TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Avaliku õiguse osakond

Marily Sillart

TEHISINTELLEKTIL PÕHINEVAD AUTOMATISEERITUD OTSUSED: ISIKUANDMETE KAITSE ÜLDMÄÄRUSE (GDPR) RAKENDAMISE PROBLEEMID JA LAHENDUSED

Magistritöö

Juhendaja
dr. iur. Mario Rosentau

Tartu 2025

SISUKORD

SISSEJUHATUS

Automatiseeritud otsuste tegemine on digitaalses ühiskonnas üha levinum, kuna suurandmed ja tehisintellekt võimaldavad kiiret ja tõhusat andmetöötlust. See mitte ainult ei paranda andmetöötlusprotsesside efektiivsust ja ei vähenda ressursikulu, vaid võimaldab ka teenuseid ja tooteid paremini isikupärastada. Seetõttu kasutatakse automatiseeritud otsuseid järjest enam erinevates valdkondades, pakkudes tõhusamaid ja kasutajate vajadustele paremini kohandatud teenuseid, ent samal ajal toovad kaasa ka uusi andmekaitse- ja läbipaistvusriske.[1]

Kuigi automatiseeritud otsused pakuvad mitmeid eeliseid, kaasnevad nendega ka märkimisväärsed riskid üksikisikute õigustele ja vabadustele. Sellised otsused võivad oluliselt mõjutada inimeste elu, tuues kaasa õiguslikke või muid olulisi tagajärgi. Näiteks kasutatakse neid laenutaotluste heakskiitmisel või tagasilükkamisel ning töölevõtu protsessides, mis võib mõjutada inimeste majanduslikku ja sotsiaalset olukorda.[2] Samal ajal tekivad ka õiguslikud ja eetilised väljakutsed, nagu läbipaistvuse tagamine, diskrimineerimise vältimine ja isikuandmete kaitse.

Suurandmete esiletõus on laiendanud nii tehisintellekti võimekust kui ka selle keerukust. Digitaalse teabe hulk, töötlemise kiirus ja mitmekesisus on saavutanud enneolematu taseme. Samal ajal on meie suutlikkus mõista keerukate tehinsintellekti mudelite sisemist toimimist endiselt piiratud, mis tekitab tõsiseid väljakutseid nii kasutajatele kui ka reguleerivatele asutustele.[3]

Kuna tehisintellektil põhinevad otsustusprotsessid võivad olla läbipaistmatud, ei pruugi inimesed olla teadlikud, et nende andmeid kasutatakse automatiseeritud otsustamiseks või profiilianalüüsiks, ega mõista selle võimalikke tagajärgi. Lisaks võib profiilianalüüs süvendada stereotüüpe ja sotsiaalset segregatsiooni, piirates inimese valikuvabadust ning lukustades teda kindlatesse kategooriatesse. Ebatäpsed ennustused võivad viia teenuste ja kaupade kättesaadavuse piiramisele või põhjendamatu diskrimineerimiseni.[4] Seetõttu on

[1] European Data Protection Board (EDPB). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251 rev.01, endorsed by the EDPB on 6 July 2018, initially adopted by the Article 29 Working Party in 2018.
[2] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, isikuandmete kaitse üldmäärus (*General Data Protection Regulation*, edaspidi GDPR), põhjenduspunkt 71.
[3] Chaudhary, G. Unveiling the Black Box: Bringing Algorithmic Transparency to AI. – Masaryk University Journal of Law and Technology 2024, Vol. 18 No. 1, lk 93jj.
[4] EDPB 2018, Guidelines on ADM and Profiling, lk 5-6.

Euroopa Liit reguleerinud automatiseeritud otsuseid isikuandmete kaitse üldmääruses (General Data Protection Regulation, edaspidi GDPR) mitmete põhimõtete kaudu, mille eesmärk on kaitsta üksikisikute õigusi ja vabadusi.

Siiski ilmnevad GDPRi rakendamisel praktikas mitmed probleemid. Ühelt poolt on küsimus selles, kuidas tagada läbipaistvus ja õiguste kaitse keerukate tehisintellekti üsteemide puhul. Teiselt poolt vajavad lahendamist olukorrad, kus isik leiab, et tema andmeid on profiilianalüüsi käigus kasutatud ebaõiglaselt või tema õigusi on rikutud. Lisaks on väljakutseks andmetöötlejate järelevalvemehhanismide tõhusus ja tehnoloogiliste arengutega sammu pidamine.

Uute tehnoloogiate laialdane levik on loonud vajaduse täiendada ja ajakohastada kehtivat õigusraamistikku, mille tulemusel on välja töötatud tehisintellekti määrus[5] (Artificial Intelligence Act, AI Act). Uute regulatsioonide kehtestamise taustal on oluline analüüsida isikuandmete kaitse üldmääruse (GDPR) rolli tehisintellekti ajastul ning uurida, kuidas seda saab kohandada ühiskonnas, kus algoritmid mõjutavad üha enam otsustusprotsesse ja teenuseid.[6]

Käesoleva teadustöö eesmärk on analüüsida, kuidas GDPR-i artikkel 22 reguleerib automatiseeritud otsuste tegemist tehisintellekti rakendustes ning millised on selle piirangud ja praktilised rakendusprobleemid. Töö keskendub ka peamistele õiguslikele probleemidele GDPR-i põhimõtete rakendamisel automatiseeritud otsustes ning käsitleb võimalikke lahendusi, mis tagaksid andmesubjektide tõhusa kaitse tehisintellekti ajastul.

Magistritöö eesmärgi saavutamiseks on püstitatud järgmised uurimisküsimused:

1. Kuidas GDPR-i artikkel 22 reguleerib automatiseeritud otsuseid ja millised on selle piirangud tehisintellekti kontekstis?
2. Millised on automatiseeritud otsuste peamised õiguslikud probleemid GDPR-i põhimõtete rakendamisel?
3. Kuidas tagada andmesubjektide õiguste kaitse TI-põhistes otsustusprotsessides?

[5] Euroopa Parlament ja Euroopa Liidu Nõukogu. Määrus (EL) 2024/1689 tehisintellekti käsitlevate ühtlustatud õigusnormide kohta, 13.06.2024. – ELT L 2024/1689, 12.07.2024.

[6] Camões, D. The challenges of the GDPR in the era of Artificial Intelligence: what can we expect from the future? – e-Publica 2024, Vol. 11 No. 3, lk 48.

Käesolev teadustöö tugineb õigusdogmaatilisele lähenemisele, mis keskendub kehtiva õiguse analüüsile ja süstematiseerimisele. Peamiste uurimismeetoditena kasutatakse õigusnormide tõlgendamist ning nende omavaheliste seoste ja rakendatavuse automatiseeritud otsuste tegemise ja profiilianalüüsi kontekstis tehisintellektisüsteemide kasutamisel.

Uurimuse aluseks on Euroopa Liidu õigusaktid, eelkõige isikuandmete kaitse üldmäärus (GDPR) ja tehisintellekti määrus (AI Act), samuti Euroopa Andmekaitsenõukogu (EDPB) suunised, andmekaitseasutuste otsused ning kohtupraktika. Lisaks kasutatakse erialakirjandust, et selgitada õigusnormide eesmärke ja rakendamise väljakutseid.

Euroopa Andmekaitsenõukogu suunised mängivad olulist rolli GDPRi tõlgendamisel ja ühtse kohaldamise tagamisel kogu Euroopa Liidus, andes praktilisi juhiseid nii andmetöötlejatele kui ka järelevalveasutustele. Andmekaitseasutuste otsused aitavad omakorda selgitada, kuidas GDPRi norme konkreetselt praktikas rakendatakse, eriti automatiseeritud otsuste tegemise ja profiilianalüüsi puhul.

Töös rakendatakse õigusdogmaatilist lähenemist, keskendudes kehtivate õigusnormide tõlgendamisele ja süstematiseerimisele, et välja selgitada GDPRi rakendamise eesmärgid ning tuvastada kitsaskohad ja praktilised väljakutsed.

Juhtumiuuringute kaudu analüüsitakse automatiseeritud otsustusprotsesse kolmes põhivaldkonnas: maksevõime hindamine panganduses, platvormitöö ning sotsiaaltoetustega seotud otsustusprotsessid avalikus sektoris. Need juhtumid aitavad illustreerida GDPRi rakendamise praktilisi probleeme ja võimalikke lahendusi.

Käesolevat magistritööd iseloomustavad märksõnad: isikuandmed, andmekaitse, tehisintellekt.

1. ÕIGUSLIK RAAMISTIK: GDPR ARTIKKEL 22 JA ÜLDPÕHIMÕTTED

1.1. GDPR-i eesmärk ja struktuur automatiseeritud otsuste reguleerimisel

Automatiseeritud otsuste ja profiilianalüüsiga seotud andmekaitseküsimused on tehnoloogia ja tehisintellekti arengu taustal muutunud üha olulisemaks. Kiire tehnoloogiline areng ja üleilmastumine on loonud uusi väljakutseid isikuandmete kaitses, kuna andmete kogumise ja jagamise ulatus on märkimisväärselt kasvanud. Nende muutuste tõttu oli Euroopa Liidus (EL) vaja tugevat ja ühtset andmekaitseraamistikku ning selle täitmise tõhusat tagamist.[7] Seetõttu loodi isikuandmete kaitse üldmäärus (GDPR), mille eesmärk on kaitsta Euroopa Liidu kodanike ja elanike isikuandmeid, tagada nende privaatsus ning sealhulgas vähendada automatiseeritud töötlusel põhinevate otsuste ja profiilianalüüsiga kaasnevaid riske. Käesolev peatükk analüüsib GDPR-i eesmärke ja struktuuri automatiseeritud otsuste reguleerimisel ning selgitab selle mõju andmetöötlejatele ja andmesubjektidele.

GDPR kehtib vastutavatele[8] ja volitatud[9] töötlejatele, kes töötlevad isikuandmeid EL-is asuva tegevuskoha tegevuse kontekstis, sõltumata sellest, kas andmetöötlus toimub EL-is või väljaspool seda (art 3 lg 1). Määrus kohaldub ka juhul, kui andmetöötlus on seotud kaupade või teenuste pakkumisega EL-is asuvatele andmesubjektidele või nende käitumise jälgimisega EL-is (art 3 lg 2 p- a ja b).

GDPR-i kohaldatakse sõltumata sellest, kas andmete töötlemine toimub täielikult või osaliselt automatiseeritult (art 2 lg 1). GDPR ei anna täpset definitsiooni automatiseeritud vahenditele, mis on mõistetav, kuna tehnoloogia kiire areng võib muuta konkreetse definitsiooni kiiresti aeguvaks.[10] Samas on määruses sätestatud isikuandmete töötlemise mõiste väga lai, hõlmates peaaegu kõiki toiminguid, sealhulgas kogumist, salvestamist, kasutamist ja edastamist, mis

[7] GDPR põhjenduspunktid 6 ja 7.
[8] GDPR art 4 p 7 kohaselt on „vastutav töötleja“ füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes üksi või koos teistega määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid.
[9] GDPR art 4 p 8 kohaselt on „volitatud töötleja“ füüsiline või juriidiline isik, avaliku sektori asutus, amet või muu organ, kes töötleb isikuandmeid vastutava töötleja nimel.
[10] Camões, lk 50.

võivad olla seotud isikuandmetega.[11] Seega saab GDPR-i rakendada tehisintellektisüsteemide (TI-süsteemide) suhtes juhul, kui nende toimingud hõlmavad isikuandmete töötlemist määruse tähenduses.

GDPR artikkel 4 punkt 4 kohaselt on profiilianalüüs igasugune isikuandmete automatiseeritud töötlemine, mille eesmärk on hinnata füüsilise isiku teatud isiklikke aspekte. GDPR määratleb profiilianalüüsi kui protsessi, mille käigus analüüsitakse või ennustatakse inimese töösooritust, majanduslikku olukorda, tervist, isiklikke eelistusi, huvisid, usaldusväärsust, käitumist, asukohta või liikumist. Seega profiilianalüüs koosneb kolmest elemendist: automatiseeritud andmetöötlusest, isikuandmete kasutamisest ja hindamisprotsessist.[12]

GDPR eristab profiilianalüüsi lihtsast isikute klassifitseerimisest. Kui inimesi jaotatakse näiteks vanuse või soo järgi pelgalt statistilise analüüsi eesmärgil, ei peeta seda profiilianalüüsiks. Kui aga andmeid kasutatakse inimese omaduste või käitumise hindamiseks ja ennustamiseks, kuulub see profiilianalüüsi alla. Profiilianalüüsi rakendatakse sageli ennustamismudelites, kus eri andmeallikate põhjal tehakse järeldusi inimese tõenäolise käitumise või omaduste kohta.[13]

Automatiseeritud otsuste tegemine on andmetöötlusprotsess, mille käigus langetatakse otsuseid tehnoloogiliste vahendite abil ilma inimese sekkumiseta. Sellised otsused võivad põhineda profiilianalüüsi tulemustel (näiteks isikuandmetest loodud profiilil) või toimuda ühes profiilianalüüsi protsessiga. Automatiseeritud otsused põhinevad mitmesugustel andmetel, sealhulgas andmesubjekti enda esitatud andmetel, jälgimise teel kogutud teabel ning tuletatud andmetel.[14] Kuigi automatiseeritud töötlusel põhinevaid otsuseid saab teha ka ilma tehisintellektita, tehakse enamik tänapäeva automatiseeritud otsuseid siiski tehisintellekti abil.[15]

---

[11] GDPR art 4 p 2 kohaselt „isikuandmete töötlemine“ on isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine.
[12] EDPB 2018, Guidelines on ADM and Profiling, lk 6-7.
[13] Samas, lk 6-8.
[14] Samas, lk 8.
[15] Cotogni, G. The Explainability of Automated Decision-Making: A Historical Perspective through EU Legislation – Journal of Law, Market & Innovation 2024, Vol. 3 Issue 3, lk 417.

Automatiseeritud töötlusel põhinevate otsuste tegemine ja profiilianalüüs ei ole alati eraldiseisvad tegevused. Profiilianalüüs võib olla automatiseeritud otsustusprotsessi osa, kui selle tulemusi kasutatakse isikute kohta käivate otsuste langetamiseks. Samas võib profiilianalüüs toimuda ka ilma otsustusprotsessita, näiteks turunduse või riskianalüüsi eesmärgil.[16]

GDPR-i kontekstis puudutavad andmesubjekti õigused ja vastutava töötleja kohustused erinevaid automatiseeritud isikuandmete töötlemise vorme, mis on seotud profiilianalüüsi ja automatiseeritud otsuste tegemisega. Euroopa Andmekaitsenõukogu suunises automatiseeritud töötlusel põhinevate üksikotsuste tegemise ja profiilianalüüsi kohta eristatakse järgmisi kasutusviise:

1. automatiseeritud profiilianalüüs ilma otsuse langetamiseta,
2. automatiseeritud profiilianalüüsil põhinev otsustamine, mis ei ole täielikult automatiseeritud,
3. üksnes automatiseeritud otsustamine, sealhulgas profiilianalüüs, mis toob kaasa õiguslikke või võrreldava mõjuga tagajärgi andmesubjektile (GDPR art 22 lg 1).[17]

GDPR kehtestab raamistiku, mis piirab automatiseeritud otsuste tegemist. Vastutavad töötlejad võivad teha nii profiilianalüüsi kui ka automatiseeritud otsuste tegemist, kui nad järgivad kõiki GDPR-i põhimõtteid ja omavad töötlemiseks seaduslikku alust. Järgnevad üldpõhimõtted käsitlevad kõiki profiilianalüüsi ja automatiseeritud otsustamise vorme, sealhulgas selliseid, mis ei ole täielikult automatiseeritud ega kuulu artikli 22 reguleerimisalasse.[18]

Isikuandmete töötlemise üldpõhimõtted (art 5) nõuavad eelkõige õiglust, läbipaistvust ja andmete eesmärgipärast kasutust. Läbipaistvus tähendab, et andmesubjektidel peab olema võimalus mõista, kuidas nende isikuandmeid töödeldakse ja milliseid tagajärgi see võib kaasa tuua. Kuna profiilianalüüs tugineb sageli tuletatud andmetele, võib see jääda andmesubjektidele märkamatuks, mistõttu on oluline tagada selge ja arusaadav teabe edastamine.[19]

---

[16] EDPB 2018, Guidelines on ADM and Profiling, lk 6-8
[17] Samas, lk 6-9.
[18] Samas, lk 8-9.
[19] Samas, lk 9-10.

Samuti on oluline eesmärgi piirang, mille kohaselt võib isikuandmeid töödelda vaid algselt määratletud ja õiguspärasel eesmärgil. Näiteks kui mobiilirakendus kogub asukohaandmeid restoranide soovitamiseks, ei tohi neid andmeid kasutada tarbijale suunatud reklaamide edastamiseks ilma selgesõnalise nõusolekuta (art 5 lg 1 p b). Lisaks sellele tuleb järgida andmete minimaalsuse põhimõtet, mille kohaselt tohib koguda vaid sellises mahus isikuandmeid, mis on hädavajalikud määratletud eesmärgi täitmiseks. Võimalusel tuleks kasutada anonüümseid või pseudonüümitud andmeid, et vähendada isikute tuvastamise ja andmete väärkasutuse riske (art 5 lg 1 p c). Profiilianalüüsi ja automatiseeritud otsuste tegemise puhul on samuti kriitilise tähtsusega andmete täpsus, kuna valede või aegunud andmete kasutamine võib viia ebaõiglaste või ekslike otsusteni, näiteks ebatäpse maksevõime hinnangu andmiseni (art 5 lg 1 p d). Lisaks tuleb järgida andmete säilitamise piirangut, mille kohaselt võib isikuandmeid säilitada vaid nii kaua, kui see on vajalik töötlemise eesmärgi saavutamiseks. Liigne andmete säilitamine võib suurendada privaatsusriske ja viia ebatäpsete otsusteni, kui andmeid ei ajakohastata piisavalt regulaarselt (art 5 lg 1 p e).[20]

Artikkel 6 sätestab põhimõtte, et isikuandmete töötlemiseks peab olema seaduslik alus. Peamised õiguslikud alused on järgmised:

1. Nõusolek (art 6 lg 1 p a) – Kuna automatiseeritud profiilianalüüsi läbipaistmatus võib raskendada andmesubjekti teadlikku nõustumist, peab vastutav töötleja tagama, et isikud mõistavad täielikult, milleks nende andmeid kasutatakse ja millised võivad olla võimalikud tagajärjed.
2. Lepingu täitmiseks vajalik töötlemine (art 6 lg 1 p b) – Profiilianalüüsi võib kasutada ainult siis, kui see on lepingu täitmiseks hädavajalik. Näiteks ei ole veebipoel õigust analüüsida kasutaja tarbimisharjumusi profiilianalüüsi kaudu, kui see ei ole otseselt seotud tellitud kaupade tarnimise või maksete töötlemisega.
3. Õigusliku kohustuse täitmine (art 6 lg 1 p c) – Profiilianalüüs võib olla vajalik seadusest tulenevate kohustuste täitmiseks, näiteks pettuste ennetamiseks või rahapesu tõkestamiseks.
4. Eluliste huvide kaitse (art 6 lg 1 p d) – Profiilianalüüsi võib kasutada inimese elu või tervise kaitseks, näiteks epideemiate leviku prognoosimisel või humanitaarkriiside lahendamisel.

[20] EDPB 2018, Guidelines on ADM and Profiling, lk 9-12.

5. Avalikes huvides oleva ülesande täitmine või ametivõimu teostamine (art 6 lg 1 p e) – Seda alust saab kasutada peamiselt avaliku sektori profiilianalüüsis, kuid ainult juhul, kui see põhineb selgelt määratletud õiguslikul alusel.
6. Õigustatud huvi (art 6 lg 1 p f) – Profiilianalüüsi võib teha, kui see on vajalik vastutava töötleja või kolmanda osapoole õigustatud huvide kaitseks. Siiski ei saa seda kasutada, kui andmesubjekti õigused ja huvid kaaluvad üles töötleja huvid. Hinnata tuleb: profiilianalüüsi detailsust, selle ulatust ja mõju andmesubjektile ning võtta kasutusele meetmed, mis tagavad õigluse, võrdse kohtlemise ja andmete täpsuse.[21]

Kui profiilianalüüs või automatiseeritud otsustamine hõlmab eriliigilisi isikuandmeid (nt terviseandmeid), tuleb täita lisaks ka artikli 9 tingimused. Vastutavad töötlejad võivad töödelda eriliigilisi isikuandmeid ainult siis, kui nad täidavad vähemalt ühe artikli 9 lõike 2 tingimuse ning lisaks ühe artikli 6 seadusliku aluse.[22] Seega tuleb automatiseeritud profiilianalüüsi ja automatiseeritud otsuste tegemisel hoolikalt valida sobiv seaduslik alus ning tagada andmesubjektide õiguste kaitse, järgides eelkõige nõusoleku, läbipaistvuse ja õigluse põhimõtteid.

Andmesubjektil on mitmeid õigusi, mida tuleb tagada automatiseeritud otsuste tegemise ja profiilianalüüsi korral. GDPR artiklite 13 ja 14 kohaselt on andmesubjektil õigus saada teavet selle kohta, kuidas ja miks tema isikuandmeid töödeldakse. Artikli 15 alusel on tal õigus nõuda teavet tema kohta käivate isikuandmete ning nende töötlemise kohta.

Vastutav töötleja peab andma andmesubjektile teavet automatiseeritud otsustamise olemasolu, kasutatava loogika ning sellise töötlemise tähenduse ja eeldatavate tagajärgede kohta juba andmete kogumisel või andmesubjekti taotlusel. Eelkõige peab andmesubjektil olema võimalik teada, kas teda hinnatakse automatiseeritud süsteemi, näiteks algoritmi abil, ning saada sisulist teavet sellise töötlemise olemuse ja mõju kohta.[23]

Lisaks on andmesubjektil õigus nõuda oma isikuandmete parandamist (art 16) ja kustutamist (art 17). See tähendab, et ebatäpsed või aegunud andmed tuleb põhjendamatu viivituseta parandada või kustutada, kui andmesubjekt seda taotleb. Õigus töötlemise piiramisele (art 18) annab andmesubjektile võimaluse nõuda, et tema isikuandmete töötlemine peatatakse või piiratakse, näiteks kuni vaidlusaluste andmete täpsus on kontrollitud. Samuti on

[21] EDPB 2018, Guidelines on ADM and Profiling, lk 12-15.
[22] Samas, lk 12-15.
[23] Samas, lk 16-17.

andmesubjektil õigus esitada vastuväiteid (art 21), mis tähendab, et ta võib teatavatel juhtudel takistada oma isikuandmete edasist töötlemist, kui selleks puudub piisav õiguslik alus.

