurti. Šie profiliai, individams to nežinant, per kelias sekundes dalis gali būti perduoti ir panaudoti kaip pagrindas individus paveikiantiems svarbiems sprendimams.

Žmonių elgesiui numatyti naudojami profiliai kelia stigmatizacijos pavojų, stiprina esamus stereotipus, socialinę ir kultūrinę segregaciją⁵¹ – toks „kolektyvinio proto“ naudojimas kenkia asmeniniam pasirinkimui ir lygioms galimybėms. Tokie „filtrų burbulai“ ir informaciją iškreipiančios sistemos galiausiai pakenkia ir pačiam kūrybiškumui, inovacijoms, saviraiškos laisvei ir jų ryšiui, leidusiam suklestėti skaitmeninėms technologijoms.

O trikdančių, asmenų stebėsenai skirtų technikų skirtingiems sluoksniams įvertinti „saugos“ sumetimais nuolat taikoma išimtis⁵². Norint suprasti tokį „priežiūros“ metodą, reikia įvertinti bendrą ilgalaikį poveikį visuomenei ir elgesiui.

ES su trečiosiomis šalimis turi imtis griežtų veiksmų, kad šios vertybės būtų gerbiamos ne tik popieriuje – jų negalima neutralizuoti internetinėje erdvėje. Ypač dabar ES turi kritinės svarbos galimybę skaitmeninėms struktūroms suteikti vertes, apibrėšiančias mūsų visuomenę, kol šių technologijų dar nepradėjo naudoti visuomenė⁵³. Reikia iš naujo įvertinti, ar naujųjų technologijų galima nauda išties priklauso nuo milijardus asmenų identifikuojančios informacijos surinkimo ir analizės. Toks įvertinimas turėtų paskatinti kurti produktus, kurie tikroju laiku nuasmenintų milžiniškus pavienės informacijos kiekius, kad atpažinti individą būtų sunkiau arba išvis neįmanoma.

Mes jau pripažįstame, kad tam tikrų duomenų (pvz., genetinių) tvarkymą reikia ne tik reglamentuoti, bet ir vertinti atsižvelgiant į platesnius visuomenės interesus. Tai atlikti galėtų etikos komitetai. Pats genetinių duomenų pobūdis lemia, kad jie susiję ne tik su vienu individu, bet ir su jo protėviais bei palikuonimis. Genetiniai duomenys ne tik leidžia nustatyti šeimos ryšius – asmens genų elementai gali suteikti informacijos apie individo tėvus bei vaikus ir lemti sprendimus valdytojų, kurie turi įtakos jų galimybėms netgi iki gimstant. Galima genetinių asmens duomenų koncentracija kelių milžiniškų rinkos dalyvių rankose turi poveikį tiek rinkos ekonomikoms, tiek duomenų subjektams. Auganti priklausomybė nuo pasaulinės nenutrūkstamo duomenų srauto surinkimo ir analizės sistemos gali padidinti visuomenės bei ekonomikos pažeidžiamumą, sukelti precedentų neturinčių saugos sutrikimų ir piktavališkų atakų.

Esama sistema gali žlugti, jei ateities neplanuosime mąstydami novatoriškai. Juntamas vis didesnis poreikis duomenų subjektą traktuoti kaip individą, o ne paprasčiausią vartotoją ar

naudotoją. Išties nepriklausomos asmens duomenų apsaugos institucijos atlieka esminį vaidmenį užkertant kelią ateičiai, kurioje individus apibūdintų algoritmai ir jų tęstinės sekos. Institucijos turi būti pasiruošusios taikyti „rūpestingumo principą“ dėl asmenų ir jų orumo internete. Paprastai į privatumo ir duomenų apsaugos koncepcijas bei principus jau būna įtrauktos etinės subtilybės, susijusios su orumo apsauga tokiose srityse, kaip užimtumas ir sveikata. Tačiau nūdienos tendencijos atvertė visiškai naują skyrių ir reikia ištirti, ar šie principai pakankamai tvirti skaitmeniniam amžiui⁵⁴. Pati asmens duomenų sąvoka turėtų iš esmės pasikeisti, nes technologijos suteikia vis daugiau galimybių asmens tapatybę pakartotinai nustatyti remiantis duomenimis, kurie laikomi anonimiškais. Be to, mašininis mokymasis ir žmogiškojo bei dirbtinio intelekto derinys pakenks asmens teisių ir atsakomybės koncepcijoms.