GDPR artiklis 22 sätestatakse täiendavad kaitsemeetmed ja piirangud automatiseeritud otsustamise suhtes. Artikli 22 lõike 1 kohaselt on andmesubjektil õigus, et tema kohta ei tehtaks otsust, mis põhineb üksnes automatiseeritud andmetöötlusel (sealhulgas profiilianalüüsil) ja mis toob kaasa tema suhtes õiguslikke tagajärgi või avaldab talle märkimisväärset mõju. Sellised täielikult automatiseeritud individuaalsed otsused on üldreeglina keelatud, välja arvatud juhul, kui kohaldatakse artikli 22 lõikes 2 loetletud erandeid.

Artikli 22 lõige 2 loetleb kolm erandit, mille korral automatiseeritud otsustamine on lubatud:

1. kui otsus on vajalik andmesubjektiga lepingu sõlmimiseks või täitmiseks;
2. kui otsus on lubatud liidu või liikmesriigi õigusega, mis näeb ette ka sobivad kaitsemeetmed andmesubjekti õiguste, vabaduste ning õigustatud huvide kaitseks;
3. kui otsus põhineb andmesubjekti selgesõnalisel nõusolekul.

Automatiseeritud otsuseid võib kasutada lepingu täitmiseks või sõlmimiseks ainult siis, kui see on hädavajalik ega ole võimalik kasutada andmemahult väiksemaid või privaatsussõbralikumaid meetodeid. Kui liikmesriigi seadus või EL-i õigus lubab automatiseeritud otsustusprotsessi, peab see sisaldama ka meetmeid andmesubjekti õiguste ja vabaduste kaitseks. Põhjenduspunktis 71 on märgitud, et selliseid otsuseid võib rakendada näiteks pettuste ennetamisel, maksudest kõrvalehoidumise tuvastamisel või teenuste turvalisuse tagamisel. Automatiseeritud otsuste tegemine on lubatud ka juhul, kui andmesubjekt on andnud selgesõnalise nõusoleku. Kuna selline töötlemine võib kujutada endast olulist andmekaitseriski, eeldab GDPR, et andmesubjektil oleks maksimaalne kontroll oma isikuandmete üle.[24]

Eelpool kirjeldatud juhtudel ja tingimustel on automatiseeritud otsustus õiguspärane, kuid vastutav töötleja peab rakendama lisameetmeid andmesubjekti õiguste kaitseks. Artikkel 22 lõige 3 sätestab, et vähemalt tuleb andmesubjektile tagada õigus inimlikule sekkumisele[25],

[24] EDPB 2018, Guidelines on ADM and Profiling, lk 23-24.

[25] „Inimlik sekkumine“ tähendab, et automatiseeritud otsuse tegemisse peab sekkuma teadlik ja pädev inimene, kes hindab otsust sisuliselt, mitte ei kinnita seda formaalselt või automaatselt. Euroopa andmekaitse töörühma suunise kohaselt ei piisa pelgalt „templi löömisest“ – inimesel peab olema võime otsust mõjutada, see vajadusel ümber hinnata ja otsuse tagajärgi mõista (EDPB 2018, Guidelines on ADM and Profiling, lk 21).

õigus esitada oma seisukoht ning õigus see otsus vaidlustada. Need meetmed peavad tagama, et andmesubjekt säilitab kontrolli oma isikuandmete ja nende alusel tehtavate otsuste üle ning tal on võimalus otsustusprotsessi mõjutada või seda tagantjärele kontrollida.

Lisaks tuleb täiendavalt arvestada artikli 22 lõike 4 nõuetega, mille kohaselt ei tohi automatiseeritud otsustamine toimuda eriliiki isikuandmete (nt rass, tervis, uskumused) alusel, välja arvatud juhul, kui andmesubjekt on andnud selgesõnalise nõusoleku vastavalt artikli 9 lõike 2 punktile a või tegemist on olulise avaliku huviga vastavalt artikli 9 lõike 2 punktile g ning rakendatakse asjakohaseid kaitsemeetmeid.

Regulatiivse raamistiku oluline osa on andmekaitsealase mõjuhinnangu (*Data Protection Impact Assessment*, DPIA) kohustus, mis on sätestatud GDPR-i artikli 35 lõike 3 punktis a. DPIA on nõutav juhul, kui kasutatakse ulatuslikku automatiseeritud isikuandmete töötlemist isiku omaduste hindamiseks (profiilianalüüs), mille tulemusel tehtavad otsused võivad andmesubjekti oluliselt mõjutada. Andmekaitsenõukogu suuniste kohaselt tuleb mõjuhinnang läbi viia kõigil juhtudel, kus andmetöötlus võib põhjustada kõrge riski andmesubjektide õigustele ja vabadustele. Selline eelnev hinnang võimaldab juba süsteemi kavandamise etapis tuvastada, kas kavandatav TI-süsteem võib minna vastuollu artikli 22 nõuetega ning milliseid kaitsemeetmeid tuleks rakendada. Lisaks on DPIA oluline vahend vastutustundliku andmetöötluse tagamiseks, võimaldades vastutaval töötlejal hinnata ja maandada võimalikke riske. Mõjuhinnang ei ole nõutav üksnes täielikult automatiseeritud otsustusprotsesside korral (art 22 lg 1), vaid ka juhul, kui osaliselt automatiseeritud otsused võivad oluliselt mõjutada andmesubjekti õigusi ja vabadusi[26]

Kokkuvõtlikult võib öelda, et GDPR-i artikkel 22 toimib olulise kaitsemehhanismina TI-süsteemide kontekstis, piirates selliste automatiseeritud otsustusprotsesside kasutamist, mis võivad andmesubjektile tuua kaasa õiguslikke tagajärgi või avaldada talle märkimisväärset mõju. Samal ajal reguleerib GDPR neid protsesse laiemas andmekaitsepõhimõtete süsteemis, mis hõlmab mitte üksnes artikli 22 keelde ja erandeid, vaid ka üldisi seaduslikkuse, läbipaistvuse, täpsuse ja andmete minimaalsuse põhimõtteid ning nõudeid seoses andmesubjekti õiguste tagamise ja järelevalveasutuste rolliga. Vastutavad töötlejad võivad kasutada profiilianalüüsi ja automatiseeritud otsustamist ainult juhul, kui nad järgivad kõiki GDPR-i nõudeid, sealhulgas omavad töötlemiseks seaduslikku alust ja rakendavad sobivaid

[26] EDPB 2018, Guidelines on ADM and Profiling, lk 29-30.

kaitsemeetmeid, mis tagavad andmesubjektide õiguste kaitse nii täielikult kui ka osaliselt automatiseeritud töötlemise korral.

1.2. GDPR artikkel 22: keeld või andmesubjekti õigus?

Nagu eelnevalt käsitletud, sätestab GDPR-i artikkel 22 olulise piirangu automatiseeritud otsustusprotsessidele, mis võivad oluliselt mõjutada andmesubjekti. See säte on tekitanud laialdast arutelu selle üle, kas artiklit tuleks mõista andmesubjekti õigusena mitte olla üksnes automatiseeritud otsuse subjekt või kui üldise keeluna selliste otsuste tegemiseks. Selle tõlgenduse tagajärjed on märkimisväärsed nii andmesubjektide kui ka vastutavate töötlejate jaoks, kuna see määrab kindlaks, kas ja millistel tingimustel on automatiseeritud otsustamine lubatud.[27] Järgnev arutelu käsitleb artikli 22 normatiivset iseloomu, tuginedes määruse sõnastusele, Euroopa andmekaitseasutuste suunistele, õiguskirjandusele ning asjakohasele kohtupraktikale.

Mõned teadlased ja kohtupraktika on leidnud, et artikkel 22 sisaldab üldreeglina keeldu, mille kohaselt automatiseeritud otsuseid võib teha ainult erandjuhtudel, mis on loetletud artiklis 22 lg 2.[28] Selle tõlgenduse aluseks on järgmised argumendid:

1. Süstemaatiline argument nõusoleku erandi põhjal - Artikkel 22 lõige 2 punkt c sätestab, et automatiseeritud otsused on võimalikud ainult juhul, kui andmesubjekt on andnud nõusoleku või kui rakendub mõni muu erand. Selline struktuur eeldab, et artikkel 22 lõige 1 kehtestab üldise keelu, millest saab erandite kaudu loobuda.[29]
2. Erikategooria isikuandmete kaitse - Artikli 22 lõike 4 kohaselt on eriliigiliste isikuandmete kasutamine automatiseeritud otsuste tegemisel rangelt piiratud. Kui artikkel 22 ei kehtestaks üldist keeldu, oleks tundlike andmete töötlemine vähem reguleeritud ja andmesubjektide kaitse nõrgem.[30]
3. Euroopa Kohtu tõlgendus - SCHUFA Holdingu kaasuses on Euroopa Kohus asunud seisukohale, et artikli 22 rakendamine ei sõltu andmesubjekti aktiivsest sekkumisest, mis

[27] Thouvenin, F., Früh, A., Henseler, S. Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right? – European Data Protection Law Review 2022, Vol. 8 No. 2, lk 183.
[28] Camões, lk 52 jj.
[29] Thouvenin, Früh, Henseler, lk 190.
[30] Samas, lk 190.

toetab käsitlust selle kui vaikimisi keelu kohta.[31] Tegemist on esimese Euroopa Kohtu otsusega, mis käsitleb artiklit 22 ning kinnitab, et tegemist on vaikimisi kohaldatava keeluga.[32] See annab tugeva suunise edaspidiseks kohtupraktikaks ja tõlgenduseks.

4. Andmekaitseasutuste seisukoht - Artikkel 29 töögrupp on oma suunistes selgitanud, et GDPR-i artiklit 22 tuleb käsitleda keeluna, mille eesmärk on vältida olukordi, kus andmesubjektid peaksid automatiseeritud otsuste puhul ise aktiivselt oma õiguste kaitseks tegutsema. Selle seisukoha kinnitas Euroopa Andmekaitsenõukogu 2018. aastal, võttes Artikkel 29 töögrupi suunised üle ja kinnitades nende jätkuva kehtivuse.[33]

Kui artikkel 22 tõlgendatakse kui keeldu, siis andmesubjektid on vaikimisi kaitstud ilma, et nad peaksid töötlejate otsuseid vaidlustama. Selline tõlgendus tähendab, et andmesubjekt on tugevamalt kaitstud – tal ei ole vaja teada iga automatiseeritud otsustamise episoodi ega sellele reageerida, mis on eriti oluline keerukates ja läbipaistmatutes tehisintellektisüsteemides. Vastutavad töötlejad peavad kindlustama, et nende automatiseeritud otsustamine vastab GDPR-i nõuetele ning tagama erandite korrektse rakendamise. Keeld piirab TI-põhise automatiseeritud otsustamise kasutuselevõttu Euroopas, kuna see nõuab erandite ranget järgimist.

Alternatiivne tõlgendus on, et artikkel 22 annab andmesubjektile õiguse mitte olla automatiseeritud otsuse subjekt, kuid ei keela selliseid otsuseid üldreeglina.[34] Selle positsiooni põhiargumendid on:

1. Sõnastuse selgus ja ajalooline kontekst - Artikli 22 sõnastus („andmesubjektil on õigus mitte olla...“) ja selle vastavus eelmise andmekaitsedirektiivi artiklile 15 toetavad käsitlust, et tegemist on andmesubjekti õigusega.[35]
2. Süstemaatiline argument (paiknemine peatükis III) - Artikkel 22 asub GDPR-i peatükis III, mis käsitleb andmesubjekti õigusi, mitte keelde. See toetab artikli käsitlemist õiguse, mitte keeluna.[36]

[31] EKo C-634/21, *SCHUFA Holding AG*, ECLI:EU:C:2023:957.
[32] Camões, lk 54-55.
[33] EDPB 2018, Guidelines on ADM and Profiling, lk-d 5 ja 19.
[34] Camões, lk 52 jj.
[35] Samas, lk 53.
[36] Samas, lk 53.

3. Õiguskindlus ja proportsionaalsus - Õigusena tõlgendamisel välditakse liiga suurt piirangut tehnoloogiliste uuenduste ja äriprotsesside rakendamisel, võimaldades rohkem paindlikkust ja õigusselgust organisatsioonidele.[37]
4. Kooskõla tehisintellekti määrusega (AI Act) - Euroopa Komisjon on AI Act-is valinud tasakaalustatud ja riskipõhise lähenemise tehisintellekti reguleerimiseks. Keelu asemel suunab regulatsioon pigem turvaliste ja läbipaistvate süsteemide arendamist. See regulatsioon ei asenda GDPR-i, vaid täiendab seda. Seetõttu säilitab GDPR artikkel 22 oma õigusliku olulisuse ka pärast AI Acti jõustumist, pakkudes jätkuvalt kaitset automatiseeritud otsuste eest, olenemata kasutatava tehnoloogia liigist või keerukusest.[38] (AI Act-i ja GDPR-i koostoimet käsitletakse põhjalikumalt peatükis 3.1.)

Kui artikkel 22 tõlgendatakse kui andmesubjekti õigust, siis andmesubjektid peavad ise oma õigusi kaitsma ja vajadusel vaidlustama automatiseeritud otsused. Vastutavad töötlejad saavad laiemalt rakendada automatiseeritud otsustamist, kuid peavad tagama, et andmesubjektid saavad oma õigusi kasutada ja vajadusel tuleb tagada inimjärelevalve.

Kokkuvõttes on võimalik esitada veenvaid argumente mõlema käsitluse kasuks. Kuid tõlgendades GDPR-i artiklit 22 süstemaatiliselt ning objektiiv-teleoloogiliselt (arvestades määruse ülesehitust, üldpõhimõtteid ja eesmärki kaitsta andmesubjektide õigusi), näib põhjendatum käsitleda seda sätet pigem üldise keeluna, millele on ette nähtud piiratud erandid. Selline tõlgendus toetab tugevamat isikuandmete kaitset ja aitab vältida tehisintellektil põhinevate otsuste liigset rakendamist ilma andmesubjektide selgesõnalise nõusoleku ja piisava teavitamiseta. Lisaks tagab see suurema selguse vastutavatele töötlejatele, kes peavad arvestama rangemate vastavusnõuetega.

1.3. Probleemid GDPR-i artikli 22 lg 1 kohaldamisel

GDPR artikli 22 lõige 1 sätestab: „Andmesubjektil on õigus, et tema kohta ei võetaks otsust, mis põhineb üksnes automatiseeritud töötlusel, sealhulgas profiilianalüüsil, mis toob kaasa

[37] Camões, lk 53–54.
[38] Samas, lk 60 jj.

teda puudutavaid õiguslikke tagajärgi või avaldab talle märkimisväärset mõju.“ Seega selleks, et GDPR artikli 22 lõige 1 kohalduks, peavad olema täidetud kolm tingimust:

1. isikut puudutav otsus,
2. otsuse tegemine põhineb üksnes automatiseeritud töötlusel,
3. otsusel on isikule oluline mõju või õiguslikud tagajärjed.

Kui eelpool nimetatud tingimused ei ole täidetud, siis ei kohaldu GDPR artikli 22 sätted ning kehtivad isikuandmete töötlemise üldpõhimõtted. Kui tingimused on täidetud ning artikli 22 lõige 1 kohaldub, peavad andmetöötlejad tõendama, et neil on töötlemiseks sobiv õiguslik alus ning täitma ka kõiki artikli 22 lõikes 2 sätestatud tingimusi. Töötlejate ainus võimalus keeldu vältida on põhjendada, et tegemist ei ole artiklis 22 määratletud automatiseeritud otsuse tegemisega.[39]

GDPR artikli 22 lõikes 1 kasutatud mõistet „otsus“ tuleb tõlgendada laialt, hõlmates erinevaid automatiseeritud protsesse, mis võivad andmesubjekti mõjutada. Otsusel ei pea olema kindlat vormi, vaid see võib sisaldada ka meetmeid, mis toetavad või täiendavad otsustusprotsessi.[40] Euroopa Kohus selgitas SCHUFA Holding kohtuasjas, et mõiste „otsus“ artikli 22 tähenduses on piisavalt lai, et hõlmata mitmesuguseid toiminguid, mis mõjutavad andmesubjekti erineval moel. Kohus tuginas seejuures GDPR-i põhjenduspunktile 71, mille kohaselt võib otsus sisaldada meedet, millel on isikut puudutavad õiguslikud tagajärjed või mis avaldab talle samaväärselt märkimisväärset mõju. Põhjenduspunktis tuuakse näitena veebipõhine krediiditaotluse automaatne tagasilükkamine või töölevõtu otsus ilma inimsekkumiseta. Samas kohtulahendis leidis kohus, et selline automaatselt määratud krediidihinnang, mis esindab tõenäosusväärtust isiku maksevõime kohta ja mida kolmas isik kasutab lepingulise otsuse tegemisel, võib kvalifitseeruda artikli 22 tähenduses otsuseks.[41]

Samas ei kvalifitseeru iga automatiseeritud tegevus GDPR-i tähenduses otsuseks – selleks peab otsustusprotsess saavutama teatud keerukustaseme. Lihtsad algoritmilised toimingud, näiteks kui süsteem saadab automaatselt meeldetuletuse maksetähtaja saabumise kohta, ei kujuta endast sellist automatiseeritud otsust, millele artikkel 22 kohaldub.[42]

---

[39] Camões, lk 55-60.
[40] Samas, lk 56.
[41] EKo C-634/21, SCHUFA Holding AG, p-d 45-46, 73.
[42] Camões, lk 56.

Kui esimese tingimuse – otsuse mõiste – tõlgendamisel on kujunenud suhteliselt ühtne lähenemine, siis on praktikas rohkem raskusi tekitanud teise ja kolmanda tingimuse – „üksnes automatiseeritud töötluse“ ning „õiguslike või märkimisväärsete mõjude“ – sisustamine. Kohtud ja andmekaitseasutused rakendavad nende hindamisel üha keerukamaid kriteeriume.[43] Järgnevad alapeatükid analüüsivad nende tingimuste sisu ja tõlgendusprobleeme lähemalt.

1.3.1. Mida tähendavad „üksnes automatiseeritud otsus“ ja inimsekkumisega otsus?

Probleeme tekitab määratlemine, millal on tegemist üksnes automatiseeritud töötlusel põhineva otsusega ning milline ja kui ulatuslik peab olema inimese mõtestatud sekkumine, et vältida GDPR artikli 22 kohaldumist. Artikli sõnastuses kasutatav termin „üksnes“ viitab otsustusprotsessile, kus puudub sisuline inimlik sekkumine.[44] Kui tõlgendada mõistet sõnasõnalt, tähendaks see, et isegi minimaalne inimsekkumine välistaks artikli 22 rakendumise. Kuid selline range tõlgendus võib kahjustada andmesubjektide õiguste kaitset.[45]

Euroopa Andmekaitsenõukogu suunised rõhutavad, et vastutav töötleja ei tohi artikli 22 kohaldamist vältida pelgalt näilise inimsekkumise abil. Inimlik järelevalve peab olema sisuline, mitte üksnes formaalne toiming. Sisuline sekkumine tähendab, et inimesel on reaalne otsustusõigus: ta omab pädevust ja volitusi otsust muuta, arvestades kõiki asjakohaseid asjaolusid ja andmeid. Vastupidiselt tähendab formaalne sekkumine olukorda, kus inimene kinnitab üksnes süsteemi poolt tehtud otsuse, mõjutamata seda sisuliselt. Kui automatiseeritud süsteem esitab otsust toetava soovituse, mida inimene kaalub koos teiste asjaoludega ning langetab seejärel lõpliku otsuse, siis ei käsitleta seda artikli 22 mõttes üksnes automatiseeritud töötlemisena.[46]

Amsterdami esimese astme kohus käsitles 2021. aastal juhtumit, kus neli Uberi platvormil töötavat sõidukijuhti vaidlustasid oma kontode deaktiveerimise. Uber põhjendas seda pettusekahtlusega, sealhulgas tühistamistasude põhjendamatu kogumise ja GPS-andmete

[43] Barros Vale, S., Zanfir-Fortuna, G. Automated Decision-Making under the GDPR: Practical Cases from Courts and Data Protection Authorities. Future of Privacy Forum 2022, lk 28 jj.
[44] EDPB 2018, Guidelines on ADM and Profiling, lk 20.
[45] Camões, lk 56-57.
[46] EDPB 2018, Guidelines on ADM and Profiling, lk 19-21.

manipuleerimisega. Hagejate väitel oli otsus tehtud üksnes automatiseeritud töötlusel põhinevalt, ilma mõtestatud inimliku sekkumiseta. See tõstatas küsimuse võimaliku rikkumise kohta seoses GDPR-i artikli 22-ga.[47]

Hagejad väitsid, et Uberi privaatsusavaldusest ja veebilehel avaldatud teabe kohaselt on nende suhtes kohaldatud täielikult automatiseeritud otsuseid GDPR-i artikli 22 tähenduses. Sisulisele inimliku sekkumise puudumisele viitavad Uberi saadetud standardiseeritud ja väga üldsõnalised sõnumid. Nendes sõnumites ei selgitanud Uber, milliseid konkreetseid pettuseakte hagejad väidetavalt toime panid.[48]

Uber eitas süüdistusi, väites, et sõidukijuhtide kontode deaktiveerimine ei toimunud üksnes automatiseeritud töötlusel põhineva otsuse tulemusena, vaid protsessis osales ka spetsiaalne riskimeeskond. Kui süsteem registreerib kahtlase tegevuse, edastatakse juhtum hoiatusena riskimeeskonna töötajatele, kelle ülesanne on hinnata, kas juhtum vajab täiendavat uurimist. Tööprotsessi käigus analüüsivad töötajad automaatselt genereeritud signaale, hindavad neid koos muude andmetega ning rakendavad oma kogemust ja kaalutlusõigust. Uberi sõnul tehakse lõplik deaktiveerimisotsus alles siis, kui kahtlused leiavad kinnitust vähemalt kahe riskimeeskonna töötaja poolt. Vajadusel kaasatakse ka kolmas töötaja, kes viib läbi sõltumatu kontrolli. Kuigi kontode deaktiveerimine võib praktikas tähendada ka lepingulise suhte lõpetamist, rõhutas Uber, et lõplik otsus langetati alles pärast mõtestatud inimlikku hindamist, mitte automaatselt.[49]

Kuna hagejad ei vaidlustanud Uberi poolt esitatud otsustusprotsessi kirjeldust ning ning Uberi esitatud seletustes vastuolud puudusid, leidis kohus, et tegemist ei olnud täielikult automatiseeritud töötlemisega. Kuna kontode deaktiveerimine toimus mõtestatud inimliku sekkumise tulemusel, ei kohaldunud sellele GDPR-i artikli 22 lõige 1.[50]

Kuid 2023. aastal arutas Amsterdami apellatsioonikohus Uberi juhtumit ning jõudis vastupidisele järeldusele võrreldes 2021. aasta esimese astme otsusega. Kohus leidis, et vähemalt kolme kaebaja kontode deaktiveerimine põhines üksnes automatiseeritud andmetöötlusel, ilma sisulise inimliku sekkumiseta otsustusprotsessi.[51]

---

[47] Rechtbank Amsterdam, 3. veebruar 2021, *Uber*, ECLI:NL:RBAMS:2021:1018.
[48] Samas, p 4.17
[49] Samas, p-d 4.18-4.26
[50] Samas.
[51] Gerechtshof Amsterdam, 24. aprill 2023, *Uber*, ECLI:NL:GHAMS:2023:793.

Hagejate väitel piirdus Uberi nn inimlik kontroll pelgalt automaatselt genereeritud otsuste kinnitamisega, kus töötajatel puudus tegelik kaalutlusõigus või võimalus otsust sisuliselt mõjutada. Kohus nõustus selle hinnanguga, rõhutades, et Uber ei esitanud piisavaid tõendeid, mis kinnitaksid sisuka inimliku sekkumise olemasolu.[52]

Kohus tugines Euroopa Andmekaitsenõukogu suunistele ning leidis, et selline formaalselt eksisteeriv osalus, kus inimene üksnes „vajutab kinnitamise nuppu", ei vasta GDPR artikli 22 mõistes nõutavale sisuka sekkumise tasemele. Lisaks osutas kohus mitmele olulisele asjaolule, mis viitasid automatiseeritud töötlemisele:

1. Uberi kehtivas privaatsusteates oli otsesõnu kirjas, et pettuse kahtluse korral deaktiveeritakse kasutajad automatiseeritud otsuste alusel;
2. Uberi kasutatav tarkvara genereeris automaatselt pettusealaseid „signaale", mille alusel otsused tehti;
3. Otsused olid koostatud üldsõnaliselt, ilma konkreetse käitumise viiteta, ning juhte ei kuulatud enne konto deaktiveerimist ära.[53]

Uber ei suutnud tõendada, et otsused langetati vajaliku inimliku läbivaatusega. Selle põhjal järeldas kohus, et deaktiveerimisotsused kvalifitseerusid täielikult automatiseeritud töötluseks GDPR artikli 22 tähenduses.[54]

Uberi juhtum ei ole ainulaadne. 2021. aastal määras Itaalia andmekaitseamet Ühendkuningriigi toidukulleriettevõttele Deliveroo seoses automatiseeritud tööprotsessidega, mis mõjutasid tööaegade jaotust kullerite vahel. Vaidlus sai alguse algoritmilise süsteemi nimega Frank kasutuse tõttu, mille abil määrati sõitjate järjestus ja töövahetused.[55]

Kolm sõitjat esitasid kaebuse, väites, et algoritm kohtles neid ebaõiglaselt ja diskrimineerivalt – eelkõige seetõttu, et töölt puudumisi käsitleti automaatselt karistusena, sõltumata puudumise põhjusest (nt haigus või streik). Algoritm hindas sõitjate töövalmidust ja usaldusväärsust, arvestades nende saadavust tippperioodidel, s.o reede, laupäeva ja pühapäeva õhtuti. ning osalemist eelnevalt broneeritud vahetustes. Need tegurid mõjutasid sõitjate järjestust, mille alusel määrati töövahetusi. Sõitjad, kes korduvalt ei ilmunud tööle,

[52] Gerechtshof Amsterdam 2023, Uber.
[53] Samas.
[54] Samas.
[55] Itaalia Andmekaitseamet. *Decision against Deliveroo Italy S.r.l.* 22. juuli 2021.

langesid järjestuses tahapoole ning nende võimalused tööd saada vähenesid – mõnel juhul viis see sisuliselt platvormilt kõrvalejäämiseni.[56]

Deliveroo väitis, et kasutatud algoritm ei kuulu GDPR-i artikli 22 kohaldamisalasse, kuna väidetavalt ei avaldanud algoritm sõitjatele „õiguslikke või samaväärselt olulisi mõjusid“ (täpsemalt järgmises peatükis) ning süsteem sisaldas teatavat inimlikku sekkumist. Samas ei selgitanud Deliveroo täpselt, kuidas ja millal see inimlik sekkumine toimus, ega toonud näiteid juhtumitest, kus inimene oleks saanud otsuse sisu muuta.[57]

Itaalia andmekaitseamet leidis, et kuigi Deliveroo väitis inimlikku sekkumist, ei olnud see sisuline ega toimunud enne otsuse mõju avaldumist. Seetõttu tehti töövõimaluste määramise otsused üksnes automatiseeritult, ilma tegeliku võimaluseta inimese sekkumiseks ning selline töötlemine kvalifitseerub GDPR artikli 22 lõike 1 kohaseks automatiseeritud otsustamiseks.[58]

Lisaks leidis Itaalia andmekaitseamet, et Deliveroo oleks pidanud enne algoritmi Frank kasutuselevõttu läbi viima andmekaitsealase mõjuhinnangu, lähtudes GDPR-i artikli 35 lõike 3 punktist a.[59] Otsuses tugines andmekaitseamet Euroopa Andmekaitsenõukogu juhistele, mille kohaselt on mõjuhinnang kohustuslik, kui töötlemine hõlmab:

1. uudse tehnoloogia kasutamist,
2. suures mahus/ultauslikku andmetöötlust (Deliveroo puhul 8000 sõitjat),
3. haavatavate andmesubjektide - platvormitöötajate - andmete töötlemist,
4. profileerimist ja automatiseeritud otsustamist, millel on olulised tagajärjed andmesubjektidele.[60]

Uberi ja Deliveroo juhtumid illustreerivad, kui keeruline võib olla eristada sisulist inimlikku sekkumist näilisest. Isegi kui organisatsioon väidab, et inimesed osalevad otsustamises, ei pruugi see tähendada, et neil on otsustusõigus või kaalutlusvabadus. Nii võib organisatsioon jätta mulje inimlikust sekkumisest, kuigi sisuliselt langetab otsuse automaatika.

Praktikas on oluline, et vastutav töötleja suudaks dokumenteerida ja põhjendada sisulise inimsekkumise olemasolu, näiteks andmekaitsemõjude hindamise kaudu, mis on kohustuslik

[56] Itaalia Andmekaitseamet, *Deliveroo*.
[57] Samas.
[58] Samas.
[59] Samas.
[60] EDPB 2018, Guidelines on ADM and Profiling, lk 29.

kõrge riskiga töötlemise korral.[61] See aitab näidata, et automatiseeritud süsteemi soovitused ei muutu automaatselt otsusteks, vaid et inimlik kaalutlus on tegelikult olemas.

Tuginedes viimaste aastate Euroopa kohtu ja andmekaitseasutuste ostustele on näha, et lähenetakse artikli 22 tõlgendamisele järjest põhjalikumalt ja kontekstitundlikumalt. Otsuse „üksnes automatiseerituse" hindamisel ei keskenduta ainult tehnoloogilisele protsessile, vaid kogu organisatsiooni ülesehitusele, töötajate väljaõppele ja otsustuskohustuse tegelikule sisule.[62] Seetõttu on põhjendatud järeldus, et sisuline inimsekkumine eeldab süstemaatilist ja dokumenteeritud lähenemist, mitte pelgalt töövoo vahepealset inimlikku kohalolu.

1.3.2. Mida tähendab „õiguslik või samaväärselt märkimisväärne" mõju?

Probleeme valmistab hinnangu andmine, millised mõjud on piisavalt olulised, et GDPR artikkel 22 kohalduks. Ehkki määrus viitab otsustele, mis toovad kaasa „õiguslikke tagajärgi" või millel on „samaväärselt märkimisväärne mõju", ei ole nende mõistete tähendus ega kohaldamisulatus täpsustatud. Andmekaitsenõukogu suuniste kohaselt viitab aga grammatiline tõlgendus sellele, et artikli 22 kohaldamisalasse kuuluvad üksnes need otsused, millel on isiku suhtes oluline ja tugev mõju.[63]

Õiguslike tagajärgedega otsuseks loetakse olukorda, kus üksnes automatiseeritud andmetöötluse tulemusena langetatud otsus mõjutab otseselt isiku seaduslikke õigusi. Sellised otsused võivad piirata näiteks valimisõigust või õigust pöörduda kohtusse. Õiguslikuks tagajärjeks loetakse ka automatiseeritud otsust, mis muudab isiku õiguslikku seisundit või tema lepingulisi õigusi. Tüüpilised näited on lepingu tühistamine, sotsiaalhüvitiste (nt lapsetoetuse või eluasemetoetuse) määramine või neist keeldumine, samuti riiki sisenemise keelamine või kodakondsuse andmisest keeldumine.[64]

GDPR kaitse ei piirdu aga üksnes juriidiliste mõjudega – see laieneb ka otsustele, mis mõjutavad isikut muul moel olulisel määral. Põhjendus 71 toob tüüpiliste näidetena välja automaatselt tehtud veebipõhise laenutaotluse tagasilükkamise või veebipõhine tööle värbamine ilma inimsekkumiseta. Kuigi need ei pruugi alati muuta inimese õiguslikku

[61] EDPB 2018, Guidelines on ADM and Profiling, lk 29.
[62] Barros Vale, Zanfir-Fortuna, viidatud raport, lk 35–36.
[63] EDPB 2018, Guidelines on ADM and Profiling, lk 22.
[64] Samas, lk 22.

staatust, võivad need siiski oluliselt mõjutada tema majanduslikku või sotsiaalset olukorda. Seega võib „märkimisväärse mõjuga" tulemuseks olla iga otsus, mille mõju on võrreldav õiguslike tagajärgedega. Suuniste kohaselt tuleb künnist hinnata sisuliselt: otsus peab olema piisavalt oluline või tõsine, et väärida GDPR-i kaitset.[65]

Selleks, et andmetöötlus kedagi märkimisväärselt mõjutaks, peab otsusel olema potentsiaal olulisel määral kujundada isiku olukorda, käitumist või valikuid; põhjustada pikaajalist või püsivat mõju andmesubjektile ning äärmuslikel juhtudel viia inimese tõrjutuse või diskrimineerimiseni. Euroopa Andmekaitsenõukogu suunised rõhutavad, et täpne määratlus, millised otsused ületavad selle künnise, on keeruline, kuid toovad välja mõned tüüpnäited. Nende hulka kuuluvad otsused, mis mõjutavad kellegi rahalist olukorda (nt nende laeunukõlblikkust), juurdepääsu tervishoiuteenustele, töövõimalusi või panevad ta väga ebasoodsasse olukorda. Samuti kuuluvad siia otsused, mis mõjutavad kellegi juurdepääsu haridusele, näiteks ülikooli vastuvõtuotsused.[66]

Eelpool käsitletud Uberi kohtuasjas (2021), kus neli Uberi platvormil töötavat autojuhti vaidlustasid oma kontode deaktiveerimise, analüüsis Amsterdami esimese astme kohus, kas otsusel oli ka õiguslik mõju isikute õigustele GDPR-i artikli 22 mõistes. Hagejate hinnangul tõi kontode sulgemine kaasa lepingulise suhte lõpetamise ning sellest tuleneva sissetuleku kaotuse. Uber väitis, et deaktiveerimine põhines pettusekahtlusel ning konto blokeeriti automaatselt ainult ajutiselt, kuni riskimeeskond võttis juhiga ühendust ja hindas olukorra tõsidust. Uberi kinnitusel langetati lõplik otsus alles pärast sisulist inimlikku kaalutlust vähemalt kahe töötaja poolt. Kohus nõustus Uberi seisukohaga ning leidis, et tegemist ei olnud täielikult automatiseeritud otsusega GDPR artikli 22 tähenduses, kuna esines mõtestatud inimlik sekkumine. Samuti rõhutas kohus, et lühiajaline ligipääsupiirang ei avaldanud püsivat ega olulist õiguslikku mõju.[67]

Kuid sama juhtumi hilisemas arengus jõudis 2023. aastal Amsterdami apellatsioonikohus vastupidisele järeldusele. Kohus tuvastas, et vähemalt kolme hageja kontode deaktiveerimine toimus üksnes automatiseeritud andmetöötluse tulemusena, ilma tõendatava sisulise inimliku sekkumiseta. Uberi väidetud riskimeeskonna roll piirdus kohtu hinnangul automaatselt genereeritud otsuste formaalse kinnitamisega, mis ei täida GDPR artikli 22 nõudeid mõtestatud inimlikule sekkumisele. Kohus viitas ka Uberi privaatsusavaldusele, milles oli

[65] EDPB 2018, Guidelines on ADM and Profiling, lk 21-22.
[66] Samas, lk 21-22.
[67] Rechtbank Amsterdam 2021, Uber.

otsesõnu märgitud, et pettusekahtluse korral deaktiveeritakse kasutajakonto automaatselt. Lisaks ei saanud juhid teada konkreetseid pettusekahtlusi ega olnud neil võimalik end enne konto sulgemist kaitsta.[68]

Seega järeldas apellatsioonikohus, et Uber rikkus GDPR-i, kuna langetas õiguslikult ja majanduslikult olulise otsuse - konto sulgemise ja töövõimaluse kaotuse - täielikult automatiseeritud viisil, ilma vastava inimliku kontrollita. Otsus kinnitas GDPR artikli 22 rakendatavust olukordades, kus algoritmil põhinev süsteem mõjutab oluliselt üksikisiku õigusi või vabadusi, eriti kui puudub läbipaistev teavitus- ja vaidlustamismehhanism. See juhtum näitab, et automatiseeritud otsused, mis toovad kaasa lepinguliste õiguste lõppemise, võivad kvalifitseeruda õigusliku tagajärjena artikli 22 tähenduses.[69]

Samaväärselt märkimisväärse mõju näitena võib esile tõsta eelpool käsitletud Deliveroo kaasuse, milles Itaalia andmekaitseasutus tegi 2021. aastal otsuse platvormitöötajate õiguste rikkumise kohta. Deliveroo väitis, et nende kasutatav süsteem ei tekitanud isegi abstraktselt õiguslikke ega märkimisväärseid mõjusid. Kuid Itaalia andmekaitseasutus leidis, et algoritmilise järjestamise tulemusel välistati teatud töötajad vahetuste valikust, mis otseselt mõjutas nende sissetulekut ja töövõimalusi. Kuigi otsused ei muutnud töötajate formaalset õiguslikku staatust, oli nende mõju praktiliselt samaväärne õiguslike tagajärgedega, kuna need mõjutasid isiku toimetulekut ja võimalust elatist teenida. Andmekaitseasutus rõhutas, et sellise automatiseeritud otsustusamise rakendamine artikli 22 kontekstis eeldab läbipaistvust, vaidlustamisvõimalust ning õiglast kohtlemist. Deliveroo juhtum kinnitab, et majandusliku olukorra või töövõimaluste oluline mõjutamine võib olla piisav, et määratleda mõju „samaväärselt märkimisväärsena“ GDPR artikli 22 mõistes.[70]

Sõidujagamisplatvormi automatiseeritud otsuse „samaväärselt märkimisväärse mõju“ käsitles Amsterdami esimese astme kohus 2021. aastal ka Ola juhtumis, kus vaidlus keskendus kahele erinevale automatiseeritud otsusele:
1. trahvide või tasude mahaarvamise otsused, mis põhinesid juhi tulemusandmetel (nt töökiirus, täpsus, tagasiside),
2. sõitude jaotamine reisijate ja juhtide vahel, mis toimus samuti algoritmiliselt.[71]

---

[68] Gerechtshof Amsterdam 2023, Uber.
[69] Samas.
[70] Itaalia Andmekaitseamet, *Deliveroo.*
[71] Rechtbank Amsterdam, 11. märts 2021, *Ola*, ECLI:NL:RBAMS:2021:1019.

Kohus leidis, et esimene neist – trahvide määramine või sõidutasude vähendamine – mõjutas juhte majanduslikult ja oli seotud nende lepinguliste kohustuste täitmise hindamisega. Seetõttu oli sellel samaväärselt märkimisväärne mõju, mis tõi kaasa GDPR artikli 22 kohaldamise. Vastupidiselt sellele ei hinnatud teist tüüpi algoritmilist otsust (sõitude jaotamist) piisavalt oluliseks – seda peeti ajutiseks ja vahetu mõjuga otsuseks, millel ei olnud pikaajalist ega püsivat mõju töötaja õigustele.[72]

Ola kaasus näitab, et isegi ühe ja sama platvormi eri funktsioonid võivad mõjutada andmesubjekte erineval määral. Kohus rõhutas, et kui automatiseeritud otsus mõjutab oluliselt isiku sissetulekut või töötingimusi, peab ettevõte tagama läbipaistvuse ning võimaluse inimlikuks sekkumiseks.[73]

Uberi, Deliveroo ja Ola juhtumid illustreerivad selgelt, et GDPR artikli 22 kohaldamisel ei saa automatiseeritud otsuse mõju hinnata pelgalt formaalsete tunnuste põhjal, vaid see eeldab sisulist, juhtumipõhist ja mitmetasandilist analüüsi. Kuigi Uberi juhtumis jõudis esimese astme kohus järeldusele, et konto deaktiveerimisel ei olnud püsivat õiguslikku mõju, leidis apellatsioonikohus, et lepingulise suhte katkemine ning juurdepääsu kaotus platvormile kujutas endast nii õiguslikku kui ka majanduslikult olulist tagajärge. Deliveroo kaasuses mõjutas automatiseeritud töövahetuste jaotamise süsteem töötajate sissetulekut ja töövõimalusi, mis kvalifitseerus „samaväärselt märkimisväärse“ mõjuna. Ola juhtum tõi esile, et isegi ühe ja sama platvormi erinevad otsustusprotsessid võivad anda erineva tulemuse: trahvide määramist peeti piisavalt mõjusaks artikli 22 tähenduses, sõitude jaotamist aga mitte. Mõju hindamisel tuleb arvesse võtta otsuse kestvust, mõju pöörduvust, selle mõju isiku õigustele, majanduslikule olukorrale, valikuvõimalustele ja sotsiaalsele positsioonile.[74]

Kokkuvõttes toob artikli 22 lõike 1 kohaldamine kaasa mitmekihilisi tõlgendusprobleeme – alates otsuse ja automatiseerituse piiritlemisest kuni mõju sisulise hindamiseni. Kuigi määruse tekst näib selge, on kohtupraktika ja järelevalveasutuste kogemus näidanud, et tõlgendus sõltub nii tehnoloogilisest keerukusest kui ka organisatsiooni sisemisest tööjaotusest ja dokumenteeritusest. Veelgi enam, andmesubjektide kaitse ei sõltu üksnes sellest, kas otsus oli automatiseeritud, vaid ka sellest, kui läbipaistev, õiglane ja vaidlustatav see oli.

---

[72] Rechtbank Amsterdam 2021, *Ola.*
[73] Samas.
[74] Barros Vale, Zanfir-Fortuna, viidatud raport, lk 35-37.

Seetõttu on põhjendatud jätkata analüüsi järgmistes peatükkides, keskendudes eraldi läbipaistvuse ja selgitusõiguse (ptk 2.1), diskrimineerimisriski ja õigluse (ptk 2.2), õiguslike aluste (ptk 2.3) ning andmesubjektide õiguste tegeliku teostatavuse (ptk 2.4) üksikasjalikule käsitlusele. Need aspektid on lahutamatult seotud artikli 22 rakendamisega ja moodustavad selle tõhusa kohaldamise.

Kuna läbipaistvuse ja selgitusõiguse probleemid on eelduseks andmesubjektide õiguste realiseerimisele ja võimaldavad tuvastada automatiseeritud süsteemide võimalikke õiguslikke ja eetilisi riske, alustatakse analüüsi nende teemade käsitlemisega.

2. GDPR-i PÕHIMÕTETE RAKENDAMISE PROBLEEMID TI-PÕHISTES AUTOMATISEERITUD OTSUSTES

Tehisintellekti süsteemidel põhinevad automatiseeritud otsused võivad olla kallutatud, ebatäpsed või diskrimineerivad ning riivata privaatsust.[75] GDPR sätestab, et isikuandmete töötlemine – sealhulgas automatiseeritud otsuste tegemine – peab olema seaduslik, õiglane ja läbipaistev (art 5 lg 1 p a). Oluline on mõista ja selgitada TI-süsteemide toimimisloogikat ehk algoritmilist läbipaistvust, sest see võimaldab hinnata otsuste õiglust ning tuvastada ja korrigeerida süsteemivigu. Läbipaistvus on seega võtmetegur mitte ainult õigluse, vaid ka vastutuse ja diskrimineerimisvabaduse tagamisel.[76] Siiski praktikas kaasneb nende põhimõtete rakendamisega mitmeid väljakutseid, mida käsitletakse põhjalikumalt selles peatükis.