3.2 Europos patariamoji etikos taryba

Nesiekiamo situaciją atvaizduoti kaip distopiją ir sukelti paniką. Diskusijos jau vyksta įvairioje aplinkoje – teisės, politikos, ekonomikos, socialinių reikalų, mokslo ir netgi religijos⁵⁵. Paprasti metodai, kurie suteikia vienašališkų pranašumų dėl ekonominio pelno ar saugos tikslais vykdomos priežiūros, veikiausiai nėra naudingesni nei pernelyg suvaržantis ir inovacijas bei pažangą stabdantis esamų įstatymų taikymas. Todėl EDAPP siūlo išsamią, plačią, skirtingas sritis apimančią analizę, kuri suteikia rekomendacijų ir informatyviai papildo socialinę diskusiją apie tai, kaip demokratinė visuomenė turėtų spręsti technologijų iššūki.

EDAPP strategija⁵⁶ siekiama sukurti etinį požiūrį į duomenų apsaugą, patvirtinantį, kad „įmanomumas įgyvendinti, nauda ar pelningumas nėra tolygūs tvarumui“, ir pabrėžiantį „mechaninės atitikties įstatymams atskaitomybę“. Mes siekiame paveikti ne tik ES pareigūnų, teisininkų ir IT specialistų bendruomenę – norime, kad mus išgirstų ir garsūs asmenys, galintys įvertinti technologinių pokyčių ir reguliavimo institucijų atsako vidutinės trukmės ir ilgalaikį poveikį. Per ateinančius mėnesius mūsų nepriklausoma institucija inicijuos išorės patariamąją grupę duomenų apsaugos etinio aspekto klausimais. Tai padės ištyrinėti ryšius tarp XXI a. žmogaus teisių, technologijų, rinkų ir verslo modelių.

Mūsų patariamąją etikos tarybą sudarys rinktinė ekspertų grupė. Jos nariai – etikos ir filosofijos, sociologijos, psichologijos, technologijų ir ekonomikos specialistai. Jiems padės papildomi ekspertai, turintys žinių ir kompetencijų tokiose srityse, kaip sveikata, transportas ir energetika, socialinė sąveika ir žiniasklaida, ekonomika ir finansai, valdymas ir demokratija, saugumas ir policija. Juos pakviesime plačiau apsvarstyti asmens duomenų rinkimo ir naudojimo etinius aspektus, o svarstymai bus kaip galima skaidresni.

4. Išvada: laikas skatinti gilesnes diskusijas

Privatumas ir duomenų apsauga yra sprendimo, o ne problemos dalis. Šiuo metu technologijas valdo žmonės. Nėra lengva potencialias plėtros tendencijas griežtai suskirstyti į blogas ar geras, pageidaujamas ar kenksmingas, naudingas ar žalingas, ypač kai platesniame kontekste matoma ne viena galima tendencija. Politikai, technologijų kūrėjai, verslininkai ir mes visi privalome rimtai apsvarstyti, ar norime paveikti technologijų raidą bei jų taikymą ir kaip tai padaryti. Vis dėlto vienodai svarbu ir tai, kad ES nedelsdama apsvarstyta, kokią reikšmę etiniai aspektai ir žmogaus orumas turės kuriant ateities technologijas.

Jau pasitvirtino, kad duomenų apsaugos principai gali apsaugoti individus ir jų privatumą nuo neatsakingo duomenų tvarkymo keliamų pavojų. Vis dėlto į nūdienos tendencijas būtina

pažvelgti iš naujo. Mes pradame naujas diskusijas apie tai, koku mastu pakanka taikyti sąžiningumo ir teisėtumo principus. Duomenų apsaugos bendruomenė gali atlikti naują vaidmenį naudodama jau turimas priemones, pavyzdžiui, išankstinius patikrinimus ir įgaliojimus, nes jokia kita institucija neturi priemonių stebėti tokį duomenų tvarkymą. Technologijoms, pasaulinėms inovacijoms ir žmonių ryšiams plėtojantis stulbinamu greičiu, mes turime galimybę atkreipti dėmesį, sukelti susidomėjimą ir pasiekti bendrą sutarimą.

Šia nuomone tikimės suteikti pagrindą platesnėms ir išsamesnėms diskusijoms apie tai, kaip ES gali užtikrinti savo vertybių neliečiamumą ir kartu pasinaudoti naujų technologijų teikiama nauda.

Priimta Briuselyje 2015 m. rugsėjo 11 d.

(pasirašyta)

Giovanni BUTTARELLI
Europos duomenų apsaugos priežiūros pareigūnas

Pastabos

¹ Šaltinis: „GSMA Intelligence“.

² Pasirodė, jog Moore'o dėsnis, kad mikroschemoje galimų įmontuoti tranzistorių skaičius kas 18 mėnesių padvigubėja, iš esmės yra teisingas; Moore, Gordon E. (1965-04-19), „Cramming more components onto integrated circuits“, „Electronics“, 2011-08-22.