2.1. Läbipaistvus ja selgitatavus versus algoritmide läbipaistmatus

GDPR seab isikuandmete töötlemise läbipaistvuse üheks põhinõudeks, mis tähendab, et andmetöötlejad peavad teavitama andmesubjekte nende isikuandmete töötlemisest selgelt ja kergesti ligipääsetaval viisil (art 12 lg 1). Vastutav töötleja on kohustatud andma teavet töötlemise kohta kas andmete kogumise hetkel, kui need saadakse otse isikult (art 13), või kindlaksmääratud aja jooksul, kui andmed on saadud kaudselt (art 14 lg 3).[77]

Andmesubjektil on õigus saada teavet nii otsust tegeva süsteemi loogika kui ka otsuse olulisuse ja tagajärgede kohta (art-d 13 lg 2 p f, 14 lg 2 p g, 15 lg 1 p h). Vastutav töötleja peab leidma selged ja lihtsasti mõistetavad viisid, et selgitada andmesubjektile automatiseeritud otsustusprotsessi loogikat või otsuste aluseks olnud kriteeriume. GDPR nõuab sisulist teavet kasutatud loogika kohta – mitte tingimata keerulist algoritmilist selgitust ega kogu algoritmi avaldamist. Oluline on, et andmesubjekt mõistaks otsuse langetamise põhimõtteid ja tagamaid. Lisaks tuleb selgitada töötlemise tähtsust ja eeldatavaid tagajärgi – see tähendab, anda ülevaade sellest, millist mõju võib automatiseeritud otsus avaldada

[75] Cotogni, lk 417.
[76] Chaudhary, G. Unveiling the Black Box: Bringing Algorithmic Transparency to AI. – Masaryk University Journal of Law and Technology 2024, Vol. 18 No. 1, lk 93-94.
[77] EDPB 2018, Guidelines on ADM and Profiling, lk 9-10.

andmesubjektile. Sellise teabe arusaadavaks tegemisel on soovitatav kasutada konkreetseid ja elulisi näiteid, mis aitavad töötlemise mõju selgemalt esile tuua.[78]

Lisaks sisulisele läbipaistvusele tuleb tähelepanu pöörata ka teabe esitamise vormile. Euroopa Andmekaitsenõukogu läbipaistvuse suunise kohaselt peab teave olema esitatud nähtaval ja arusaadaval kujul ning olema kergesti ligipääsetav, vältides olukorda, kus oluline info on peidetud pikkadesse privaatsustingimustesse. Läbipaistvuse saavutamisel on määrava tähtsusega selge ja lihtne keel. Automatiseeritud töötlemise selgitused ei tohiks sisaldada üksnes tehnilisi termineid, vaid peaksid tooma arusaadava paralleeli, näiteks kirjeldades automatiseeritud otsustusprotsessi igapäevase olukorra kaudu. Selline keelekasutus aitab andmesubjektil, kellel puudub tehniline taust, mõista töötlemise olemust.[79]

Läbipaistvuse eesmärk ei ole pelgalt informeerimine, vaid andmesubjekti võimestamine. GDPR põhjenduspunkt 39 ja artikkel 5 lõige 1 punkt a sätestavad, et läbipaistvus on eeltingimus, et andmesubjekt saaks oma õigusi realiseerida. Kuid suunis täpsustab, et läbipaistvus tähendab ka õiguste kasutamise võimaldamist, mitte pelgalt kohustuse formaalset täitmist.[80]

GDPR pakub kolm võimalikku õiguslikku alust, millele tuginedes võib andmesubjektil olla õigus saada selgitusi automatiseeritud otsuste kohta:
1. Kaitsemeetmed – artikli 22 lõige 3 koos põhjenduspunktiga 71 viitab sellele, et andmesubjekti kaitseks tuleb rakendada sobivaid meetmeid, sealhulgas anda teavet otsustusprotsessi kohta.
2. Teavitamiskohustused – artiklid 13 ja 14 ning põhjenduspunktid 60–62 sätestavad, et andmesubjektile tuleb esitada arusaadav ja asjakohane teave automatiseeritud töötlemise kohta, sealhulgas selle loogika ja mõjude kohta.
3. Andmetega tutvumise õigus – artikli 15 ja põhjenduspunkti 63 kohaselt on andmesubjektil õigus saada teavet selle kohta, kas teda puudutav otsus on tehtud automatiseeritult, ning saada selgitusi kasutatud loogika ja võimalike tagajärgede kohta.[81]

---

[78] EDPB 2018, Guidelines on ADM and Profiling, lk 24-29.
[79] European Data Protection Board (EDPB). Guidelines on Transparency under Regulation 2016/679, WP260 rev.01, endorsed by the EDPB on 11 April 2018, initially adopted by the Article 29 Working Party on 29 November 2017, lk 8-12.
[80] Samas, lk 5.
[81] Wachter, S., Mittelstadt, B., Floridi, L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. – International Data Privacy Law 2017, Vol. 7, No. 2, lk 79.

GDPR-is mainitakse õigust selgitusele otsesõnu ainult põhjenduses 71. Seetõttu on osad eksperdid seisukohal, et kuna põhjendused ei ole õiguslikult siduvad, siis ei tulene GDPR-ist andmesubjekti õigust selgitusele, vaid selle asemel on õigus olla informeeritud. Artiklid 13–14 sätestavad andmetöötleja teavitamiskohustuse, samas kui artikkel 15 annab andmesubjektile aktiivse õiguse seda teavet taotleda.[82] Siiski on leitud, et õigust selgitusele võib tuletada GDPR-i ülesehitusest ja eesmärgist, kuna läbipaistvus on vajalik õiguste realiseerimiseks. Eksperdid rõhutavad, et GDPR-i põhjendused aitavad selgitada õigusnormide tähendust ja kohaldamisulatust. Ehkki neil ei ole iseseisvat õigusjõudu, annavad need olulisi suuniseid määruse tõlgendamiseks ja rakendamiseks.[83]

Kokkuvõttes on võimalik tuua esile tugevaid argumente nii õiguse selgitusele olemasolu kui ka selle formaalse puudumise kasuks. Kuid tõlgendades GDPR-i üldpõhimõtteid ning läbipaistvuse ja õiguste realiseerimise eesmärki, näib põhjendatum seisukoht olevat, et andmesubjektil on sisuline õigus saada selgitust teda puudutava automatiseeritud otsustamise kohta. Selline tõlgendus tagab, et läbipaistvuse põhimõte ei jää üksnes formaalseks nõudeks, vaid toetab andmesubjekti tegelikku võimalust mõista ja vaidlustada teda mõjutavaid automatiseeritud otsuseid. Lisaks aitab see tõlgendus tugevdada andmekaitse taset ning suunab vastutavaid töötlejaid rakendama tõhusaid ja sisulisi teavitamismeetmeid.

Kuid algoritmide olemus tekitab tõsiseid praktilisi probleeme, kuna tehisintellektisüsteemid on sageli nn musta kasti tüüpi lahendused – nende otsustusprotsessi ei ole isegi spetsialistidel lihtne mõista. Mustad kastid tähistavad süsteeme, mille arvutuslikud protsessid on sedavõrd keerulised, et muutuvad kasutajate (sh arendajate) jaoks raskesti jälgitavaks ja mõistetavaks.[84]

Lisaks sellele, et algoritmide otsustusprotsessi selgitamine on tehniliselt keeruline probleem, on tõenäoline, et andmesubjektid ei saaks sellistest selgitustest märkimisväärset kasu, kuna need võivad olla liiga keerulised ja spetsiifilised.[85] Mõistmise võib keerukaks teha ka asjaolu, et profiilianalüüs põhineb sageli tuletatud andmetel.[86] Seega seisneb väljakutse selles, kuidas

[82] Wachter, Mittelstadt, Floridi, lk 79-90.
[83] Chaudhary, lk 100-103.
[84] Cotogni, lk 439.
[85] Chaudhary, lk 103.
[86] EDPB 2018, Guidelines on ADM and Profiling, lk 9-10.

pakkuda mõistetavat selgitust andmesubjektile juhul, kui otsuse aluseks või tegijaks on keeruline TI-süsteem.

Lisaks algoritmide keerukusest ja ettearvamatusest tulenevatele tehnilistele takistustele tuleb arvestada ka õiguslike ja regulatiivsete probleemidega. Ettevõtted soovivad piirata teatud detailide avalikustamist, et kaitsta ärisaladusi ja intellektuaalomandit. Kuna algoritmid kujutavad endast olulist konkurentsieelist, ei ole ettevõtted valmis avaldama teavet oma vara kohta. Privaatsuse ja turvalisuse eksperdid rõhutavad, et organisatsioonide sisemise toimimise avalikustamine võib suurendada küberrünnakute riski, mistõttu on vaja tagada tasakaal läbipaistvuse ja turvalisuse vahel. Teabe kättesaadavust tuleb piirata riigisaladuste kaitseks ning avalike huvide korral tuleb teha kaalutletud otsus, lähtudes konkreetse juhtumi oludest.[87]

Lisaks tehnilistele ja juriidilistele takistustele on oluline arvestada ka sellega, kas edastatav teave on andmesubjekti jaoks sisuliselt tähenduslik ja mõistetav. GDPR ei pruugi tagada piisavalt tugevat de facto läbipaistvust automatiseeritud otsustes, eriti kui tegemist on keerukate masinõppe mudelitega, mille sisemist loogikat on raske või isegi võimatu selgitada tavakasutajale mõistetaval viisil. Kuigi õiguslik raamistik (nt art 15 või art 22 lg 3) näeb ette teabe edastamise, ei pruugi see alati tagada, et andmesubjekt saab tähenduslikku teavet. Seetõttu võib tema võimalus oma õigusi tõhusalt kasutada jääda piiratud. Selline normatiivne läbipaistvus ei taga alati sisulist läbipaistvust andmesubjekti vaatenurgast. Seetõttu on oluline keskenduda sellele, kuidas teavet esitatakse ning millisel viisil see aitab andmesubjektil oma õigusi realiseerida.[88]

GDPR põhjenduspunkt 63 märgib, et teiste isikute õigusi (sh intellektuaalomandit ja tarkvara autoriõigusi) tuleb küll arvestada, kuid see ei tohi kaasa tuua teabe andmesubjektile andmisest täielikku keeldumist. Seega ärisaladusele tuginemine on piiratud ning algoritmide töö kohta peab avaldama vähemalt põhialused. See tekitab siiski konflikte võimaliku ärisaladusega ning mitmes praktilises vaidluses on see teema juba tõstatunud. Näiteks eelpool käsitletud Uberi ja Ola kaasustes (vt ptk 1.3.1. ja 1.3.2.) püüdsid ettevõtted kohtus põhjendada, et nad ei pea algoritmi toimimise infot täielikult avaldama, viidates ärisaladusele.

---

[87] Chaudhary, lk 106-107.

[88] Wachter, S., Mittelstadt, B., Russell, C. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. – Harvard Journal of Law & Technology 2018, Vol. 31 No. 2, lk 861–863.

Ola kohtuasjas käsitles Amsterdami esimese astme kohus ärisaladusele viitamist seoses andmesubjektide õigusega saada teavet nende kohta tehtud automatiseeritud otsuste ja profileerimise kohta. Ola püüdis piirata teabe andmist, viidates vajadusele kaitsta oma teenuse toimemehhanisme, algoritmilisi hinnanguid ja sisekorra tagamise meetmeid. Ettevõte tugines GDPR artikli 15 lõikele 4, mille kohaselt võib keelduda isikuandmete koopia edastamisest, kui see kahjustaks teiste isikute õigusi või vabadusi – näiteks ärisaladust või süsteemide turvalisust.[89]

Kohus rõhutas, et artikli 15 lõike 4 rakendamine eeldab konkreetset ja hästi põhjendatud selgitust, miks läbipaistvuse võimaldamine ohustaks olulisi õigusi. Pelgalt üldsõnaline viide ärisaladusele ei ole piisav keeldumiseks. Kuna Ola ei suutnud näidata, et läbipaistvus ohustaks otseselt süsteemi terviklikkust või turvalisust, leidis kohus, et teatud isikuandmete (sh profiilide koostamise sisendandmete ja otsustuskriteeriumide) osas tuleb ligipääs võimaldada. Kohus rõhutas, et läbipaistvus on vajalik selleks, et andmesubjekt saaks kontrollida andmete töötlemise seaduslikkust ja kaitsta oma õigusi, mistõttu ärisaladuse kaitse ei saa seda õigust ebaproportsionaalselt piirata.[90]

2023. aastal leidis Amsterdami apellatsioonikohus, et teave Uberi algoritmiliste otsustusprotsesside tööpõhimõtete kohta on hädavajalik töötajate õiguste kaitseks. Uber põhjendas keeldumist ärisaladuse kaitsega. Kohus aga leidis, et platvormi keeldumine sellist teavet jagada oli ebaproportsionaalne, kuna algoritmilised otsused olid juba toonud kaasa konkreetseid tagajärgi – nimelt juhtide töölepingu lõpetamisi. Kohus rõhutas, et läbipaistvuse puudumine ei võimaldanud töötajatel oma õigusi tõhusalt kaitsta. Seetõttu ei kaalu ärisaladuse kaitse üles töötajate õigust saada selgitust nende lepingulise suhte lõpetamise aluseks olnud automatiseeritud otsuste kohta.[91]

SCHUFA Holding kohtuasjas analüüsis Euroopa Kohus andmesubjekti õigust saada teavet automatiseeritud otsuste tegemisel kasutatud isikuandmete töötlemise loogika kohta. Saksamaal tegutsev krediidiregistri pidaja SCHUFA Holding AG arvutas inimese krediidivõimekust spetsiaalsete algoritmide abil, andes tulemuseks skoori ehk

[89] Rechtbank Amsterdam 2021, *Ola*.
[90] Samas.
[91] Gerechtshof Amsterdam 2023, *Uber*.

tõenäosusväärtuse, mille põhjal otsustatakse, kas isik saab krediiti või millistel tingimustel ta seda saab. Andmesubjekt palus SCHUFA-lt selgitust selle kohta, kuidas tema skoor arvutati, sh algoritmi ja arvutamise tegureid. SCHUFA keeldus, põhjendades seda sellega, et konkreetse arvutamise loogika ja tegurite avalikustamine kujutab endast ärisaladust.[92]

Kohus leidis, et GDPR artikkel 15 annab isikule õiguse teada saada, et tema suhtes toimub automatiseeritud otsustamine. See õigus hõlmab ka üldist selgitust otsustamise loogikast ja kasutatud tegurite kategooriatest. Samas kinnitas kohus, et artiklist 15 ei tulene absoluutset õigust saada teavet algoritmi konkreetsete detailide kohta, eriti juhul, kui teabe avaldamine võib kahjustada ettevõtte ärisaladusi või intellektuaalset omandit. Oluline on saavutada tasakaal andmesubjekti õiguse vahel saada piisavalt teavet oma andmete töötlemisest ja ettevõtte õigustatud huvi vahel kaitsta ärisaladust. Andmesubjektile tuleb siiski võimaldada arusaadavas vormis info selle kohta, millist tüüpi andmed ja üldised tegurid mõjutasid tema krediidiskoori, ilma et see tähendaks algoritmi detailide täielikku avaldamist.[93]

2023. aastal määras Berliini andmekaitse järelevalveasutus trahvi ühele pangale, kuna see keeldus avaldamast kliendile automaatselt tehtud krediitkaardiotsuse põhjendusi, viidates vajadusele kaitsta ärisaladust ja sisemisi otsustusreegleid. Järelevalveasutus rõhutas, et automaatotsuste kasutamisel tekib vastutajal eriline läbipaistvuskohustus: tuleb esitada konkreetset infot kasutatud andmebaasi, otsust mõjutanud tegurite ja kriteeriumide kohta, et isik saaks otsusest aru ja saaks seda vaidlustada. Antud juhul leidis järelevalve, et panga tegevus rikkus läbipaistvuse ja õigluse põhimõtet (GDPR art 5 lg 1 p a), samuti andmesubjekti ligipääsuõigust loogikainfole (art 15 lg 1 p h) ning artikli 22 lg 3 nõudeid, ning määras pangale 300 000 € suuruse trahvi.[94]

Kohtulahendid ja järelevalvepraktika näitavad, et kuigi GDPR ei sätesta täpselt, kui põhjalik peab andmesubjektile antav selgitus olema, on regulatiivne suundumus liikumas suurema läbipaistvuse nõude suunas. See tähendab, et andmesubjektile ei piisa pelgast teavitamisest automatiseeritud töötlemise olemasolu kohta – talle tuleb esitada ka sisulist ja mõistetavat teavet kasutatud loogika ning otsuste tagajärgede kohta.

[92] EKo C-634/21, SCHUFA Holding AG.
[93] Samas.
[94] Berliini Andmekaitseamet. Otsus 31. mai 2023.

Samas jääb praktikas ebaselgeks, millises mahus ja millist laadi teavet peab edastama, et see oleks piisav GDPR-i nõuete täitmiseks. Tõlgendusruum loob ebakindlust nii andmetöötlejatele kui ka järelevalveasutustele. Kuid selge on see, et pelk ärisaladusele või sisemistele protsessidele viitamine ei vabasta läbipaistvuskohustusest.

Teabele juurdepääs on kujunenud TI-põhiste otsustussüsteemide reguleerimise keskseks küsimuseks. See on oluline nii järelevalveasutuste ja audiitorite tööks, kes hindavad süsteemide toimimist ja riske, kui ka andmesubjektide jaoks, kes vajavad mõistlikku selgitust, et oma õigusi kasutada.[95]

Läbipaistvuse üks sageli alahinnatud aspekt on teavitamine üldse sellest, et otsuse langetab algoritm. Mitmed probleemid on tekkinud olukordades, kus inimesed ei ole teadlikud, et nende üle otsustab automatiseeritud süsteem, mitte inimene. GDPR artiklid 13–14 püüavad seda riski maandada, nõudes teavitust juba andmete kogumisel või kindlaks määratud aja jooksul.

Praktikas on need teavitused sageli formaalsed ning esitatud keerulises juriidilises keeles, näiteks privaatsustingimustes, kus neid ei loeta või ei mõisteta. Seetõttu võivad andmesubjektid sellisest infost mööda vaadata ega teadvusta, et nende kohta langetati otsus automaatselt. See toob esile praktilise väljakutse: kuidas kujundada selgitusviisid ja -kanalid nii, et algoritmide toimimine oleks tavakasutajale nähtav ja arusaadav.

Teadmatus või segadus algoritmilise otsustamise osas võib õõnestada usaldust tehisintellekti ja selle kasutava organisatsiooni vastu.[96] Sellest tulenevalt arutletakse põhjalikumalt peatükis 3.2.1. selgitatava tehisintellekti (*explainable AI*) meetodite üle, mille eesmärk on muuta ka keerulised nn musta kasti mudelid inimestele mõistetavamaks.

Algoritmilise läbipaistvuse eesmärk on mitte ainult TI-süsteemide toimimise ja otsustusprotsessi mõistmine ning selgitamine, vaid ka õigluse ja diskrimineerimise vältimise tagamine. Kui me ei tea, kuidas AI-süsteem otsuseid langetab, on võimatu hinnata, kas selle

[95] Chaudhary, lk 107.
[96] Cotogni, lk 418.

tulemused kohtlevad kõiki inimesi võrdselt. Seetõttu sätestab GDPR, et lisaks läbipaistvusele peab andmete töötlemine olema õiglane (art 5 lg 1 p a).

2.2. Diskrimineerimisrisk ja võrdse kohtlemise tagamine TI-põhistes otsustes

Algoritmilise läbipaistvuse eesmärk ei piirdu üksnes TI-süsteemide toimimise ja otsustusloogika mõistmisega. Selle sügavam tähendus seisneb ka õigluse ja võrdse kohtlemise tagamises. Kui ei ole teada, kuidas algoritm otsuseid langetab, on võimatu hinnata, kas otsused kohtlevad kõiki inimesi võrdselt või tekitavad varjatud ebaõiglust.[97] Seetõttu sätestab GDPR, et andmete töötlemine peab lisaks läbipaistvusele olema ka õiglane (art 5 lg 1 p a), vältides diskrimineerivaid ja ebaõiglasi tulemusi.[98] Ehkki GDPR-i põhjenduspunktis 39 ja artiklis 5 lg 1 p a öeldakse, et isikuandmeid tuleb töödelda õiglaselt (õigluse põhimõte), ei selgita määrus, mida õiglus tähendab ning kuidas seda saavutada.[99]

Õiglust liigitatakse tavaliselt kaheks: menetluslikuks ja sisuliseks. Menetluslik õiglus keskendub otsuse tegemise protsessi õiguspärasusele. Andmekaitseõiguses tähendab see eelkõige seda, kas isikuandmeid on kogutud või muul viisil töödeldud ebaausate võtetega – näiteks petlikult või andmesubjekti teadmata. Sisuline õiglus seevastu keskendub andmetöötluse tulemustele ja nende mõjule andmesubjektidele. Need tagajärjed ja mõjud võivad hõlmata andmesubjektide ootusi, kasulikke või kahjulikke tagajärgi ning osapoolte tegelikke huve.[100] Õigluse mõiste GDPR-is tuleb seetõttu mõista mitte üksnes formaalse protseduuri järgimisena, vaid ka sisuliselt tasakaalustava põhimõttena, mis eeldab, et andmetöötlus ei kahjustaks ebaproportsionaalselt haavatavaid gruppe või looks varjatud ebaõiglust.[101]

GDPR sätestab menetlusliku õigluse nõudeid näiteks läbipaistvuse (art 5 lg 1 p a), turvameetmete (art 5 lg 1 p f) ja andmesubjekti õiguste tagamise (art-d 12–22) kaudu.[102]

---

[97] Chaudhary, lk 93.
[98] EDPB 2018, Guidelines on ADM and Profiling, lk 9-10.
[99] Häuselmann, A., Custers, B. Substantive fairness in the GDPR: Fairness Elements for Article 5.1a GDPR. – Computer Law & Security Review 2024, Vol. 52, lk 2.
[100] Samas, lk 2-4.
[101] Malgieri, G. The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation. – Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20), January 27–30, 2020, ACM, New York, lk 154 jj.
[102] Häuselmann, Custers, lk 3-4.

Diskrimineerimise vältimiseks on keelatud töödelda eriliigilisi isikuandmeid, nagu päritolu, vaated, uskumused, seksuaalsus ja terviseandmed (art-d 9 ja 22 lg 4). Kuna selliste andmete töötlemisel on suurem diskrimineerimise oht, aitab nende töötlemise piiramine kaudselt vältida diskrimineerimist.[103] Samas on tõstatatud küsimus, kas tundlike andmete töötlemise range piiramine võib paradoksaalselt takistada diskrimineerimise tuvastamist. Näiteks ei pruugi olla võimalik kontrollida, kas automatiseeritud otsused on eelarvamuslikud, kui puuduvad andmed rassi või usutunnistuse kohta, mis võimaldaksid läbi viia süsteemset auditit.[104]

Siiski sätestab GDPR ka olukorrad, kus eriliigiliste isikuandmete töötlemine on lubatud. Artikkel 22 lg 4 kohaselt on eriliigilistel andmetel põhinev automatiseeritud üksikotsuste tegemine lubatud, kui andmesubjekt on andnud selgesõnalise nõusoleku nende isikuandmete töötlemiseks või kui töötlemine on vajalik olulise avaliku huvi tõttu ning kehtestatud on asjakohased meetmed andmesubjekti õiguste, vabaduste ja õigustatud huvide kaitsmiseks. Artikkel 9 lg 2 annab veel rohkem aluseid eriliigiliste isikuandmete töötlemiseks, nagu näiteks töötlemine tööõigusest või sotsiaalkaitseõigusest tulenevate kohustuste täitmiseks või andmesubjekti eluliste huvide kaitsmiseks.

Sisulist õiglust käsitleb GDPR palju vähem selgelt, kuid viitab sellele siiski töötlemistoimingu tulemuse või mõju kaudu. Näiteks, kui andmetöötleja kavatseb töödelda isikuandmeid muul eesmärgil kui see, milleks need algselt koguti, tuleb arvesse võtta sellise täiendava töötlemise võimalikud tagajärjed (art 6 lg 4 p d ja põhjenduspunkt 50). Lisaks nõuded, et andmesubjektile antakse teavet automatiseeritud otsuste tegemise ja profiilianalüüsi eeldatavate tagajärgede kohta (art-d 13 lg 2 p f ja 14 lg 2 p g), andmetöötleja peab hindama kavandatava töötlemise mõju isikuandmete kaitsele, kui töötlemisel võib olla suur oht füüsiliste isikute õigustele ja vabadustele (art 35 lg 1) ja järelevalveasutused peavad GDPR-i rikkumise eest halduskaristust määrates arvestama tagajärgi, mis rikkumisega kaasnesid (põhjenduspunkt 150).[105] Sellised sätted viitavad sellele, et õigluse nõue GDPR-is ei ole pelgalt abstraktne, vaid seotud konkreetsete tagajärgede ja ohtudega andmesubjekti seisukohast.[106]

---

[103] Wiedemann, K. Profiling and (automated) decision-making under the GDPR: A two-step approach. – Computer Law & Security Review 2022, Vol. 45, lk 8-9.
[104] van Bekkum, M., Zuiderveen Borgesius, F. Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? – Computer Law & Security Review 2023, Vol. 48, lk 2 jj.
[105] Häuselmann, Custers, lk 3-4.
[106] Malgieri, lk 163.

Sisuline õiglus on seotud ka osapoolte vahelise tegeliku õiglusega, tasakaalustades ebavõrdseid olukordi. Andmetöötleja ja andmesubjekti vahelise suhte tasakaalu rõhutab GDPR-i artikkel 6 lg 4 p b ja põhjendus 50, mille kohaselt peab andmetöötleja arvesse võtma oma suhet andmesubjektiga, kui ta soovib andmeid töödelda muul kui esialgse kogumise eesmärgil.[107] Seda toetab ka Malgieri, kelle hinnangul tähendab õiglus GDPR-is rohkem kui menetluslike sammude järgimist – see peab hõlmama sisulist tasakaalu andmetöötleja ja andmesubjekti huvide vahel, eriti kui tegemist on haavatavate isikurühmadega.[108]

Siiski keskendub GDPR eeskätt menetluslikele nõuetele, mille järgimine peaks levinud käsitluse kohaselt tagama andmetöötluse lubatavuse ja õigluse. Selline eeldus võib siiski olla ekslik. Ehkki määrus nõuab, et isikuandmete töötlemine oleks õiglane (art 5 lg 1 p a), ei täpsusta GDPR õiglusnõude sisu ega anna juhiseid selle rakendamiseks. Kuna määruses puudub sisulise õigluse eraldi käsitlus, võib andmetöötlus vastata küll formaalsetele menetlusnõuetele, kuid olla siiski sisuliselt ebaõiglane.[109]

Euroopa Komisjoni kõrgetasemeline tehisintellekti ekspertgrupp rõhutab oma suunises „Usaldusväärse tehisintellekti eetikasuunised“, et tehisintellekti, sealhulgas automatiseeritud otsuste süsteemide arendamine ja kasutamine peab olema õiglane nii sisulisel kui ka menetluslikul tasandil.[110] Need suunised toetavad seisukohta, et pelgalt menetlusnõuete järgimine ei pruugi tagada andmetöötluse sisulist õiglust.

Kuid tehisintellektil põhinevad automatiseeritud otsused võivad tahtmatult viia andmesubjektide ebavõrdse kohtlemiseni ning tugevdada sotsiaalset ebavõrdsust. Kuigi algoritme peetakse sageli objektiivseks ja inimlikest eelarvamustest vabaks, on need siiski inimeste loodud ning treenitud ajalooliste andmete põhjal, mis võivad peegeldada sügavalt juurdunud sotsiaalseid eelarvamusi ning sellega kaasa aidata diskrimineerimise ja ebaõigluse süvenemisele. Seetõttu kanduvad andmetes sisalduvad kallutused üle ka otsustesse, mille tulemuseks võib olla süsteemne ebaõiglus. Näiteks võib vähemusgruppide alaesindatus treeningandmestikes viia selleni, et neid gruppe diskrimineeritakse tulevikus töölevõtmisel või maksevõime hindamisel. Kuigi GDPR sätestab artikli 22 lõikes 1 piirangu automatiseeritud üksikotsuste tegemisele, keskendub see säte üksikisiku tasandile ega käsitle

[107] Häuselmann, Custer, lk 4.
[108] Malgieri, lk 154jj.
[109] Häuselmann, Custer, lk 1-12.
[110] Euroopa Komisjoni kõrgetasemeline tehisintellekti ekspertgrupp. *Ethics Guidelines for Trustworthy AI*. 8.aprill 2019, lk 14.

piisaval määral olukordi, kus otsused võivad diskrimineerida terveid inimrühmi.[111] Seda piirangut on kritiseerinud mitmed autorid, kelle hinnangul peaks GDPR käsitlema ka nn kollektiivset diskrimineerimist – olukorda, kus süsteem mõjutab ebaõiglaselt tervet rühma, isegi kui üksikjuhtumi tasandil seda pole lihtne tõendada.[112]

Diskrimineerivad mustrid võivad algoritmilistes süsteemides kujuneda mitte ainult otsese kallutatuse kaudu, vaid ka kaudselt – läbi õppimise andmetest, mis peegeldavad olemasolevat sotsiaalset ebavõrdsust.[113] Lisaks võivad tundlikud järeldused tekkida ka näiliselt neutraalsetest andmetest – näiteks on uuringus jõutud järeldusele, et inimese Facebooki laikide põhjal suudeti suure tõenäosusega ennustada tema seksuaalset orientatsiooni, rahvust ja religiooni.[114] Seda nähtust süvendab algoritmide läbipaistmatuse probleem ehk nn must kast – süsteemide tööloogika jääb sageli varjatuks nii andmesubjektidele kui ka andmekaitse spetsialistidele, muutes diskrimineerimise tuvastamise ja hindamise keeruliseks.[115] Selline läbipaistmatuse ja eelarvamuste kombinatsioon raskendab tehisintellektil põhinevate otsuste diskrimineeriva mõju tuvastamist ja ennetamist.

Üks kõnekas näide sellest, kuidas algoritmilise läbipaistvuse ja õigluse puudumine võib praktikas ohustada inimõigusi, pärineb Hollandist. SyRI kaasuses pidi kohus hindama, kas riiklik tehisintellektil põhinev süsteem vastas isikuandmete kaitse ning õiglase andmetöötluse põhimõtetele.

SyRI (Systeem Risico Indicatie) on Hollandi valitsuse loodud algoritmiline tööriist, mille eesmärk oli ennetada ja avastada maksu- ja sotsiaaltoetuste pettusi, ühendades mitmete riigiasutuste andmekogusid ja analüüsides neid riskimudeli alusel. 2020. aasta veebruaris tegi Haagi esimese astme kohus pretsedenti loova otsuse, milles tunnistas SyRI kasutamise vastuolus olevaks Euroopa Inimõiguste Konventsiooni[116] (EIÕK) artikli 8 lõikega 2, mis kaitseb õigust eraelu puutumatusele.[117]

---

[111] Castets-Renard, C. Accountability of Algorithms in the GDPR and beyond: A European Legal Framework on Automated Decision-Making. – Fordham Intellectual Property, Media & Entertainment Law Journal 2019, Vol. 30 No. 1, lk 94-125.
[112] van Bekkum, Zuiderveen Borgesius, lk 2 jj.
[113] Castets-Renard, lk 91–101.
[114] EDPB 2018, Guidelines on ADM and Profiling; lk 15 viidatud uuringule: Kosinski, M., Stillwell, D., Graepel, T. Private traits and attributes are predictable from digital records of human behavior. – Proceedings of the National Academy of Sciences of the United States of America 2013, Vol. 110 No. 15, lk 5802–5805.
[115] Castets-Renard, lk 101.
[116]
[117] District Court of The Hague, 5. veebruar 2020, NJCM et al. v. the State of the Netherlands, ECLI:NL:RBDHA:2020:865; vt ka EIÕK art 8 lg 2.

Kohtu hinnangul oli SyRI-l oluline mõju andmesubjektide eraelule, kuna süsteem töötles suures mahus mitmekesist isikuandmestikku, sealhulgas potentsiaalselt tundlikke andmeid, ning võimaldas profiilide koostamist ja riskiraportite genereerimist ilma piisava läbipaistvuse ja kontrollimehhanismideta. Kohus rõhutas, et SyRI süsteemi tööpõhimõtted – sealhulgas kasutatavad riskinäitajad, algoritmilise mudeli loogika ja seoste loomise alused – olid mitteavalikud, mis tähendas, et andmesubjektid ei saanud mõista ega vaidlustada nende kohta tehtavaid riskihinnanguid. See rikkus isikuandmete kaitse põhimõtteid nagu läbipaistvus, andmete minimaalsuse printsiip ja eesmärgipärasus (GDPR art 5 lg 1).[118]

Lisaks tõi kohus esile, et kuna SyRI rakendati valdavalt nn „probleempiirkondades", siis suurendas see diskrimineerimise ja sotsiaalsete eelarvamuste kordumise ohtu. Arvestades töödeldavate andmete ulatust – sealhulgas eriliigilisi isikuandmeid – ning süsteemi sõltuvust riskiprofiilidest, esines reaalne oht kallutatud seoste tekkeks. SyRI võis tahtmatult seostada inimesi teatud tunnustega, näiteks madalama sotsiaalmajandusliku staatuse või immigratsioonitaustaga, mis suurendas diskrimineerimise riski. Samas jättis lahtiseks küsimuse, kas selline riskiraporti koostamine vastab täielikult automatiseeritud individuaalse otsustamise määratlusele GDPR-i artikli 22 tähenduses, ning juhul kui vastab, kas selleks esines õiguslikult aktsepteeritavaid erandeid.[119]

Eelpool käsitletud Deliveroo juhtumis analüüsiti, kuidas TI-põhine automatiseeritud otsuste tegemine võib põhjustada ebaõiglast ja diskrimineerivat kohtlemist platvormitöötajate suhtes. Itaalia andmekaitse järelevalveasutus leidis, et Deliveroo rakendatud algoritm nimega Frank, mis määras kullerite järjestuse tööpakkumisteks, oli ebaõiglane ja diskrimineeriv. Algoritm karistas kullereid puudumiste eest sõltumata puudumise põhjusest (nt haigus, laste hooldamine, streigid), vähendades nende töösaamise võimalusi ja viies neid madalamale positsioonile tulevikus tehtavate tellimuste jaotamisel.[120]

Otsuses rõhutati, et selline automatiseeritud otsustusprotsess peab vastama GDPR-i nõuetele, sealhulgas läbipaistvuse põhimõttele (art 5 lg 1), andmesubjekti teavitamiskohustusele (art 13) ning automatiseeritud otsustamise eriregulatsioonile (art 22). Samuti märkis järelevalveasutus, et Deliveroo oleks pidanud läbi viima andmekaitsealase mõjuhinnangu, mis on nõutav

[118] District Court of The Hague 2020, *NJCM et al. v. the State of the Netherlands.*
[119] Samas.
[120] Itaalia Andmekaitseamet, *Deliveroo*.

GDPR-i artikli 35 kohaselt, kuna tegemist oli ulatusliku, innovatiivse tehnoloogia rakendamisega, mis puudutas haavatavat elanikkonnagruppi.[121]

Kuigi juhtumis käsitleti töötajate õiglast kohtlemist, lahendati see siiski andmekaitse raames GDPR-i alusel, mitte tööõiguse ega võrdse kohtlemise põhimõtte alusel. See juhtum illustreerib riski, kuidas järelevalveta automatiseeritud otsused võivad suurendada ebavõrdset kohtlemist ja luua püsivalt ebasoodsamaid tingimusi.

Seetõttu peab vastutav töötleja ennetavalt tagama, et algoritmilised otsused oleksid GDPR-iga kooskõlas ning õiguspärased, läbipaistvad ja mitte meelevaldsed. Euroopa Andmekaitsenõukogu suunises on välja toodud mitmeid soovituslikke praktikaid, mis aitavad ennetada kallutatust ja tugevdada õiglast andmetöötlust – seda eriti tehisintellektil põhinevate automatiseeritud otsuste puhul. Näiteks soovitatakse regulaarselt hinnata kasutatavaid andmestikke, et tuvastada ja korrigeerida võimalikke kaldeid, korraldada algoritmide auditeid ning testida pidevalt tulemuste täpsust ja neutraalsust.[122]

2.3. Automatiseeritud otsustamise erandid ja nende rakendamise piirid

Artikkel 22 lg 2 loetleb kolm erandit, mille korral automatiseeritud otsuste tegemine on lubatud: a) kui otsus on vajalik andmesubjektiga lepingu sõlmimiseks või täitmiseks, b) kui otsus on lubatud liikmesriigi või EL õigusega, mis ühtlasi sätestab ka sobivad kaitsemeetmed, või c) kui otsus põhineb andmesubjekti selgesõnalisel nõusolekul. Nende erandite rakendamine nõuab põhjalikku õiguslikku kaalutlust, kuna praktikas on sageli keeruline hinnata, kas eeldused selleks on täidetud.

Üheks erandiks on olukord, kus automatiseeritud töötlusel põhinev otsustamine on lepingu sõlmimiseks või täitmiseks vältimatult vajalik (art 22 lg 2 p a). Vajaduse hindamisel tuleb arvestada, et see peab olema objektiivselt mõõdapääsmatu – pelgalt töötlemise otstarbekus või tehniline tõhusus ei ole piisav. Euroopa Andmekaitsenõukogu suunised rõhutavad, et automatiseeritud otsustamine peab olema konkreetses lepingulises olukorras hädavajalik, mitte lihtsalt mugav lahendus. Näiteks võib selline vajadus ilmneda olukorras, kus suur

[121] Itaalia Andmekaitseamet, *Deliveroo*.
[122] EDPB 2018, Guidelines on ADM and Profiling; lk 27-28.

andmemaht muudab manuaalse töötlemise ebapraktiliseks. Lisaks võib automatiseeritud otsustamine olla põhjendatud ka lepingueelses faasis, näiteks maksevõime hindamisel enne lepingu sõlmimist. Kuid töötlejal lasub kohustus tõendada, et alternatiivsed ja vähem eraelu puutumatust riivavad meetodid ei võimaldaks eesmärki samaväärselt saavutada.[123]

Automatiseeritud töötlemise lubatavus artikli 22 lõike 2 punkti a alusel eeldab, et töötlemine oleks ühtlasi kooskõlas GDPR artikli 6 lõike 1 punktiga b. Selle alusel on töötlemine lubatud ainult siis, kui see on objektiivselt vajalik lepingu täitmiseks või lepingueelsete sammude tegemiseks andmesubjekti taotlusel. Nagu Andmekaitsenõukogu suunistes rõhutatakse, ei piisa pelgalt sellest, et töötlemine on mainitud lepingus – see peab olema lepingu sisulise toimimise seisukohalt möödapääsmatu.[124] Sama põhimõtet toetab ka teaduskirjandus: automatiseeritud otsustamine ei või põhineda üksnes lepingutingimustel, vaid peab olema kooskõlas andmekaitse üldpõhimõtetega, sh läbipaistvuse ja proportsionaalsuse nõuetega.[125] Seega automatiseeritud otsustamine ei tohi tugineda lepingule, kui see on vastuolus andmesubjekti põhiõigusi.

Selle kriteeriumi kitsendav tõlgendus leiab kinnitust ka Euroopa Kohtu praktikast. Kohtuasjas Huber vs Saksamaa leiti, et isikuandmete töötlemine peab olema proportsionaalne ning piirduma üksnes sellega, mis on eesmärgi saavutamiseks hädavajalik.[126] Kui eesmärki on võimalik saavutada vähem riivaval viisil, ei ole andmetöötlus õigustatud. Sama lähenemine kehtib ka automatiseeritud otsustamise puhul – tegemist peab olema objektiivselt möödapääsmatu lahendusega, mitte pelgalt tehnoloogiliselt tõhusa valikuga. Vastasel juhul võib selline töötlemine olla ebaproportsionaalne ja andmesubjekti põhiõigusi kahjustav.[127]

Artikkel 22 ei täpsusta, millal on automatiseeritud otsus vajalik lepingu täitmiseks või sõlmimiseks. Seega lasub vajalikkuse hindamine andmetöötlejal. Kui automatiseeritud otsustamise vajalikkust ei hinnata läbipaistvalt ja süsteemselt, tekib risk, et seda rakendatakse ilma tegeliku õigusliku aluseta. Selline olukord võib andmesubjekti jaoks tähendada, et ta ei ole teadlik teda puudutavast otsusest ega saa seda ennetavalt mõjutada. GDPR artikkel 22

---

[123] EDPB 2018, Guidelines on ADM and Profiling; lk 23-24.
[124] European Data Protection Board (EDPB). Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0, 8 October 2019, lk 9jj.
[125] Nišević, M., Sears, A. M., Fosch-Villaronga, E., Custers, B. Understanding the legal bases for automated decision-making under the GDPR. – Research Handbook on EU Data Protection, eds. Kostas, E., Leenes, R., Kamara, I., Edward Elgar Publishing 2022, lk 10.
[126] EKo C-524/06, *Heinz Huber vs. Saksamaa*, ECLI:EU:C:2008:724, p 52.
[127] EDPB 2018, Guidelines on ADM and Profiling, lk 24.

lõige 3 annab andmesubjektile küll õiguse taotleda inimlikku sekkumist, avaldada oma arvamust või otsust vaidlustada, kuid need kaitsemehhanismid rakenduvad alles pärast otsuse tegemist.[128] Seega on töötlejal kohustus mitte ainult vastata formaalsetele tingimustele, vaid ka tagada tegelik läbipaistvus ja ennetav õiguskaitse.[129]

Lisaks jääb GDPR-is määratlemata, kas automatiseeritud otsustamise õiguspäraseks rakendamiseks peab leping olema juba sõlmitud või piisab kavatsusest see sõlmida, see tähendab lepingueelsest suhtest. Selliste olukordade tõlgendamisel tuleb seetõttu tugineda lepinguõigusele, mis aitab kindlaks teha, kas pooltevaheline suhe on õiguslikult siduv.[130] Samuti ei sätesta määrus, millises vormis peab olema sõlmitud leping, mis sisaldab automatiseeritud otsustamist, ega seda, kuidas tagada andmesubjekti teadlik osalus ja tegelik võimalus oma õiguste kasutamiseks. Kuigi artikli 22 lõike 2 punkt a alusel võib selline töötlemine olla õigustatud, ei kujuta lepingus sisalduv automatiseeritud otsustamise klausel endast iseseisvat õiguslikku alust – töötlemine peab vastama kõigile GDPR-i põhimõtetele, sealhulgas läbipaistvusele ja proportsionaalsusele.[131]

Teise erandina on automatiseeritud otsuste tegemine lubatud juhul, kui see põhineb andmesubjekti selgesõnalisel nõusolekul (art 22 lg 2 p c). Nõusolekut reguleeritakse GDPR-i artiklis 4 punktis 11, kus see on määratletud kui „vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega;“. Artiklis 7 sätestatakse täiendavad tingimused kehtiva nõusoleku andmiseks, sealhulgas õigus see igal ajal tagasi võtta.

Siiski ei ole määruses täpsustatud, mida mõistetakse „selgesõnalise nõusoleku“ all artikli 22 kontekstis. Andmekaitsenõukogu on selgitanud, et selgesõnaliseks võib pidada üksnes sellist nõusolekut, mis on antud selgelt väljendatud viisil – näiteks digiallkirjastatud vormi või kirjaliku kinnituse kaudu.[132]

Suunistes on rõhutatud, et sellise nõusoleku kogumiseks tuleb kasutada selgeid ja usaldusväärseid mehhanisme – näiteks kahe- või mitmeetapilist kinnitamist – ning see peab

[128] Nišević Sears jt 2022, lk 9.
[129] EDPB 2018, Guidelines on ADM and Profiling, lk 19-20.
[130] EDPB 2019,.Guidelines on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, lk 4-5.
[131] EDPB 2018, Guidelines on ADM and Profiling, lk 24.
[132] European Data Protection Board (EDPB). Guidelines 05/2020 on consent under Regulation 2016/679, adopted on 4 May 2020, version 1.1, lk 20-21.

olema eraldi muudest nõusolekutest. Seejuures eraldi nõusolek tuleb koguda iga konkreetse töötlemise eesmärgi jaoks (nt profiilianalüüs, otseturundus), et tagada andmesubjekti teadlik ja konkreetne valik. Nõusoleku lisamine lepingutingimuste hulka või selle muutmine eeltingimuseks teenusele juurdepääsuks, kui töötlemine ei ole objektiivselt vajalik, rikub nõusoleku vabatahtlikkuse põhimõtet ja on vastuolus artikli 7 nõuetega.[133]

Samas tõstatub küsimus, kas isegi nõuetekohaselt antud selgesõnaline nõusolek on piisav kaitsemehhanism automatiseeritud otsuste tegemise kontekstis. Kuigi GDPR nõuab, et nõusolek oleks teadlik, konkreetne ja vabatahtlik, ei taga see iseenesest, et andmesubjektil on sisuline kontroll oma andmete üle. Andmekaitsenõukogu suunistes juhitakse tähelepanu asjaolule, et formaalselt korrektne nõusolek võib praktikas jääda pealiskaudseks, eriti kui puudub piisav läbipaistvus või tegelik valikuvabadus.[134]

Praktikas ongi nõusolek sageli formaalne ega pruugi peegeldada andmesubjekti teadlikku otsust. Inimesed puutuvad igapäevaselt kokku suure hulga nõusolekupäringutega, mistõttu privaatsusteated jäävad sageli lugemata või on raskesti mõistetavad.[135] Selle tulemusel võib andmesubjekt anda nõusoleku teadmata, millega ta täpselt nõustub. Probleemi süvendab asjaolu, et automatiseeritud otsustamise süsteemid on tehniliselt keerukad, ning vastutavad töötlejad ei pruugi suuta (või soovida) selgitada kasutatava algoritmilise loogika olemust.[136]

See võib tähendada, et nõusolek kaotab sisulise tähenduse või osutub kehtetuks, kui andmesubjektil puudub informeeritud otsustamise võimalus. Samuti piirab nõusoleku ulatust asjaolu, et see piirdub andmetega, mida andmesubjekt aktiivselt edastab, samas kui kaasaegsed tehnoloogiad võimaldavad andmeid tuletada või koguda kaudselt – tihti andmesubjekti teadmata.[137]

Eraldi probleemina tõstatub praktikas sageli segadus selgesõnalise nõusoleku ja lepingu alusel toimuva töötlemise vahel. GDPR artikkel 22 lõige 2 eristab selgelt need kaks õiguslikku alust. Ent teenuse kasutamise protsessis esitatud nõusolekuklauslid ei pruugi

[133] EDPB 2020, Guidelines on consent, lk 10-21.
[134] EDPB 2018, Guidelines on ADM and Profiling, lk 25.
[135] EDPB 2020, Guidelines on consent, lk 15–16.
[136] Nišević, Sears jt 2022, lk 15–16.
[137] Samas, lk 16–17.

võimaldada andmesubjektil eristada, kas andmetöötlus toimub tema nõusoleku või lepingu alusel.[138]

Andmekaitsenõukogu suunise kohaselt ei ole nõusolek kehtiv, kui see on seatud teenuse kasutamise eeltingimuseks, kuid ei ole tegelikult vajalik selle teenuse osutamiseks. Näiteks juhul, kui platvormi kasutamiseks nõutakse nõusolekut profileerimiseks, kuigi profileerimine ei ole teenuse toimimiseks hädavajalik, ei saa nõusolekut pidada vabatahtlikuks.[139]

Nõusoleku tagasivõtmine on oluline mehhanism, mille kaudu andmesubjekt saab teostada oma õigusi, sh katkestada automatiseeritud andmetöötlus. Samas kaasnevad sellega mitmed praktilised takistused, mis võivad piirata tagasivõtmise efektiivsust – eriti juhul, kui töötlemine põhineb läbipaistmatul algoritmil või kui teenus muutub ilma andmetöötluseta kasutamiskõlbmatuks.[140] (Nõusoleku tagasivõtmisega seotud probleeme käsitletakse täpsemalt pt 2.4.)