³ Nathan Eagle, Alex (Sandy) Pentland, „Reality mining: sensing complex social systems“, „Journal Personal and Ubiquitous Computing“, T. 10, Nr. 4, 2006 m. kovo mėn., p. 255–268. Shoshana Zuboff straipsnyje „Big Other: surveillance capitalism and the prospects of an information civilization“ („Journal of Information Technology“, 2015 m., Nr. 30, p. 75–89) rašo: „Kompiuteriai naudojami kaip tarpininkai. Tai lemia, kad beveik kiekvienas mūsų pasaulio aspektas paverčiamas nauju simbolių matmeniu – įvykiai, objektai, procesai ir žmonės tampa matomi, žinomi ir bendrinami nauju būdu.“ Zuboff numato „naujos universalios architektūros susiformavimą“, kurį ji vadina Didžiuoju Kitu („Big Other“). „Tai visuotinis į tinklą sujungtų institucijų režimas, kuris įrašo, keičia ir sudaiktina kiekvieną kasdienę patirtį: nuo skrudintuvo iki kūno, nuo bendravimo iki minties. Visa tai daroma siekiant atverti naujus kelius į piniginę naudą ir pelną“; p. 77, 81.

⁴ „BBC Micro Bit computer's final design revealed“, 2015-07-07, <http://www.bbc.com/news/technology-33409311> (žiūrėta 2015-09-10); „No assembler required: How to teach computer science in nursery school“, „The Economist“, 2015-08-01.

⁵ Nė viena iš dešimties stipriausių (pagal rinkos kapitalizaciją) technologijų sektoriaus įmonių nėra įsikūrusi ES – dešimtuką sudaro aštuonios JAV, viena Kinijos ir viena Taivano įmonė (šie duomenys paskelbti 2015 m. kovo 31 d. atnaujintame PWC pasaulio įmonių dešimtuکه pagal rinkos kapitalizaciją) („Global Top Ten Companies by Market Capitalisation, 31 March 2015 Update“).

⁶ „Dideli duomenų rinkiniai reiškia eksponentinį augimą – tiek informacijos prieinamumo, tiek automatinio jos naudojimo aspektu. T. y. įmonės, vyriausybės ir kitos stambios organizacijos kaupia milžiniškus skaitmeninius duomenų rinkinius, kurie vėliau intensyviai analizuojami naudojant kompiuterio algoritmus“; (WP29 nuomonė Nr. 3/2013 dėl tikslo apribojimo). 2014 m. Baltųjų Rūmų ataskaitoje dideli duomenų rinkiniai apibūdinti kaip „augantis technologinis gebėjimas vis greičiau užfiksuoti, kaupti ir tvarkyti vis didesnius kiekius vis įvairesnių duomenų“; žr. „Big Data: Seizing Opportunities, Preserving Values“, Executive Office of the President („Podesta“ ataskaita), 2014 m. gegužė.

⁷ ES teisės aktuose „asmens duomenys“ apibrėžiami kaip „bet kuri informacija, susijusi su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta; asmuo, kurio tapatybė gali būti nustatyta, yra tas asmuo, kurio tapatybė gali būti nustatyta tiesiogiai ar netiesiogiai, ypač pasinaudojus nurodytu asmens kodu arba vienu ar keliais to asmens fizinei, fiziologinei, protinei, ekonominei, kultūrinei ar socialinei tapatybei būdingais veiksniais“; Direktyvos 95/46/EB 2 straipsnio a punktą. Ši apibrėžtis iš esmės panaši į kitas apibrėžtis – Europos Tarybos patvirtintą Konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (vadinamoje Konvencija Nr. 108) ir pateiktą EBPO gairėse dėl privatumo apsaugos ir tarptautinio asmens duomenų judėjimo. Išsamią analizę žr. 29 straipsnio darbo grupės nuomonėje Nr. 4/2007 dėl asmens duomenų koncepcijos, WP136.

⁸ Žr., pvz., Jungtinių Amerikos Valstijų federalinės prekybos komisijos pirmininkės kalbą, pasakytą 2014 m.: „Prietaisų, kuriuose naudojamas internetas, gausėjimas, informacijos rinkimo, laikymo ir tvarkymo kaštų mažėjimas ir duomenų tarpininkų bei kitų subjektų gebėjimas suderinti neinternetinius ir internetinius duomenis reiškia, kad įmonės gali surinkti praktiškai neribotus vartotojų informacijos kiekius ir juos laikyti neribotą laiką. Naudodamos prognozuojamąją analizę, apie kiekvieną iš mūsų jos gali sužinoti neįtikėtinai daug.“ (FTC pirmininkės Edith Ramirez atidarymo kalba „Big Data: A Tool for Inclusion or Exclusion?“, Vašingtonas, 2014 m. rugsėjo 15 d. Pasak Sandy Pentland, „socialinė fizika yra kiekybinis socialinis mokslas, apibūdinantis patikimus,

matematinis ryšius tarp informacijos ir, viena vertus, idėjų srauto, antra vertus, žmonių elgesio... Ji leidžia mums numatyti mažų grupių, įmonių skyrių ar netgi išties miestų produktyvumą“. Būtent to reikia norint sukurti geresnes socialines sistemas (p. 4, 7) ir „suteikti galimybę (vyriausybės pareigūnams, pramonės vadovams ir piliečiams) naudoti socialinių tinklų paskatas – priemones, leidžiančias kurti naujas elgesio normas“ (p. 189) (pasviruoju šriftu išryškino mes) (Pentland, „*Social Physics: How Good Ideas Spread: The Lessons from a New Science*“.