Kolmanda erandina võib GDPR-i artikli 22 lõike 2 punkti b alusel automatiseeritud otsuste tegemise õiguslikuks aluseks olla EL-i või liikmesriigi õigus, kui sellega kehtestatakse asjakohased meetmed andmesubjekti õiguste ja vabaduste ning õigustatud huvide kaitsmiseks. Kuigi GDPR artikkel 22 lõige 3 annab andmesubjektile õiguse taotleda inimlikku sekkumist, esitada oma seisukoht ning vaidlustada automatiseeritud otsus, kehtib see vaid juhul, kui töötlemine toimub artikli 22 lõike 2 punktide a või c alusel. Seega ei sätestata artikli 22 lõike 2 punkt b alusel konkreetseid kaitsemeetmeid ning nende kehtestamine jääb EL-i või liikmesriigi õiguse määrata.

Põhjenduspunkt 71 lubab automatiseeritud otsuste tegemist erinevatel eesmärkidel, näiteks maksupettuste ennetamiseks või teenuste turvalisuse tagamiseks. Kuid põhjenduspunkt 73 viitab sellele, et liikmesriigid võivad avaliku huvi eesmärgil piirata andmesubjektide teatud õigusi (nt teavitamiskohustus või juurdepääsuõigus), näiteks eetikanõuete järgimise või riiklike registrite pidamise korral. Samas jääb ebaselgeks, milline on liikmesriikide ulatus oma siseriiklikus õiguses automatiseeritud otsuste tegemise lubamiseks, sealhulgas millised kaitsemeetmed on minimaalselt nõutavad ja kuidas neid praktikas tagatakse.[141]

---

[138] EDPB 2019,.Guidelines on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, lk 7.
[139] EDPB 2020, Guidelines on consent, lk 9 jj.
[140] Nišević, Sears jt 2022, lk 20.
[141] Samas, lk 12.

Praktilise näitena GDPR artikli 22 lõike 2 punkti b rakendamise piiridest võib tuua eelpool käsitletud SyRI juhtumi. Kuigi SyRI süsteemi automatiseeritud riskiskooride genereerimine põhines liikmesriigi õigusel - Hollandi sotsiaalkindlustusseaduse alusel - ei vastanud see GDPR-is sätestatud nõuetele. Kohus leidis, et puudusid piisavad õiguslikud tagatised, mis kaitseksid andmesubjektide põhiõigusi automatiseeritud andmetöötluse kontekstis, nagu nõuab artikkel 22 lg 2 p b. Kohtuotsuses ei nimetatud selgesõnaliselt, kas SyRI loodud riskiraport kujutab endast automatiseeritud individuaalset otsust artikli 22 tähenduses, kuid leiti, et süsteemil oli oluline mõju andmesubjektide eraelule ning puudus tegelik võimalus oma andmete töötlemisest teada saada või seda vaidlustada. Seetõttu loeti süsteem põhiõigustega vastuolus olevaks, eeskätt proportsionaalsuse ja läbipaistvuse puudumise tõttu.[142]

Kokkuvõttes võib öelda, et automatiseeritud otsustamise lubatavus artikli 22 lõike 2 alusel eeldab erandite väga hoolikat ja põhjendatud rakendamist. Vastutavad töötlejad peavad selgelt dokumenteerima, millisele õiguslikule alusele nad töötlemise puhul toetuvad, ning tagama, et selle aluse rakendamiseks nõutavad eeltingimused on täidetud. Näiteks kui töötlemine põhineb andmesubjekti nõusolekul, peab see olema selgesõnaline, teadlik ja igal ajal tagasivõetav; kui töötlemise alus on leping, peab see olema vältimatult vajalik lepingu täitmiseks; kui automatiseeritud otsus tuleneb seadusest, peab see seadus sisaldama ka piisavaid kaitsemeetmeid andmesubjekti õiguste kaitseks. Vastasel juhul võib töötlemine olla vastuolus mitte ainult GDPR-iga, vaid ka andmesubjektide põhiõigustega, eelkõige õigusega eraelule ja andmekaitsele.

2.4. Andmesubjekti õiguste realiseerimise raskused

GDPR annab andmesubjektile rea õigusi, mille eesmärk on võimaldada tal kontrollida oma isikuandmete kasutamist ning kaitsta teda ebaõiglase või läbipaistmatu andmetöötluse eest. Nende õiguste hulka kuuluvad:

- õigus oma nõusolek tagasi võtta (artikkel 7 lg 3),
- õigus saada teavet ja juurdepääs oma andmetele (artiklid 12–15),
- õigus andmete parandamisele (artikkel 16),

[142] District Court of The Hague 2020, NJCM et al. v. the State of the Netherlands.

- õigus andmete kustutamisele, tuntud ka kui „õigus olla unustatud“ (artikkel 17),
- õigus piirata andmete töötlemist (artikkel 18),
- õigus esitada vastuväiteid (artikkel 21),
- õigus mitte olla automatiseeritud otsuste, sealhulgas profiilianalüüsi, objektiks (artikkel 22),
- ning õigus esitada kaebus ja kasutada õiguskaitsevahendeid (artiklid 77–79).

Nagu eelnevalt käsitletud, muutuvad need õigused eriti oluliseks automatiseeritud töötlusel põhinevate otsuste kontekstis, kuna sellised otsused võivad olla keerulised, raskesti mõistetavad ning oluliselt mõjutada andmesubjekti elu. Kuigi GDPR näeb ette tugeva õiguste kaitsemehhanismi, võib nende õiguste tegelik rakendamine praktikas osutuda keerukaks.

GDPR artikli 7 lõike 3 kohaselt on andmesubjektil õigus oma nõusolek igal ajal tagasi võtta, kusjuures tagasivõtmine peab olema sama lihtne kui nõusoleku andmine. Lisaks peab andmesubjektil olema võimalik nõusolek tagasi võtta ilma kahjuta – see tähendab näiteks, et tagasivõtmine peab olema tasuta ja ei tohi viia teenuse kvaliteedi languseni. Tagasivõtmise tulemusel tuleb andmetöötlus, mis põhines nõusolekul, koheselt lõpetada, välja arvatud juhul, kui töötlemine saab jätkuda mõnel muul õiguslikul alusel. Nõusoleku tagasivõtmine ei mõjuta enne selle toimumist läbi viidud andmetöötluse seaduslikkust, mis tähendab, et tagasivõtt kehtib ainult edasiulatuvalt.[143] See tähendab, et tagasivõtmine ei pruugi lõpetada kogu andmetöötlust, kui andmetöötleja saab jätkata töötlemist mõne muu õigusliku aluse, nagu näiteks lepingu täitmise (art 6 lg 1 p b) või õigustatud huvi (art 6 lg 1 p f) alusel. See võib viia olukorrani, kus andmesubjekt eeldab, et tema andmeid enam ei töödelda, kuigi töötlemine võib siiski jätkuda muul õiguslikul alusel.

Praktikas ei pruugi andmesubjekt olla teadlik, et ta on üldse andnud nõusoleku – eriti juhtudel, kus see saadakse kaudselt, näiteks üldtingimustesse peidetud klauslite või eelnevalt märgistatud valikukastide kaudu. Kuid nõusoleku kehtimiseks peab see vastama GDPR artikli 4 punkti 11 kriteeriumitele – see tähendab, et nõusolek peab olema vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus. Need kriteeriumid on ühtlasi eelduseks, et andmesubjekt saaks oma nõusoleku artikli 7 alusel kehtivalt tagasi võtta. Kui nõusolek ei

[143] EDPB 2020, Guidelines on consent, lk 23-25.

vasta neile tingimustele, võib selle kehtivus olla algusest peale küsitav, mis omakorda tähendab, et ka nõusoleku tagasivõtmisel ei pruugi olla õiguslikku tähendust.[144]

Kui nõusoleku kehtivus on olemas ning andmesubjekt otsustab selle tagasi võtta, tuleb arvesse võtta ka tagajärgi andmete töötlemisele. Isikuandmete puhul, mida on töödeldud üksnes nõusoleku alusel, tuleb need pärast nõusoleku tagasivõtmist kustutada, eeldusel et nende säilitamiseks puudub muu õiguslik alus (art 17 lg 1 p b). Lisaks on andmesubjektil õigus taotleda ka muul alusel töödeldud andmete kustutamist (art 17 lg 1). Andmetöötlejad peavad igal juhul hindama andmetöötluse jätkamise põhjendatust – seda isegi siis, kui andmesubjekt pole esitanud otsest kustutamistaotlust.[145]

Kuigi GDPR annab andmesubjektile õiguse oma andmete kustutamiseks, piiravad selle õiguse rakendamist mitmed erandid, mis on sätestatud artikli 17 lõikes 3. Lisaks võib andmete kustutamine olla tehniliselt keeruline või isegi võimatu, eriti automatiseeritud süsteemides, kus andmed on juba edasi jagatud teistele töötlejatele või volitatud töötlejatele. Seetõttu võib nõusoleku tagasivõtmine ja andmete kustutamine olla automatiseeritud otsuste kontekstis piiratud kasuteguriga, mis vähendab selle tõhusust andmesubjekti kaitsemehhanismina.[146] Seega, kuigi nõusoleku tagasivõtmine ja andmete kustutamine on GDPR-is ette nähtud kui tugevad individuaalsed kontrollimehhanismid, võivad nende tegelikku tõhusust vähendada jätkuvalt kehtivad muud õiguslikud alused, tehniline teostamatus ning andmesubjekti jaoks keeruline või ebaselge võimalus oma andmeid kustutada. Automatiseeritud otsustamise ja tehisintellekti laialdasema kasutuse korral võib see õigus sisuliselt üha nõrgeneda, kuna see ei taga andmesubjektile ette nähtud kaitset ega soovitud tulemusi.

GDPR-i kohaselt saab andmeid koguda kas otse või kaudselt. Automatiseeritud otsuste tegemise süsteemides, eriti tehisintellektil põhinevates rakendustes, kasutatakse ulatuslikult tuletatud andmeid ja profiile. Need andmed ei ole otseselt andmesubjekti poolt esitatud (art 13) ega kolmandalt isikult saadud (art 14), vaid tekivad andmetöötluse käigus. Kuigi GDPR

[144] Nišević, Sears jt 2022, lk 13-14.
[145] EDPB 2020, Guidelines on consent, lk 23-25.
[146] Nišević, Sears jt 2022, lk 19-20.

sätestab selged õigused isikuandmete töötlemise osas, ei ole selge, kas need õigused kehtivad ka tuletatud andmete suhtes.[147]

Teabe saamise õigus (art 12–14 GDPR-is) on andmesubjekti õiguste süsteemi keskne osa ja eeldus teiste õiguste kasutamiseks. See annab isikule ülevaate isikuandmete töötlemisest ja loob aluse teadlikuks osalemiseks andmekeskkonnas. Kuigi see õigus hõlmab laialdast teavet, näiteks töötlemise eesmärke, õiguslikku alust ja profiilianalüüsi loogikat, ei ole selge, kas see katab järeldatud andmeid ja profiile, mis ei ole otseselt andmesubjektilt saadud. Artikkel 13 kehtib ainult siis, kui andmed on kogutud otse andmesubjektilt – järeldatud andmed siia alla ei kuulu. Artikkel 14 käsitleb kaudselt saadud andmeid, kuid grammatilise tõlgenduse järgi ei hõlma see andmetöötleja enda poolt genereeritud andmeid, nagu profiilid või järeldused. Siiski on võimalik eesmärgipõhine tõlgendus, mille kohaselt võiks järeldatud andmed kuuluda artikli 14 alla, kui neid käsitleda kas teistelt andmetöötlejatelt saadud või töötleja enda omandatud teabena.[148] Seda lähenemist toetab ka Euroopa Kohtu otsus SCHUFA kohtuasjas, kus rõhutati, et teabe saamise õigust tuleb tõlgendada GDPR-i artikli 22 eesmärgi valguses – st isiku kaitseks automatiseeritud töötlemise ja profiilianalüüsi eest.[149] Järelikult teabe saamise õigus otsesõnu ei hõlma järeldatud andmeid ega profiile, kuid laiema ja eesmärgipõhise tõlgenduse kohaselt võiks neid käsitleda selle õiguse osana, eriti seoses automatiseeritud töötlemisega.[150]

Andmesubjekti õigus tutvuda andmetega (art 15) on üks väheseid õigusi, mis osaliselt ulatub ka tuletatud andmetele. Seda kinnitab määruse põhjenduspunkt 63, mille kohaselt hõlmab juurdepääsuõigus muu hulgas ka arsti loodud hinnanguid ja diagnoose – seega andmeid, mida andmesubjekt ise ei ole esitanud. Samas on praktikas jäänud ebaselgeks, kas näiteks algoritmilise analüüsi tulemusel loodud ennustused või hinnangud kuuluvad samuti selle õiguse kaitse alla. Lisaks võib juurdepääs olla piiratud juhul, kui see kahjustaks teiste isikute õigusi ja vabadusi (art 15 lg 4), sealhulgas andmetöötleja ärisaladusi või intellektuaalomandit.[151] Euroopa Andmekaitsenõukogu on siiski väljendanud seisukohta, et

[147] Custers, B., Vrabec, H. Tell me something new: data subject rights applied to inferred data and profiles. – Computer Law & Security Review, 2024, Vol. 52, lk 3-12.
[148] Samas, lk 6-7.
[149] EKo C-634/21, SCHUFA Holding AG.
[150] Custers, Vrabec, lk 6-7.
[151] Samas, lk 7-9.

andmesubjektidel peaks olema ligipääs ka nende kohta loodud profiiliandmetele ning soovitanud andmetöötlejatel võimaldada sellele ligipääs.[152]

Erinevalt eelnevast on õigus andmete parandamisele (art 16) piiritletud vaid faktiliselt ebaõigete või puudulike andmete parandamisega ning ei laiene järeldatud andmetele, mis põhinevad andmetöötleja hinnangutel või tõenäosusmudelitel. Kuid õigus kustutamisele (art 17) ning õigus töötlemise piiramisele (art 18) võivad teatud tingimustel laieneda ka tuletatud andmetele, juhul kui nende töötlemine on ebaseaduslik või vaidlustatud. Siiski on nende kohaldamine keerulisem, kuna need õigused eeldavad, et tegemist oleks isikuandmetega ning andmesubjekt oleks teadlik nende olemasolust.[153]

Kokkuvõttes võib öelda, et andmesubjekti õiguste rakendamine tuletatud või järeldatud andmetele sõltub suurel määral konkreetse õiguse sõnastusest ning selle tõlgendamisviisist. Kitsas, grammatiline tõlgendus kipub välistama selliste andmete kaitse, samas kui laiem, teleoloogiline tõlgendus – mis lähtub GDPR üldeesmärgist tagada isikuandmete töötlemise õiglus ja läbipaistvus – võib õigustada tuletatud andmete hõlmamist andmesubjekti õiguste kohaldamisalasse. Selles küsimuses on kohtupraktikat seni vähe, mistõttu regulatsiooni rakendamine sõltub tihti andmetöötlejate tõlgendusest ning andmesubjektide teadlikkusest.[154]

Artikkel 22 nõuab, et kõigil juhtudel rakendataks asjakohaseid kaitsemeetmeid andmesubjekti õiguste, vabaduste ja õigustatud huvide kaitseks. See hõlmab andmesubjekti õigust inimese sekkumisele, oma seisukoha arvesse võtmisele ning võimalust vaidlustada automatiseeritud töötlemise tulemusel tehtud otsus.[155] Lisaks annavad artiklid 77-79 andmesubjektile õiguse esitada kaebus ja kasutada muid õiguskaitsevahendeid.

GDPR eeldab, et andmesubjektid on teadlikud oma õigustest ning suudavad neid kasutada, kui nende andmeid töödeldakse automatiseeritud süsteemide kaudu. Tegelikkuses on aga suur osa inimestest nendest võimalustest kas teadmatuses või ei oma piisavalt oskusi ja ressursse nende õiguste rakendamiseks.

---

[152] EDPB 2018, Guidelines on ADM and Profiling, lk 31.
[153] Custers, Vrabec, lk 9-11.
[154] Samas, lk 3-12.
[155] Nišević, Sears jt 2022, lk 8-9.

Warwicki Ülikooli doktorant Yulu Pi viis oma doktoritöö raames läbi mitmeid katseid, et uurida, kuidas suurendada inimeste võimalusi mõjutada automatiseeritud otsuseid. Tema uuringud näitavad, et pelgalt selgituste pakkumine automatiseeritud otsuste puhul ei taga, et inimesed mõistaksid neid selgitusi ega suudaks otsuseid edukalt vaidlustada. Kuigi detailsemad selgitused suurendasid osalejate usaldust ja enesekindlust, ei parandanud need nende tegelikku suutlikkust tuvastada süsteemipoolseid vigu ega teha informeeritud otsuseid. Eriti ilmnes, et tehnilised või üldsõnalised selgitused ei pruugi olla piisavad, kui puudub arusaam sellest, milline oli automatiseeritud süsteemi roll otsuses ning millised on inimese võimalused seda mõjutada. See rõhutab vajadust kujundada selgitusi nii, et need oleksid mitte ainult läbipaistvad, vaid ka arusaadavad ning toetaksid andmesubjekti tegelikku tegutsemisvõimet konkreetses kontekstis.[156]

Samuti on probleemiks see, et paljud automatiseeritud otsustamise süsteemid tuginevad nn musta kasti mudelitele, mille tööloogika ei ole isegi ekspertidele alati täielikult arusaadav (nagu käsitletud peatükis 2.1). Lisaks tehnilistele takistustele tuleb arvestada ka nn infoväsimust ja psühholoogilisi barjääre. Andmesubjekti õiguste rakendamine sõltub suuresti indiviidi võimest ja valmisolekust neid kasutada. Õiguste kehtestamine GDPR alusel eeldab aktiivset kaebamist või taotluse esitamist, mis jääb paljudele inimestele kättesaamatuks väheste teadmiste, vähese keeleoskuse, ajapuuduse või muude ressursipiirangute tõttu. Nii muutub õigus deklaratiivseks, tegelikult kättesaamatuks kaitsemehhanismiks.[157]

Ka institutsionaalselt võib andmesubjekti püüdlus takerduda – andmetöötlejad ei pruugi pakkuda kasutajasõbralikke kanaleid õiguste kasutamiseks või võivad selgitusi anda viisil, mis on liiga tehniline, piiratud või kaitstud ärisaladuse ettekäändel.[158] Lisaks on takistuseks andmekaitseasutuste piiratud volitused ja ressursid. Kuigi GDPR annab andmekaitseasutustele volitusi õiguste jõustamiseks ja järelevalveks, keskenduvad paljud nende tegevused individuaalkaebuste lahendamisele, mitte ennetavale või süsteemsele sekkumisele. Samuti ei ole paljud riiklikud andmekaitseasutused varustatud piisavate tehniliste teadmiste, rahaliste ressursside ega poliitilise sõltumatusega, et jõuliselt sekkuda

[156] Pi, Y. Empowering Individuals in Automated Decision-Making: Explainability, Contestability and Beyond. – CSCW Companion '24, November 9–13, 2024, San Jose, Costa Rica, ACM, New York, lk 1-4.
[157] Padden, M., Öjehag-Pettersson, A. Digitalisation, democracy and the GDPR: The efforts of DPAs to defend democratic principles despite the limitations of the GDPR. – Big Data & Society, October–December 2024, Vol. 11, No. 4, lk 7-9.
[158] Mazur, J., Bernatt, M. Can the Automated State Be Trusted? The Role of Rule of Law Safeguards for Governing Automated Decision-Making and Artificial Intelligence. – Georgia Law Review, 2024, Vol. 58, No. 3, lk 1100–1109.

näiteks tehisintellektipõhiste automatiseeritud süsteemide analüüsimisse või algoritmilise kallutatuse tuvastamisse.[159]

Kokkuvõttes saab öelda, et kuigi GDPR sätestab andmesubjektile mitmeid õigusi, mis peaksid pakkuma kaitset automatiseeritud andmetöötlusel põhinevate otsuste vastu, jääb nende õiguste praktiline rakendamine sageli piiratud mõjuga. Teadmatus õiguste olemasolust, süsteemide tehnoloogiline keerukus, institutsionaalsed takistused ning vähene juurdepääs arusaadavale teabele loovad olukorra, kus formaalselt olemasolevad õigused ei taga andmesubjektile tegelikku mõjuvõimu ega kontrolli isikuandmete kasutamise üle. Eriti tehisintellektil põhinevate süsteemide puhul võib andmesubjekt seista silmitsi otsustega, mille aluseks olevat loogikat ta ei mõista ega saa vaidlustada. Seetõttu on vajalik liikuda edasi lahendustega, mis toetavad õiguste sisulist rakendamist – näiteks kasutajakesksed selgitusmehhanismid, kollektiivsete õiguste tugevdamine ning institutsionaalne tugi automatiseeritud otsuste läbipaistvuse ja vastutuse tagamiseks.

[159] Padden, Öjehag-Pettersson, lk 7-15.

3. ÕIGUSLIKUD JA PRAKTILISED LAHENDUSED ISIKUANDMETE KAITSEKS TI-PÕHISTES AUTOMATISEERITUD OTSUSTES

GDPR-is on sätestatud mitmeid põhimõtteid andmesubjektide õiguste kaitseks. Siiski praktikas kaasneb nende põhimõtete rakendamisega mitmeid väljakutseid. Selles peatükis käsitletakse põhjalikumalt, millised on võimalikud õiguslikud ja praktilised lahendused, et tagada andmesubjektide isikuandmete kaitse TI-põhistes automatiseeritud otsustes.

3.1. Kas AI Act lahendab GDPR-i kitsaskohad?

Nagu eelnevas peatükis käsitletud, on GDPR loonud tugeva aluse automatiseeritud otsuste reguleerimiseks, kuid see on jäänud tehnoloogilise arengu valguses teatud aspektides ebapiisavaks. Eriti ilmne on see tehisintellekti põhiste automatiseeritud otsuste puhul. Tehisintellekti määrus (AI Act) on välja töötatud selleks, et lahendada neid tõrkeid, täiendades GDPR-i ning pakkudes selgemaid ja rakendatavamaid regulatsioone tehisintellekti kasutamisel isikuandmete töötlemisel. AI Act võeti vastu 2024. a ning jõustub järk-järgult lähiaastatel. Järgnevalt analüüsitakse, milliseid GDPR-i kitsaskohti AI Act suudab lahendada ning millised probleemid jäävad siiski alles.

Nagu selgitatud peatükis 2.1, siis GDPR ei sätesta otsest õigust saada automatiseeritud otsuste kohta selgitusi, vaid see õigus tuleneb kaudselt GDPR-i artiklitest 13–15 ning põhjenduspunktist 71. Samas AI Act artikkel 86 kujutab endast esmakordset selgelt sõnastatud õigust saada tehisintellektisüsteemi otsuste kohta sisukaid selgitusi.[160] AI Act artikkel 86 lõige 1 sätestab, et igal mõjutatud isikul on õigus selgele ja sisukale selgitusele tehisintellektisüsteemi rolli kohta otsustusprotsessis ning tehtud otsuse olulisemate elementide kohta (nt kasutatud kriteeriumid või kaalutlused). See muudab õiguse selgitusele rakendatavaks mitte üksnes formaalselt, vaid ka sisuliselt. Siiski kehtib artikkel 86 lõige 1 ainult suure riskiga tehisintellektisüsteemide puhul.

AI Act jagab tehisintellekti rakendused kolme riskikategooriasse, lähtudes nende võimalikust mõjust Euroopa Liidu põhiväärtustele ja põhiõigustele: keelatud praktikad, suure riskiga süsteemid ning madala või minimaalse riskiga süsteemid. ELi seadusandja otsustas, et õigus

[160] Metikoš, L., Ausloos, J. The right to an explanation in practice: insights from case law for the GDPR and the AI Act. – Law, Innovation and Technology, 2025, lk 4.

saada selgitusi tehisintellekti otsustusprotsessi kohta on tagatud ainult suure riskiga süsteemide puhul, nagu näiteks tervishoius, tööhõives ja õigusemõistmises kasutatavad süsteemid. Selle eesmärk on vältida olukorda, kus juurutajatelt[161] nõutakse selgitusi ka juhtudel, kui TI-süsteemid kujutavad endast väiksemat ohtu. Põhjenduspunktid 54–61 määratlevad iga kõrge riskiga kategooria puhul vastavad põhiõigused ja õiguslikud põhimõtted, mida läbipaistvuse ja selgitatavuse nõuded aitavad kaitsta.[162] Kõrge riskiga kategooriate määratlemine AI Actis põhineb pigem süsteemi funktsionaalsel mõjul õigustele, mitte üksnes töödeldavate andmete iseloomul, mis tugevdab GDPR-i andmesubjekti õiguste kaitset tehisintellekti ajastul.[163]

GDPR artikkel 22 kohaldub ainult selliste automatiseeritud otsuste puhul, mille tegemisel puudub sisuline inimsekkumine ja mis võivad oluliselt mõjutada andmesubjekti. Praktikas on aga keeruline tõendada, kas inimkontroll on sisuline või üksnes näiline: andmetöötlejad võivad vastutusest hoidumiseks rakendada fiktiivset inimsekkumist. AI Act artikkel 86 reguleerib laiemat valikut juhtumeid, kuna see ei eelda täielikult automatiseeritud otsust – piisab, kui tehisintellektisüsteem mõjutab otsust, mille langetab inimene. Seetõttu kehtib artikkel 86 ka olukordades, kus TI-süsteemi kasutatakse inimese tehtud otsuse toetamiseks. See laiendab isikuandmete kaitse ulatust ja takistab formaalsetest nõuetest möödahiilimist.[164] Kuna määrus lähtub TI-süsteemi funktsioonist ja riskist, mitte üksnes töödeldavate andmete liigist, võimaldab see reguleerida ka juhtumeid, kus GDPR-i kohaldamine on piiratud või ebaselge.

Kui GDPR ei sätesta otseselt, et andmesubjektil oleks õigus saada tehisintellektil põhineva automatiseeritud otsuse kohta detailset selgitust, siis tehisintellekti määrus (AI Act) kehtestab teatud juhtudel kohustuse selliste otsuste sisulist põhjendamist ja dokumenteerimist. AI Act artikkel 86 lõige 1 näeb ette, et suure riskiga tehisintellektisüsteemide puhul on mõjutatud isikul õigus saada juurutajalt selged ja sisukad selgitused TI-süsteemi rolli kohta otsustusprotsessis ning tehtud otsuse peamiste sisuliste elementide kohta, nagu kasutatud andmed, loogilised ja statistilised põhimõtted ning kriteeriumid, mis mõjutasid otsuse tegemist.

[161] AI Act artikkel 3 punkt 4 kohaselt on „juurutaja“ – füüsiline või juriidiline isik, ametiasutus, ametkond või muu organ, kes kasutab tehisintellektisüsteemi oma volituste alusel, välja arvatud juhul, kui tehisintellektisüsteemi kasutatakse isikliku, mitte kutselise tegevuse jaoks.
[162] Cotogni, lk 424-427.
[163] Camões, lk 49–50.
[164] Cotogni, lk 424–425.

Lisaks sellele kehtestab AI Act artikkel 11 dokumenteerimiskohustuse, artiklid 12–14 aga sätestavad kõrge riskiga süsteemide jälgitavuse, läbipaistvuse ja inimjärelevalve nõuded, mille eesmärk on tagada nende süsteemide ohutus ja usaldusväärsus.

Dokumenteerimise kohustuse sätestab AI Act artikkel 11, mille lõike 1 kohaselt tuleb suure riskiga tehisintellektisüsteemi tehniline dokumentatsioon koostada enne süsteemi turule laskmist või kasutuselevõttu ning seda tuleb pidevalt ajakohastada. Dokumentatsioon peab olema koostatud viisil, mis tõendab süsteemi vastavust AI Act II jaos sätestatud nõuetele ning võimaldab pädevatel asutustel ja määruse alusel teavitatud vastavushindamisasutustel hinnata selle vastavust.

Täiendavalt peab dokumentatsioon sisaldama vähemalt IV lisas loetletud sisulisi ja tehnilisi andmeelemente, sealhulgas süsteemi ja selle algoritmide üldist loogikat, peamisi klassifitseerimisvalikuid (nt kuidas ja mille alusel süsteem jaotab andmesubjekte või otsuseobjekte kategooriatesse), kasutatud parameetrite olulisust, eeldatavat väljundit ja väljundi kvaliteedi kirjeldust, koolitusmetoodikaid ja -tehnikaid, kasutatud treeningandmestikke ning inimese järelevalve mehhanisme vastavalt artiklile 14.[165] Selline ulatuslik dokumenteerimiskohustus toetab nii GDPR-i läbipaistvusnõudeid kui ka võimaldab praktiliselt rakendada õigust selgitusele ja otsuste vaidlustamise võimalust.[166]

Artikkel 12 kohustab tagama kõrge riskiga tehisintellekti süsteemide toimingute jälgitavuse, nõudes, et need süsteemid võimaldaksid sündmuste (logide) automaatset salvestamist kogu eluea jooksul. Selle eesmärk on suurendada läbipaistvust ning toetada auditeeritavust ja selgitatavust. Ka artikkel 13 keskendub TI-süsteemide läbipaistvusele, rõhutades, et nende toimimine peab olema kasutajatele arusaadav. Selle tagamiseks peavad süsteemidega kaasnema kasutusjuhendid, mis sisaldavad teavet nende täpsuse, töökindluse, küberturvalisuse ja võimalike riskide kohta. Samuti tuleb kirjeldada, kas ja kuidas süsteem suudab oma otsuseid selgitada.[167]

[165] Cotogni, lk 425.
[166] Metikoš & Ausloos, lk 8jj.
[167] Cotogni, lk 426.

Artikkel 14 kehtestab inimese järelevalve põhimõtte, mille kohaselt peavad määratud isikud suutma jälgida süsteemi toimimist, tuvastada võimalikke anomaaliaid ning vältida liialt suurt sõltuvust süsteemi väljundist (nn „moutonnier-efekt“[168]). Samuti peavad nad olema võimelised süsteemi väljundit kriitiliselt hindama ja vajadusel selle kasutamisest loobuma või süsteemi töö katkestama. Sätte eesmärk on tagada inimese sekkumise põhimõtte („human in the loop“) järgimist ning nõuab, et kõrge riskiga süsteemid töötataks välja disainiga, mis võimaldab inimese järelevalvet (läbipaistvus disaini kaudu – „transparency-by-design“), vähendades või ennetades seeläbi tervise, ohutuse või põhiõigustega seotud riske, mis võivad tekkida tehisintellekti süsteemi kasutamisel.[169]

AI Acti rakendamine eeldab ka toimivat järelevalveraamistikku. Seetõttu näeb määruse artikkel 74 lg 1 ette, et liikmesriigid peavad hiljemalt 2. augustiks 2025 määrama ühe või mitu pädevat asutust, kes vastutavad määruse täitmise järelevalve ja turujärelevalve teostamise eest. Need asutused mängivad keskset rolli kõrge riskiga süsteemide kasutamise ohutuse ja läbipaistvuse tagamisel ning rakendavad vajalikku järelevalvet koostöös teavitatud asutuste ja Euroopa tehisintellektiametiga.

Märkimist väärib ka AI Act artikkel 10, mis sätestab, et tehisintellekti süsteemi koolitus-, valideerimis- ja testimisandmed peavad vastama kindlatele kvaliteedinõuetele. Eelkõige nõuab määrus, et andmed oleksid asjakohased, piisavad ja esinduslikud ning et nende kogumisel ja töötlemisel järgitaks statistilisi põhimõtteid, mis minimeerivad kallutatust ja maksimeerivad üldistatavust. Kuigi GDPR artikkel 5 sätestab, et isikuandmed peavad olema ajakohased ning ebaõiged andmed tuleb kustutada, siis AI Act artikkel 10 läheb sisuliselt kaugemale ja käsitleb andmete kvaliteeti laiemas mõttes, hõlmates ka mitteisikulisi andmeid ja süsteemide õppimisvõime aspekti.

See on mõistetav, kuna andmete kvaliteedi põhimõttel on otsustusalgoritmide puhul eriti suur tähtsus – algoritmid õpivad ja langetavad otsuseid just neile andmetele tuginedes. Lisaks

[168] Moutonnier-efekt tähendab olukorda, kus inimene järgib tehisintellekti süsteemi väljundit kriitikavabalt ja automaatselt, ilma oma hinnangut kujundamata – sarnaselt karjamentaliteedile. Mõiste on kasutusel, et osutada võimalikule psühholoogilisele sõltuvusele masinlikust otsustusprotsessist.
[169] Cotogni, lk 426-427.

tulenevad paljud tehisintellekti süsteemide väljundeid mõjutavad kallutatused just halva kvaliteediga andmetest.[170]

AI Act kehtestab kõrge riskiga süsteemidele lisaks kvaliteedinõuetele ka nõuded, mis suunavad õigluse ja võrdse kohtlemise tagamisele juba arendusprotsessis. Artikli 10 lõike 2 punkt f kohaselt tuleb koolitus-, valideerimis- ja testimisandmestikud hinnata võimalike kallutatuste suhtes ning rakendada sobivaid andmehalduse ja juhtimise praktikaid, arvestades süsteemi kavandatud kasutusotstarvet. Eesmärk on tuvastada ja vähendada riske, mis võivad viia diskrimineerimiseni vastavalt liidu õigusaktidele. Samas ei sätesta määrus, millal ebavõrdne kohtlemine oleks ebaseaduslik — selle üle peab otsustama olemasolev diskrimineerimisvastane õigusraamistik.[171]

Lisaks artikli 10 lõige 5 võimaldab erandkorras töödelda eriliiki isikuandmeid (nt rass, etniline päritolu, sugu), kui see on rangelt vajalik kõrge riskiga süsteemide puhul eelarvamuste tuvastamiseks ja korrigeerimiseks, tuginedes avaliku huvi kaalutlusele. Selline lähenemine aitab vältida varjatud diskrimineerimist, mis võiks tekkida, kui kaitstavate tunnuste mõju ei analüüsita. AI Act loob seega normatiivse raamistiku, mis toetab „fairness by design“ ja „ethics by design“ põhimõtteid, rõhutades, et võrdsus ja mittediskrimineerimine tuleb integreerida juba süsteemide projekteerimise faasi.[172]

Seega täiendab AI Act GDPR-i, kuna selle kohaldamisala on laiem: AI Act ei piirdu ainult isikuandmete töötlemisega, vaid reguleerib kõiki kõrge riskiga TI-süsteeme, sõltumata andmetüübist. Lisaks sätestab määrus õiguse saada selge ja sisukas selgitus tehisintellektisüsteemi rolli ja tehtud otsuse peamiste elementide kohta. Samuti kehtestab AI Act kõrge riskiga süsteemidele jälgitavuse, läbipaistvuse ja inimjärelevalve nõuded, mis on olulised TI-süsteemide usaldusväärsuse ja ohutuse tagamiseks. Täiendavalt pööratakse tähelepanu andmekvaliteedile ja algoritmilise kallutatuse ennetamisele.

---

[170] Samas, lk 427.
[171] Deck, L., Müller, J.-L., Braun, C., Zipperling, D., Kühl, N. Implications of the AI Act for Non-Discrimination Law and Algorithmic Fairness. – CEUR Workshop Proceedings, EWAF'24: European Workshop on Algorithmic Fairness, 1–3 July 2024, Mainz, Germany, lk 1-5.
[172] Samas, lk 1-5.

Selgete riskijuhtimise suuniste kehtestamisega seab AI Act globaalse eeskuju turvaliseks ja eetiliseks tehisintellekti kasutamiseks. Määruse kooskõla GDPR-iga tagab ühtlasi ühtse regulatiivse keskkonna, mis tasakaalustab innovatsiooni ja privaatsuse kaitset.[173]

Kuigi AI Act täiendab GDPR-i mitmes aspektis, jäävad siiski alles mõned olulised probleemid. Nendeks on muuhulgas:

1. Piiratud kohaldumisala - AI Act kehtib eelkõige kõrge riskiga tehisintellektisüsteemide suhtes. Kui süsteem ei kuulu sellesse kategooriasse, ei kohaldu ka artikli 86 alusel kehtiv selgitusõigus. See jätab mitmed igapäevased ja mõjuvõimsad tehisintellekti otsustusmehhanismid – nagu näiteks reklaamialgoritmid ja isikupõhised soovitussüsteemid – kaitse alt välja. Selliste süsteemide puhul ei kehti samad läbipaistvusnõuded, mistõttu andmesubjektide kaitse sõltub valdkonnaspetsiifilistest normidest, nagu tarbijakaitse või digiteenuste määrus.[174]
2. Mõiste „selge ja sisukas selgitus“ ebamäärasus – Kuigi artikkel 86 kohustab andma mõjutatud isikule „selge ja sisuka“ selgituse, ei ole määratletud, milline teave on selleks piisav. See tekitab ebakindlust rakendamisel ja võib viia olukorrani, kus selgituste tase varieerub oluliselt sõltuvalt juurutajast.[175] Ebaselge sõnastus võib tekitada killustatust ehk olukorda, kus reegleid tõlgendatakse ja rakendatakse eri riikides erinevalt. See omakorda võib suurendada õigusliku ebakindluse riski.[176]
3. Vastutuse jaotus süsteemi juurutaja ja looja vahel – AI Act suunab peamised kohustused süsteemi juurutajale (*deployer*), mitte selle loojale (*provider*). Kui juurutajal puudub sügavam arusaam süsteemi sisemisest toimimisest, võib see takistada tähendusliku selgituse andmist. Samas ei ole see tingimata vastutuse lünk, vaid vajadus vastutuse teadlikuks delegeerimiseks (nt lepinguõiguse kaudu).[177]
4. Automatiseeritud otsuste sisuline hindamine – AI Act keskendub peamiselt protseduurilisele vastavusele (läbipaistvus, selgitus), kuid ei sisalda mehhanisme, mis võimaldaks hinnata automatiseeritud otsuste sisulist õiglust, nt kas tulemus on

[173] Ijaiya, H., Odumuwagun, O. O. Advancing Artificial Intelligence and Safeguarding Data Privacy: A Comparative Study of EU and US Regulatory Frameworks Amid Emerging Cyber Threats. – International Journal of Research Publication and Reviews, 2024, Vol. 5, No. 12, lk 3361.
[174] Nišević, M., Cuypers, A., De Bruyne, J. Explainable AI: Can the AI Act and the GDPR go out for a date? – 2024 International Joint Conference on Neural Networks (IJCNN), IEEE, 2024, lk 1–8.
[175] Samas, lk 1-8.
[176] Metikoš, Ausloos, lk 8jj.
[177] Nišević, Cuypers, De Bruyne, lk 1-8.

diskrimineeriv või ebaproportsionaalne. See võib vähendada õiguskaitse efektiivsust diskrimineerimisega seotud juhtumites.[178]

5. Õiguse piiramine teiste EL-i õigusaktide kasuks – AI Act artikkel 86 lõige 2 sätestab, et selgitusõigus ei kohaldu, kui olukorda reguleerib mõni muu EL-i õigusakt, nagu GDPR. See võib tekitada olukorra, kus mõlemad regulatsioonid välistavad oma kohaldamise, mistõttu isikul puudub praktiline võimalus selgitust saada. Lisaks võib tekkida vastuolu ärisaladuse kaitsega – näiteks juhul, kui selgituse andmine eeldaks ettevõttesisese algoritmi loogika avaldamist, mida loetakse ärisaladuseks.[179]
6. Erinevused kohaldamisalas – GDPR keskendub isikuandmete kaitsele, samas kui AI Act reguleerib TI-süsteeme nende funktsiooni ja riski põhjal. Seetõttu võivad esineda olukorrad, kus üks määrus kohaldub, teine aga mitte – või ka mõlemad (nt isikuandmetega seotud kõrge riskiga süsteemide korral). Samas on võimalik, et ei kohaldu kumbki, näiteks mitteisikuliste andmetega seotud madala riskiga rakenduste puhul. See võib kaasa tuua ebaselgust regulatiivses järelevalves ja õiguskaitses, sest konkreetse juhtumi puhul võib olla keeruline otsustada, millist õigusraamistikku kohaldada või kas neid kohaldatakse paralleelselt.[180]

Kokkuvõttes kujutab AI Act endast olulist sammu läbipaistvama ja vastutustundlikuma tehisintellekti kasutuse suunas. See täiendab GDPR-i, kuid ei lahenda täielikult kõiki selle regulatiivseid lünki ega kõrvalda õigusselguse puudujääke. Näiteks määrus jätab määratlemata selgitusõiguse sisu ning ei reguleeri piisavalt vastutuse jaotust juurutaja ja looja vahel. Samuti võivad tekkida vastuolud teiste EL-i õigusaktidega, näiteks GDPR-iga, mis võib tekitada järelevalve ja õiguskaitse praktikas ebakindlust.

Vaatamata nendele puudustele loob AI Act siiski selgema ja laiapõhjalisema regulatiivse raamistiku: see sätestab esmakordselt õiguse selgitusele, nõuded süsteemide läbipaistvusele ning hõlmab lisaks isikuandmete töötlemisele ka mitteisikuliste andmetega toimivaid süsteeme, mida GDPR ei kata.

[178] Deck jt, lk 1-5.
[179] Metikoš, Ausloos, lk 1-34.
[180] Camões, lk 50–52.

3.2. Andmesubjektide kaitse: lahendused ja rakenduspraktikad TI-põhistes otsustes

Automatiseeritud otsuste tegemine, eriti kui see põhineb tehisintellektil, tekitab olulisi väljakutseid andmesubjektide õiguste kaitsel. Kuigi GDPR kehtestab mitmeid kaitsemehhanisme, on nende tõhusus praktikas sageli piiratud. Arvestades, et tehisintellektisüsteemid põimuvad üha tihedamalt ühiskonna toimimisega, on andmesubjektide õiguste kaitse seisukohalt üheks kriitiliseks väljakutseks tasakaalu leidmine innovatsiooni, õigluse ja läbipaistvuse nõuete vahel[181]. Järgnevalt käsitletakse olemasolevaid ja oodatavaid lahendusi, mis on suunatud andmesubjektide kaitse tugevdamisele, samuti esitatakse soovitusi GDPR-i täiendamiseks.