⁹ „Special Eurobarometer 431 on Data Protection“, 2015 m. birželis, ir „Pew Research Panel Survey January 2014 on Public Perceptions of Privacy and Security in the Post-Snowden Era“. Kaip atskleidė vienas tyrimas, vidutiniškai per apsilankymą vienoje interneto svetainėje atliekami 56 duomenų rinkimo veiksmai (Julia Angwin „*Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*“, 2012 m.). 2014 m. Baltųjų Rūmų ataskaitoje dėl didelių duomenų rinkinių teigiama, kad „precedentų neturinti kompiuterijos įtaka ir sudėtingumas... sukūrė jėgų asimetriją tarp tų, kurie kaupia duomenis, ir tų, kurie tikslingai arba per neapsižiūrėjimą juos teikia“; „vienas iš esminių šioje apžvalgoje atskleistų iššūkių susijęs su faktu, jog didelių duomenų rinkinių analizė gali... sukurti tokią neskaidrią sprendimų priėmimo aplinką, kad asmens autonomiškumas pradingsta nesuvokiamame algoritmų rinkinyje“.

¹⁰ Naudojant 1990 m. atlikto gyventojų surašymo viešuosius asmeninius duomenis, 87 proc. JAV gyventojų būtų galima nustatyti pagal penkių skaitmenų pašto kodą, lytį ir gimimo datą; žr. Paul Ohm, „Broken promises of privacy: responding to the surprising failure of anonymisation“, „*UCLA Law Review*“, 2010 m., ir „Record linkage and privacy: issues in creating new federal research and statistical info“, 2011 m. balandis. DNR yra unikali (išskyrus identiškų dvynių atvejus) ir išlieka nepakitusi visą gyvenimą. Joje slypi informacija apie etninę kilmę ir polinkį į ligas. Pagal DNR galima nustatyti kitus šeimos narius. 2013 m. sausio mėn. tyrėjams pavyko nustatyti asmenų ir jų šeimų tapatybę pagal anoniminius DNR duomenis, pateiktus viešai prieinamose genealogijos duomenų bazėse; Gymrek, M., McGuire, A. L., Golan, D., Halperin, E., ir Erlich, Y. „*Science*“, Nr. 339, p. 321–324 (2013 m.). Taip pat žr. „Poorly anonymized logs reveal NYC cab drivers’ detailed whereabouts“, 2014-06-23 <http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/> (žiūrėta 2015-09-10). Taip pat žr. WP29 nuomonę Nr. 04/2007 dėl asmens duomenų koncepcijos; WP29 nuomonę Nr. 03/2013 dėl tikslo ribojimo; WP29 nuomonę Nr. 06/2013 dėl atvirųjų duomenų ir viešojo sektoriaus informacijos pakartotinio naudojimo; WP29 nuomonę Nr. 05/2014 dėl anonimiškumo.

¹¹ Šaltinis: Gartner.

¹² Pvz., žr. viešąją diskusiją „What is the future of official statistics in the Big Data era?“, „Royal Statistical Society“, Londonas, 2015 m. sausio 19 d.; <http://www.odi.org/events/4068-future-official-statistics-big-data-era> (žiūrėta 2015-09-10).

¹³ „Ten technologies which could change our lives: potential impacts and policy implications“, Scientific Foresight Unit, European Parliamentary Research Service, 2015 m. sausis.

¹⁴ Ši plėtra remiama pagal ES programos „Horizontas 2020“ 2016–2017 m. darbo programą. Be to, rengiami plataus masto bandomieji projektai, skirti privatumui ir etiniams klausimams įvertinti.

¹⁵ Draudimas apibūdinamas kaip „prigimtinis daiktų interneto verslo modelis“; „From fitness trackers to drones, how the ‘Internet of Things’ is transforming the insurance industry“, „*Business Insider*“ (2015-06-11). SESV 102 straipsnyje, kuriuo draudžiamas dominavimas rinkoje taikant „nesąžiningų pirkimo ar pardavimo kainų arba kokių nors kitų nesąžiningų prekybos sąlygų tiesioginių ar netiesioginių nustatymą“, pavartotas konkurencijos teisės terminas „diskriminacija kainomis“. Jis ypač ginčytinas, žr. Damien Gerardin ir Nicolas Petit, „Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting Principles“ (2005 m. liepa), „*Global Competition Law Centre Working Paper Series*“, Nr. 07/05. Apie didelius duomenų rinkinius ir jų (anot autorių, kol kas neišnaudotą) potencialą skatinti kainų suasmeninimą žr. Executive Office of the President of the United States, „Big Data and Differential Pricing“ (2015 m. vasaris). Taip pat žr. neseniai atliktą analizę, kurios išvadose teigiama, jog kainų suasmeninimas iš esmės apima asmens duomenų

tvarkymą, todėl jam turi būti taikomas duomenų apsaugos teisės skaidrumo principas, pagal kurį reikalaujama, kad įmonės žmonės informuotų apie jų asmens duomenų tvarkymo tikslą – įmonės turi nurodyti, kad šis tikslas yra kainų suasmeninimas. Be to, jeigu įmonė, siekdama atpažinti asmenį, naudoja slapuką, pagal Elektroninio privatumo direktyvą reikalaujama, kad tokia įmonė informuotų asmenį apie slapuko tikslą (Frederik Borgesius darbinis projektas „Online Price Discrimination and Data Protection Law“. Pateikiama http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665 (žiūrėta 2015-09-10).

¹⁶ ES teisėje vartojama medicinos prietaisų sąvokos apibrėžtis pateikiama Tarybos direktyvoje 93/42/EEB dėl medicinos prietaisų, iš dalies pakeistoje 2007 m. rugsėjo 5 d. Europos Parlamento ir Tarybos direktyva 2007/47/EB. Apie duomenų apsaugos taikymą „mobiliesios sveikatos“ srityje žr. EDAPP nuomonėje Nr. 1/2015.

¹⁷ Eurostato duomenimis, ES debesijos kompiuterijos saugyklų paslaugomis naudojami 21 proc. individų ir 19 proc. įmonių.

¹⁸ „Jeigu pasaulinio masto internetas būtų valstybė, pagal elektros suvartojimą jis atsidurtų dvyliktoje vietoje – kažkur tarp Ispanijos ir Italijos. Tai sudaro maždaug 1,1–1,5 proc. bendro pasaulinio elektros suvartojimo (2010 m. duomenimis). Šiltnamio efektą sukeliančių dujų kasmet išskiriama tiek, kiek jų išskiria 70–90 stambių (500 megavatų) elektra kūrenamų jėgainių.“ Gamtos išteklių gynybos taryba, Duomenų centro efektyvumo įvertinimas „Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers“, 2014 m.

¹⁹ Tyrimo „SMART 2013/0043 - Uptake of Cloud in Europe“ ataskaita.

²⁰ Šaltinis: Eurostatas.

²¹ Terminas „dalijimosi ekonomika“ sulaukia kritikos dėl klaidinimo: „The Sharing Economy Isn't About Sharing at All“, Giana M. Eckhardt ir Fleura Bardhi, „Harvard Business Review“, 2015-01-28.

²² Rachel Botsman ir Roo Rogers, „*What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*“, 2011 m.

²³ „Future of Privacy Forum“, „User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy“, 2015 m. birželio mėn.

²⁴ Žr. 2015 m. birželio 9 d. JAV Federalinės prekybos komisijos seminarą „Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy“, <https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/> (žiūrėta 2015-09-10).

²⁵ Apie duomenų apsaugos taikymą bepiločiams orlaiviams ar nuotoliniu būdu valdomoms orlaivių sistemoms žr. EDAPP nuomonėje dėl Komisijos komunikato Europos Parlamentui ir Tarybai „Nauja aviacijos era. Aviacijos rinkos atvėrimas saugiai ir tvariai civiliniais tikslais naudojamoms nuotolinio valdymo orlaivių sistemoms“ (2014 m. lapkritis).

²⁶ Šaltinis: „Boston Consulting Group“.

²⁷ Gartner.

²⁸ „Facebook DeepFace“ veido atpažinties algoritmas sėkmingai veikia 97 proc. atvejų – t. y. jis tikslesnis nei žmogus; „DeepFace: Closing the Gap to Human-Level Performance in Face Verification“, paskelbta „EEE Conference on Computer Vision and Pattern recognition“ (2014 m. birželis) ataskaitoje.

²⁹ Sąvoka „robotas“ apibrėžiama kaip „pasaulyje esantis įrenginys, kuris jaučia, mąsto ir veikia“; Bekey, G., „Current trends in robotics: technology and ethics“, leidinyje „Robot Ethics - The ethical and social implications of robotics“, „The MIT Press2“, 2012 m., p. 18. Numatyta, kad nuo 2013 iki 2016 m. bus parduota 22 mln. paslaugas teikiančių robotų; „IRF World Robotics Report“, 2013 m. Apie dirbtinį intelektą žr. „Rise of the Machines“, „Economist“, 2015-05-09, ir „Pew Research Centre

Internet Project“, 2014 m. 2014 m. pirmaujanti technologijų įmonė įsigijo dirbtinio intelekto srities įmonę – su sąlyga, kad bus inicijuota etikos ir saugos taryba ir laikomasi draudimo dirbtinį intelektą naudoti kariniais arba žvalgybos tikslais; „Forbes“, „Inside Google's Mysterious Ethics Board,“ 2014-02-03.

³⁰ Pentland, „*Social physics*“, p. 147.

³¹ Žr. pirmiau pateiktą 9 pastabą. Pentland, „*Social Physics*“, p. 153. „Sveikatos apsaugos, transporto, energetikos ir saugumo srityse galime pasiekti milžinišką pažangą... pagrindinės kliūtys siekti šių tikslų – tai nerimas dėl privatumo ir faktas, kad dar nesame pasiekę susitarimo dėl asmeninės ir socialinės vertės suderinimo.“ Debatai dėl 2014 m. Ebolos viruso pandemijos Vakarų Afrikoje atskleidžia, kaip brėžiama ši klaidinga atskirtis tarp asmeninio privatumo ir visuomenės poreikių. Ligoms sekti ir jų ilgalaikiškumui vertinti įprasta naudoti apklausas ir surašymus, tačiau tokie duomenys greitai pasensta ir juos sunku ekstrapoliuoti siekiant nustatyti, kur įvyks kitas proveržis. Didelių duomenų rinkiniai buvo naudojami siekiant sekti maliarijos proveržį Namibijoje ir Kenijoje, o 2009 m. per Meksikos kiaulių gripo krizę vyriausybės išpėjimų dėl sveikatos efektyvumui stebėti. Vienas iš duomenų šaltinių – skambučių mobiliuoju telefonu įrašai. Jie atskleidžia, kurioje bazinėje stotyje buvo apdorojamas skambutis, ir tikroju laiku gali suteikti informacijos apie apytikslę žmonių buvimo vietą ir judėjimo kryptį. Tokių įrašų rinkimas nėra tikslinis – jis nepadedą atskirti, kurie asmenys užsikrėtę Ebola. Švedijos ne pelno organizacija sudarė Vakarų Afrikos gyventojų judėjimo planą, tačiau jo duomenimis nebuvo pasinaudota – mobiliojo ryšio operatoriai prieigos prie šių duomenų patvirtintiems išorės tyrėjams nesuteikė. Savo sprendimą jie argumentavo tuo, kad turėjo gauti vyriausybės nurodymus, o vyriausybė savo ruožtu minėjo susirūpinimą dėl privatumo, kurio nebūtų buvę galima garantuoti pagal ES įstatymus; <http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola> (žiūrėta 2015-09-10).

³² EDAPP nuomonė Nr. 3/2015.

³³ Didelių duomenų rinkinių prielaida, kad „N = visi“, reiškia visų duomenų, o ne vieno jų pavyzdžio vertinimą: Viktor Mayer-Schönberger ir Kenneth Cukier, „*The Rise of Big Data: How it's changing the way we think about the world*“ (2013 m.). Lisabonos tarybos ir pažangios politikos instituto teigimu, klestėjimą sustiprins maksimalus „skaitmeninis tankis“ – „vienam asmeniui tenkančių naudojamų duomenų kiekis ekonomikoje“. <http://www.lisboncouncil.net/component/downloads/?id=1178> (žiūrėta 2015-09-10). Tarptautinė darbo grupė dėl duomenų apsaugos telekomunikacijų srityje (vadinama Berlyno grupe) pasiūlė didelių duomenų rinkinių atveju atsitraukti nuo duomenų apsaugos principų; http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf (žiūrėta 2015-09-10). Pasaulio ekonomikos forumas pakvietė susitelkti ne į rinkimą, o į naudojimą ir atsisakyti reikalavimo pateikti sutikimą dėl asmens duomenų rinkimo; „Unlocking the Value of Personal Data: From Collection to Usage“, 2013 m.

³⁴ Žr. EDAPP pirminę nuomonę dėl privatumo ir konkurencingumo didelių duomenų rinkinių amžiuje.

³⁵ Pagrindinių teisių chartijos 21 straipsniu draudžiama „bet kokia diskriminacija <...> dėl asmens lyties, rasės, odos spalvos, tautinės ar socialinės kilmės, genetinių bruožų, kalbos, religijos ar tikėjimo, politinių ar kitokių pažiūrų, priklausymo tautinei mažumai, turtinės padėties, gimimo, negalios, amžiaus, seksualinės orientacijos“. Daugeliui šių duomenų kategorijų („susijusių su rasine ar etnine kilme, politiniais, religiniais ir filosofiniais įsitikinimais, naryste profesinėje sąjungoje, taip pat informacijai apie asmens sveikatą ar intymų gyvenimą“) taikoma sustiprinta apsauga pagal Direktyvos 95/46/EB 8 straipsnį.

³⁶ Apie idėją dėl bendrų skaitmeninių duomenų bazių žr. „Ambition numérique: „Pour une politique française et européenne de la transition numérique“, Prancūzijos skaitmeninė taryba, 2015 m. birželis, p. 276; Bruce Schneier skatina internete kurti „niekam nepriklausančias viešąsias erdves“ – kaip viešuosius parkus; „*Data and Goliath*“, p. 188–189; Sandy Pentland yra už „bendras viešųjų duomenų bazes“, „*Social Physics*“, p. 179. Informaciją apie surinktų duomenų rinkinių viešinimo

(kaip atvirųjų duomenų) saugumo įvertinimą žr. WP29 nuomonėje Nr. 06/2013 dėl atvirųjų duomenų ir viešojo sektoriaus informacijos pakartotinio naudojimo.

³⁷ „Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent“ <http://crackedlabs.org/studie-kommerzielle-ueberwachung/info>. Apie kokybišką skaidrumą žr., pvz., Frank Pasquale, „*The Black Box Society: The Secret Algorithms that Control Money and Information*“.

³⁸ „Už technologijų, kurios veikia mūsų socialinius santykius, slypi tie patys socialiniai santykiai“; David Noble, „Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools“, paskelbta leidinyje „*Case Studies in the Labor Process*“, red. Andrew Zimbalist, 1979 m. Taip pat žr. Judy Wajzman, „*Pressed for Time: The Acceleration of Life in Digital Capitalism*“, 2014 m., p. 89–90; ir Zuboff, „Big Other“ (citata 3 pastaboje).

³⁹ Nuomonė Nr. 05/2014 dėl anonimiškumo metodų, priimta 2014 m. balandžio 10 d. (WP 216.)

⁴⁰ Apie siauriai apibrėžtą duomenų apsaugos taisyklių netaikymą grynai asmeninių ar buitinių tikslų atveju žr. ESTT sprendime byloje C-212/13 *František Ryneš / Úřad pro ochranu osobních údajů*.

⁴¹ Terminą „profesionalus vartotojas“ pirmasis pavartojo Alvin Toffler darbe „*The Third Wave*“, 1980 m. Diskusiją apie „profesionalių vartotojų aplinką“ ir jos reguliavimą žr. Ian Brown ir Chris Marsden, „*Regulating Code*“, 2013 m.

⁴² Europos Komisijai skirta Europos mokslo ir naujų technologijų etikos grupės nuomonė „*Ethics of Security and Surveillance Technologies*“, nuomonė Nr. 28, 2015-05-20, p. 74.

⁴³ Pz., žr. „*Homer Economicus: The Simpsons and Economics*“, red. Joshua Hall, 2014 m.

⁴⁴ Taikant nuosaikiausią klaidos apibrėžtį, tai reiškia, kad faktinių klaidų yra 23 mln. amerikiečių vartotojų ataskaitose. Penkių procentų tyrimo dalyvių ataskaitose buvo klaidų, kurias ištaisius kredito balai išaugo, todėl kreditą buvo galima gauti už mažesnę kainą; Federal Trade Commission, „*Report To Congress Under Section 319 Of The Fair And Accurate Credit Transactions Act Of 2003*“, 2012 m. gruodis; Chris Jay Hoofnagle, „*How the Fair Credit Reporting Act Regulates Big Data*“ (2013 m. rugsėjo 10 d.). „*Future of Privacy Forum Workshop on Big Data and Privacy: Making Ends Meet*“, 2013 m. Pateikiama SSRN: <http://ssrn.com/abstract=2432955>.

⁴⁵ WEF duomenis traktuoja kaip vertingą asmens turtą. Teisės į šio turto turėjimą, naudojimą ir platinimą gali būti suteiktos įmonėms ir vyriausybėms mainais už paslaugas. Taip pat žr. neseniai pasakytas Komisijos pirmininko pavaduotojo Ansipo kalbas, pvz., 2015-09-07 „Bruegel“ metiniame susirinkime nuskambėjusią kalbą „*Productivity, innovation and digitalisation - which global policy challenges?*“: „Duomenų srautų nuosavybė ir valdymas, duomenų naudojimas ir pakartotinis naudojimas. Duomenų valdymas ir laikymas. Šiais elementais grindžiami svarbiausi besiformuojantys sektoriai, tokie kaip debesijos kompiuterija, daiktų internetas ir dideli duomenų rinkiniai.“

⁴⁶ „Tad kam priklauso teisė naudoti informaciją ir duomenis, kurie išties nepriklauso patys sau? Tai klausimas, peržengiantis prekybos, etikos ir moralės ribas ir kviečiantis svarstyti privatumo ir privatumo apsaugos klausimus“; Al-Khouri, 2012 m. lapkritis, http://www.academia.edu/6726887/Data_Owner_ship_Who_Owns_My_Data_036. Taip pat žr. Margaret Jane Radin, „*Incomplete Commodification in the Computerized World*“, paskelbtą leidinyje „*The Commodification of Information*“, Nr. 3 (17), red. Niva Elkin-Koren ir Neil Weinstock Netanel., 2002 m.: „Esama skirtumo, kaip privatumas vertinamas – kaip žmogaus teisė, jam tenkanti dėl žmogiškosios prigimties, ar nuosavybės teisė, t. y. tai, ką žmonės gali turėti ir kontroliuoti. Rinka negali pretenduoti į žmogaus teises, tačiau gali pretenduoti į nuosavybės teises.“

⁴⁷ Kelių ES įsikūrusių įmonių remiamo projekto „MIT Computer Science and Artificial Intelligence Lab's Crosscloud“ tikslai: „1) supaprastinti keliems naudotojams skirtos (socialinės) programinės įrangos kūrimą naudojant tik „front-end“ metodą ir gerbiant vartotojų teises bei privatumą; 2) suteikti vartotojams laisvę lengvai judėti tarp programų, aparatinės įrangos platformų ir socialinių tinklų,

išsaugant savo duomenis ir socialinius ryšius“; <http://openpds.media.mit.edu/#architecture> (žiūrėta 2015-09-10).

⁴⁸ Žr. Pagrindinių teisių chartijos 1 straipsnio paaiškinimą.

⁴⁹ Martha Nussbaum, „Objectification“, leidinyje „Philosophy and Public Affairs“ Nr. 24 (4), 1995 m.

⁵⁰ 1983 m. gruodžio 15 d. sprendimas, BVerfGE 65, 1-71, Volkszählung.

⁵¹ Žr. European Group on Ethics in Science and New Technologies, „Opinion on Ethics and Surveillance“, p. 75. Tyrimas atskleidė, kad tikslinių reklamų algoritmui būdingas diskriminavimas. Lankantis darbo skelbimų svetainėse, geriau apmokamo darbo skelbimai vyrams buvo pakartotinai rodomi dažniau nei moterims; Carnegie Mellon universitetas ir Tarptautinis kompiuterių mokslo institutas. Apie tendencijas skaitmeninėms pagalbos programoms nesvarsčius suteikti moterišką balsą žr. Judy Wajcman, „Feminist theories of technology“. „Cambridge Journal of Economics“, Nr. 34 (1), p. 143–152, 2010 m.

⁵² Giorgio Agamben, „*State of Exeption*“, 2005 m.

⁵³ Neil Richards, Neil ir Jonathan King, „Big Data Ethics“ (2014 m. gegužės 19 d.), „Wake Forest Law Review“, 2014 m.

⁵⁴ BBC, „Information watchdog investigates ‘charity data sales‘, 2015-09-01.

⁵⁵ Žr. „Future of Life Institute“ laišką. Popiežiaus enciklika „*Laudato Si*“: „įsivyravusios medijos ir skaitmeninis pasaulis gali paveikti žmones ir nebeleisti jiems mokytis išmintingai gyventi, giliai mąstyti ir dosniai mylėti. Susiklosčius tokioms aplinkybėms, informacijos pertekliaus triukšmas gali sutrukdyti išgirsti praeityje sukauptą išmintį. Reikia stengtis, kad šios medijos taptų naujos žmonijos kultūrinės pažangos šaltiniais, o ne pavojumi giliausiems mūsų turtams. Tikroji išmintis – savianalizė, dialogų ir gilios žmonių sąveikos vaisius – nesukuriama paprasčiausiai renkant duomenis. Duomenų rinkimas galiausiai lemia perteklių ir maišatį, tam tikrą proto taršą. Tikrus santykius su kitais žmonėmis (ir visus iššūkius, su kuriais susiduriame bendraudami), keičia bendravimas internetu, leidžiantis mums vadovautis savo užgaidomis ir kurti arba atsisakyti santykių – taip sukuriamos naujo pobūdžio dirbtinės emocijos, glaudžiau susijusios su įrenginiais ir ekranais nei su kitais žmonėmis ir gamta. Dabartinės medijos mums suteikia galimybę bendrauti ir dalytis savo žiniomis bei jausmais. Vis dėlto kartais jos mus apsaugo nuo tiesioginio sąlyčio su skausmu, baimėmis ir mėgavimusi kitais bei sudėtingomis jų asmeninėmis patirtimis. Todėl turėtume nepamiršti, kad medijos siūlo ne tik jaudinančias galimybes – jos gali paskatinti ir gilų, melancholišką nepasitenkinimą asmeniniais santykiais arba žalingą izoliacijos pojūtį.“

⁵⁶ Žr. 2015–2020 m. EDAPP strategijos 4 veiksmą dėl duomenų apsaugos etinio aspekto kūrimo.