3.2.1. Läbipaistvuse ja selgitatavuse suurendamine

Läbipaistvuse ja selgitatavuse nõuded on kujunenud automatiseeritud otsuste reguleerimisel kesksekseks teemaks. Nagu analüüsitud peatükis 2.1, ei taga GDPR-i sätted alati sisulist ega mõistetavat selgitust automatiseeritud otsuste kohta. Üheks võimalikuks tehniliseks lahenduseks on selgitatava tehisintellekti (explainable AI - XAI) meetodid, mis võimaldavad esitada otsuse põhjenduse arusaadaval kujul. XAI eesmärk on avada nn must kast nii, et otsustusprotsess oleks tõlgendatav mitte ainult arendajatele, vaid ka otsuse adressaadile.[182]

XAI saab tugevdada andmesubjekti õigusi ainult siis, kui esitatud selgitused on tähenduslikud – need võimaldavad mõista otsuse sisu, hinnata selle asjakohasust ja vajadusel sellele vastu vaielda. Uuringud näitavad, et XAI võib suurendada usaldust ja kontrollitunnet, kuid ainult juhul, kui selgitused on kohandatud kasutaja kontekstile ja esitatud sobival kujul, nt verbaalselt või visuaalselt.[183]

Praktikas on probleemiks, et XAI-d käsitletakse mõnikord vaid keerulise tehnilise teabe esitamisena. Sellisel juhul võivad selgitused küll eksisteerida, kuid need ei pruugi olla andmesubjekti jaoks tähenduslikud ega võimalda tal otsust mõista või sellele vajadusel reageerida. Chaudhary pakub välja kvalifitseeritud läbipaistvuse (*qualified transparency*) kontseptsiooni, mille kohaselt tuleks selgitused kohandada vastavalt sidusrühmade (nt

[181] Ijaiya, Odumuwagun, lk 3357jj.
[182] Chaudhary, lk 111.
[183] Pi, lk 2 jj.

andmesubjektid, audiitorid) vajadustele ja arusaamisvõimele, pakkudes tähenduslikke ja praktilisi juhiseid.[184]

Ühe võimalusena tähendusliku selgitatavuse tagamiseks on pakutud vastandfaktilised selgitused (*counterfactual explanations)*, mille eesmärk ei ole süsteemi sisemise loogika avaldamine, vaid andmesubjektile arusaadava konteksti loomine. Näiteks kui sinu sissetulek oleks olnud 45 000 eurot, oleks laen heaks kiidetud.[185] Sellised selgitused aitavad andmesubjektil paremini mõista, kuidas tema andmed mõjutasid tulemust, ning annavad võimaluse tulevasi otsuseid teadlikumalt suunata või olemasolevaid otsuseid vaidlustada.

Vastandfaktilise lähenemise eelis seisneb ka selles, et see ei nõua keeruka algoritmilise loogika avalikustamist ega riku ärisaladust. See teeb sellest sobiva lahenduse andmetöötlejatele, kes soovivad täita läbipaistvuskohustusi, säilitades samas konfidentsiaalsuse.[186]

Lisaks on oluline rõhutada kontekstuaalse ja kihilise informatsiooni esitusviiside potentsiaali. Andmekaitsenõukogu läbipaistvuse suunis soovitab kasutada kihilist lähenemist, kus esmavajalik teave esitatakse kohe ning detailsem teave on kättesaadav täiendavate kihtide kaudu. Samuti toetab juhend just-in-time lahendusi – näiteks hüpikaknaid või visuaalseid ikoonikesi, mis ilmuvad automatiseeritud otsuse tegemise hetkel ja selgitavad selle mõju.[187]

Visuaalsed selgitusvahendid, nagu skeemid, infograafikud ja lühivideod, võivad suurendada arusaamist eriti tehniliste süsteemide puhul, mille sisemine loogika on keeruline. Sellised vahendid muudavad keerulise otsustusprotsessi mõistetavamaks ka neile, kellel puudub tehniline taust, mis on kooskõlas Andmekaitsenõukogu soovitusega kasutada selget ja lihtsat keelt.[188]

Kuid selgitusõigus ei saa olla tõhus ilma selle tiheda sidumiseta otsuse vaidlustamise võimalusega. Kohtupraktika (nt eelpool käsitletud SCHUFA, Uberi ja Ola juhtumid) näitab, et selgitusõiguse ebapiisav määratlus GDPR-is võib takistada andmesubjektil oma õiguste

[184] Chaudhary lk 110-111.
[185] Wachter, Mittelstadt, Russell, lk 860–871.
[186] Wachter, Mittelstadt, Russell, lk 865–867.
[187] EDPB 2018, Guidelines on transparency, lk 19jj.
[188] EDPB 2018, Guidelines on transparency, lk 25.

kasutamist, eriti olukordades, kus otsus on tehtud automatiseeritult. See tähendab, et selgituse eesmärk ei ole üksnes informeerimine, vaid ka see, et andmesubjekt saaks otsust mõista ning vajadusel sellele vastu vaielda.[189] Seetõttu on oluline, et tehnilised lahendused integreeritaks õiguste realiseerimise mehhanismidesse: vaidlustamise õigusse, inimsekkumise võimalusse ja järelevalveasutuste pädevusse hinnata selgituse sisukust.

Tehnilis lahendusi on vaja toetata selge õigusliku raamistikuga. GDPR ei sisalda siduvat õigust selgitusele ning seetõttu ei ole nt XAI rakendamine iseenesest piisav. Tõhus selgitatavus eeldab nii andmesubjekti õigust nõuda selgitust kui ka andmetöötleja kohustust esitada see arusaadaval kujul, et andmesubjekt saaks teha vajalikke järeldusi ja oma õigusi realiseerida. Lahenduseks on soovitatud muuta GDPR artikli 22 lõige 3 selliselt, et see sisaldaks sõnaselget ja siduvat õigust saada individuaalne, inimesele arusaadav ja tähenduslik selgitus automatiseeritud otsuse kohta.[190] Kuigi AI Act kehtestab täiendavad läbipaistvuse nõuded ning õiguse selgitusele, teeb ta seda ainult suure riskiga rakendustele, jättes paljud igapäevased ja mõjuvõimsad TI-põhinevad automatiseeritud otsused väljapoole kaitseulatust (nagu käsitletud pt 3.1). Seetõttu oleks GDPR-i täiendamine asjakohane.

Lisaks GDPR-ile ja AI Act-le on Euroopa Liit hakanud üha enam rõhutama läbipaistvuse ja selgitatavuse olulisust ka teistes õigusvaldkondades, kus automatiseeritud otsustel võib olla märkimisväärne mõju andmesubjektide õigustele. Näiteks 2019. aasta tarbijakaitsereformi raames kehtestati nõue teavitada tarbijaid hinnapakkumiste personaliseerimisest automatiseeritud otsuste abil abil ning kohustus avalikustada toodete järjestamise põhiparameetrid (direktiiv 2019/2161 ja määrus 2019/1150). Digiteenuste määrus sisaldab mitmeid sätteid, mille eesmärk on suurendada läbipaistvust ja seletatavust veebiplatvormide sisumodereerimise ja soovitussüsteemide kasutamise kohta. Samuti on automatiseeritud otsuste läbipaistvus ja seletatavus tõusnud keskseks teemaks tööõiguses – eeskätt platvormitöö direktiivis, mille eesmärk on tagada töötajatele õiglane ligipääs tööle ja selged töötingimused ka siis, kui nende töötingimusi mõjutavad algoritmilised otsused. Seega selgitatavust nõutakse just sellisel kujul, mis võimaldab tegelikku arusaamist automatiseeritud otsuste loogikast ja mõjust. See toetab lähenemist, et selgitused ei tohi piirduda üksnes süsteemikesksete kirjeldustega (kuidas algoritm töötab), vaid peavad olema

[189] Metikoš, Ausloos, lk 1–34.
[190] Wachter, Mittelstadt, Floridi, lk 97.

isikupõhised ja kontekstiteadlikud – st selgitama, miks just sellele inimesele konkreetne otsus tehti.[191]

Kuid tehisintellekti reguleerimisel võib suureneda ka standardite roll. AI Act artikli 40 kohaselt eeldatakse, et süsteemid, mis vastavad ELi harmoniseeritud standarditele, vastavad ka määruse nõuetele. Euroopa Komisjonil on volitus anda standardiorganisatsioonidele, nagu Euroopa Standardikomitee (CEN) ja Euroopa Elektrotehnilise Standardimise Komitee (CENELEC), ülesandeks nende standardite koostamine.

Kuigi standardiseerimine võib toetada ühtlustamist ja praktilist rakendamist, peitub selles ka oht: läbipaistvus ja selgitatavus võivad muutuda formaalseteks vastavuskontrolli objektideks, mille tegelik mõju andmesubjektide õigustele jääb tagaplaanile.[192] Samuti on tehnilistes standardites risk nihutada rõhk arendajate ja süsteemide sisemisele dokumentatsioonile, mitte selgitustele, mis on mõistetavad lõppkasutajale.[193] Praktikas võib see viia olukorrani, kus tehnilised standardid muutuvad de facto regulatiivseks raamistikuks, millega määratletakse näiteks selgitatavuse ja läbipaistvuse tase. Siiski tuleb rõhutada, et standardiseerimine keskendub peamiselt tehnilistele aspektidele ega pruugi tagada vastavust laiematele õiguspõhimõtetele, nagu andmekaitse, läbipaistvus ja vastutus.[194]

Veelgi enam, määruse artikkel 86 ei täpsusta, mida tähendab „selge ja sisukas“ selgitus – see mõiste jääb määratlemata ning võib saada standardite kaudu kaudse sisu, mis sõltub tehnilisest tõlgendusest, mitte õiguspõhimõtetest.[195]

Seetõttu on oluline tagada, et standardite väljatöötamisel osaleksid lisaks inseneridele ja tootjatele ka andmekaitseeksperdid, õigusteadlased ja kodanikuühiskonna esindajad. Ainult interdistsiplinaarne koostöö võimaldab vältida olukorda, kus tehnilised kriteeriumid varjutavad sellised normatiivsed põhimõtted nagu läbipaistvus, õiglus ja vastutus.[196]

Tulevikusuunana on soovitatud töötada välja selgituste kvaliteedihindamise kriteeriumid – kas esitatud XAI-lahendus toetab reaalselt andmesubjekti õigusi? Kas see aitab mõista otsuse mõju ja tausta? Sellised kriteeriumid võiksid olla osa EDPB või Euroopa Komisjoni

[191] Cotogni, lk 428-437.
[192] Chaudhary, lk 109–110.
[193] Cotogni, lk 427.
[194] Nišević, Cuypers, De Bruyne, lk 1–8.
[195] Metikoš, Ausloos 2024, lk 1-34.
[196] Ijaiya, Odumuwagun 2024, lk 3361.

juhendmaterjalidest. Seetõttu oleks vajalik koostada täiendav juhendmaterjal, mis määratleks kriteeriumid, mille alusel hinnata selgituse sisulisust ja arusaadavust.[197]

Seejuures tuleb arvestada ka asjaoluga, et erinevates sektorites ja rakenduskontekstides (nt krediidihindamine, tööalased algoritmid, avaliku sektori automatiseeritud süsteemid) võivad selgitusvajadused erineda. Seetõttu oleks põhjendatud sektoripõhiste juhiste või kontrollnimekirjade väljatöötamine, mis aitaksid tagada, et selgitatavus ei jääks formaalsuseks, vaid toetaks tegelikku õiguste teostamist.[198]

3.2.2. Andmekaitse- ja eetikapõhimõtted TI-süsteemides

Nagu käsitletud peatükis 2.2, võivad TI-l põhinevad automatiseeritud süsteemid suurendada ebavõrdset kohtlemist ja luua püsivalt ebasoodsamaid tingimusi. Seetõttu peab vastutav töötleja ennetavalt tagama, et algoritmilised otsused oleksid õiguspärased ja eetilised.

Tehisintellekti süsteemide arenduses rõhutatakse üha enam vajadust integreerida eetilised ja õiguslikud põhimõtted süsteemidesse juba projekteerimise faasis. Sellist ennetavat lähenemisviisi tähistatakse mõistetega *ethics by design* ja *fairness by design*. See tähendab, et tehnoloogiliste lahenduste loomisel tuleb proaktiivselt arvestada inimväärikust, isiksuse autonoomiat, võrdset kohtlemist ja otsustusprotsessi läbipaistvust – mitte käsitleda neid üksnes tagantjärele järelevalve või vastutuse kontekstis. Seni on Euroopa Liidu diskrimineerimisvastane õigus keskendunud üksikjuhtumite lahendamisele pärast tehisintellekti süsteemide rakendamist, mistõttu see ei suuda tõhusalt ennetada süsteemset ebaõiglust.[199]

Nagu eelpool käsitletud, võib AI Act aidata tuvastada ja vähendada diskrimineerimise riski - nt artikli 10 lõike 2 punkt f kaudu - ning suunab õigluse ja võrdse kohtlemise tagamisele juba arendusprotsessis. Samas ei sätesta määrus, millal ebavõrdne kohtlemine oleks ebaseaduslik ning seetõttu peab selle otsustama olemasolev diskrimineerimisvastane õigusraamistik.

Täiendavalt on pakutud järgmisi lahendusi:

---

[197] Metikoš, Ausloos 2024, lk 1-34.
[198] EDPB 2018, Guidelines on ADM and Profiling, lk 22.
[199] Deck jt, lk 1-5.

1. Treeningandmete kallutatuse analüüs ja korrigeerimine. Tehisintellekti kallutatus tekib siis, kui algoritmid annavad diskrimineerivaid tulemusi, mis tulenevad kallutatud treeningandmetest või vigasest süsteemidisainist. Seetõttu soovitatakse organisatsioonidel hinnata treeningandmestike kvaliteeti ning rakendada meetmeid algoritmilist kallutatuse vähendamiseks. Sellisteks meetmeteks võivad nt olla andmestike mitmekesistamine või õiglust arvestavad masinõppe tehnilised lahendused.[200] Samuti rõhutatakse vajadust arvestada, et diskrimineerimisvabadus ja õiglase kohtlemise põhimõtted tuleb tagada kogu süsteemi elutsükli jooksul, mistõttu treeningandmete kallutatuse analüüs ei tohiks piirduda ainult arendusetapiga, vaid peab jätkuma ka süsteemi kasutamise ja järelevalve etappides.[201]
2. Regulaarne audit ja järelevalve. Soovitatakse kehtestada regulaarne algoritmiline audit, mille eesmärk on tuvastada kallutatused, hinnata süsteemide õigluse taset ja tagada vastavus kehtivatele privaatsuse ja eetika standarditele.[202] Arvestades läbipaistvuse ja usaldusväärsuse olulisust, võiksid selliseid auditeid läbi viia sõltumatud järelevalveorganid, näiteks andmekaitseasutused või eetikanõukogud. Eetikasuuniste järgi tuleb auditite käigus eraldi tähelepanu pöörata läbipaistvusele ja otsustusprotsesside jälgitavusele, et oleks võimalik tuvastada vastutajad ja tagada vaidlustamise võimalus, eriti kui AI süsteem mõjutab õigusi ja vabadusi.[203]
3. Eetilised tehisintellekti raamistikud. Soovitatakse välja töötada juhtimisraamistikud, mis hõlmavad õiglust, läbipaistvust ja vastutust.[204] Eetikasuunistes on rõhutatud, et eetiliste juhiste loomisel tuleb teadvustada ja dokumenteerida tehnoloogia ja erinevate väärtuste (nt innovatsioon vs privaatsus) vahel tekkivad pinged ning esitada läbipaistvad otsused nende kompromisside kohta.[205]
4. Interdistsiplinaarne koostöö. Süsteemide kujundamisse ja järelevalvesse tuleks lisaks IT-spetsialistidele kaasata ka inimõiguste eksperte ja ühiskonnateadlasi. See aitaks ennetada konflikte tehniliste ja normatiivsete tõlgenduste vahel ning tagaks laiapõhjalise vaate.[206] Lisaks on välja pakutud, et süsteemide arenduse ja järelevalve etappidesse tuleks kaasata eetikanõukogud ning toetada interdistsiplinaarsete pilootprojektide elluviimist. Sellised struktuurid võimaldaksid hinnata süsteemide vastavust mitte üksnes tehnilistele nõuetele,

[200] Ijaiya & Odumuwagun, lk 3368.
[201] Euroopa Komisjoni kõrgetasemeline tehisintellekti ekspertgrupp, viidatud juhend, lk 2jj.
[202] Ijaiya & Odumuwagun, lk 3368.
[203] Euroopa Komisjoni kõrgetasemeline tehisintellekti ekspertgrupp, viidatud juhend, lk 14-15.
[204] Ijaiya & Odumuwagun, lk 3368.
[205] Euroopa Komisjoni kõrgetasemeline tehisintellekti ekspertgrupp, viidatud juhend, lk 3 ja II pt.
[206] van Bekkum, Zuiderveen Borgesius, lk 1-12.

vaid ka laiematele ühiskondlikele ja moraalsetele põhimõtetele.[207] Eetikasuunised soovitavad interdistsiplinaarse koostöö raames tagada ka aktiivne sidusrühmade kaasamine kogu tehisintellekti süsteemi elutsükli vältel, et erinevate väärtuste tasakaalustamisel oleks tagatud ka nõrkade huvirühmade hääl.[208]

5. Erand tundlike andmete kasutamiseks diskrimineerimise ennetamisel. Kuna diskrimineerimise tuvastamine eeldab sageli tundlike andmete (nt rahvus, sugu) töötlemist, on soovitanud lisada GDPR-i erand, mis võimaldaks töödelda selliseid andmeid üksnes õiguskaitselisel eesmärgil – diskrimineerimise ennetamiseks või tuvastamiseks, mitte äriliseks kasutuseks. Samas on rõhutatud, et sellise erandi kehtestamisega peab kaasnema täiendavate kaitsemeetmete rakendamine, nagu tundlike andmete pseudonüümimine, rangete kasutuspiirangute kehtestamine ja andmete kasutamise läbipaistvuse tagamine.[209] Sellist lähenemist toetab ka AI Act, mille artikkel 10 lõige 5 võimaldab erandkorras töödelda eriliiki isikuandmeid, kui see on rangelt vajalik kõrge riskiga süsteemide puhul eelarvamuste tuvastamiseks ja korrigeerimiseks, tuginedes avaliku huvi kaalutlusele.

Selleks, et tagada õiglane ja inimest austav tehisintellekt, peavad eetilised ja õiguslikud põhimõtted olema süsteemide loomise lahutamatu osa. Lähenemine, mis ühendab andmete teadliku valiku, regulaarne järelevalve, interdistsiplinaarse koostöö ja vajadusel ka õiguslike erandite loomise, annab võimaluse ehitada usaldusväärseid ja kaasavaid tehnoloogilisi lahendusi.

3.2.3. Andmesubjekti õiguste kaitse tugevdamine

Automatiseeritud otsustamise kasutuselevõtt ei saa piirduda üksnes õigusliku aluse valikuga. See peab tuginema sisulistele ennetusmehhanismidele, mis tagavad, et andmesubjekti õigused ja vabadused on kaitstud juba enne otsuse tegemist. Selline ennetav lähenemine on kooskõlas GDPR-i artikkel 22 lõikega 3 ning Euroopa Andmekaitsenõukogu suunistega, mille kohaselt

[207] Deck jt, lk 1-5.
[208] Euroopa Komisjoni kõrgetasemeline tehisintellekti ekspertgrupp, viidatud juhend
[209] van Bekkum, Zuiderveen Borgesius,lk 1-12.

tuleb rakendada sobivaid kaitsemeetmeid andmesubjekti huvide kaitseks. Lisaks peab olema tagatud reaalne võimalus oma õigusi realiseerida.[210]

Automatiseeritud otsustamisega seotud riskide ennetamiseks on vajalik rakendada tehnilisi ja korralduslikke kaitsemeetmeid, mis aitavad vältida andmesubjekti õiguste kahjustamist juba otsustamise protsessi algfaasis. Selliste meetmete hulka kuuluvad näiteks andmete krüpteerimine, diferentsiaalne privaatsus ja anonümiseerimine.[211]

Ennetava meetmena tuleks rakendada mõjuhinnangut, mis on GDPRi artikli 35 kohaselt nõutav kõrge riskiga andmetöötluse, sh automatiseeritud otsustamise korral. Mõjuhinnangu koostamine ei ole üksnes formaalne nõue, vaid toimib sisulise ennetava kaitsemehhanismina, mille abil saab tuvastada ja maandada riske enne nende realiseerumist. Korralikult läbi viidud hinnang aitab selgitada, kas ja kuidas võib automatiseeritud töötlemine mõjutada andmesubjektide õigusi ning milliseid meetmeid tuleb nende kaitseks rakendada. Nagu eelnevalt käsitletud Deliveroo juhtum näitab, jäävad mõjuhinnangud praktikas sageli koostamata või puudulikuks.

Praktikas jäävad mõjuhinnangud aga sageli formaalseteks dokumentideks, mille eesmärk on pigem näidata vastavust kui tegelikke riske maandada. Mõjuhinnangutega seoses viidatakse vajadusele, et andmetöötlejad ja järelevalveasutused teeksid koostööd riskide hindamisel ja maandamisel. Neid võiks käsitleda vahendina, mille kaudu on võimalik hinnata ja maandada riske enne nende realiseerumist.[212]

Nagu peatükis 2.3 käsitletud, sätestab artikli 22 lõige 2 kolm erandit, mille korral on automatiseeritud otsuste tegemine lubatud. Nende erandite rakendamine nõuab aga põhjalikku õiguslikku kaalutlust, sest praktikas on sageli keeruline hinnata, kas nende eeldused on täidetud. Vastutavad töötlejad peavad selgelt dokumenteerima, millisele õiguslikule alusele nad töötlemise puhul toetuvad, ning tagama, et selle aluse rakendamiseks nõutavad eeltingimused on täidetud. Seetõttu on vaja selgemaid juhiseid ja tugevamaid vastutuskohustuse mehhanisme, et tagada, et artikli 22 alusel ette nähtud kaitsemeetmed ja õigused ei jääks pelgalt teoreetiliseks.

---

[210] EDPB 2018, Guidelines on ADM and Profiling, lk 19jj.
[211] Ijaiya & Odumuwagun, lk 3368jj.
[212] Chaudhary, lk 111-112.

Andmetöötlejatele võiks välja töötada konkreetsed juhendid, mille alusel dokumenteerimist korraldada ning automatiseeritud töötlusel põhinevate otsuste tegemise lubatavust hinnata.

Soovitusena on pakutud ka selgitada artikli 22 lõike 2 punkti a sõnastust „vajalik lepingu sõlmimiseks või täitmiseks“. Kuna selliste otsuste vajalikkust tõlgendab tõenäoliselt vastutav töötleja ja punkt a ei nõua andmesubjekti nõusolekut (kuna see on eraldi loetletud punktis c), võib see erand andmesubjektide õigusi nõrgendada.[213] Seega oleksid selgemad juhised asjakohased.

Nagu käsitletud peatükis 2.4. näeb GDPR ette tugeva õiguste kaitsemehhanismi andmesubjektidele, kuid praktikas võib nende õiguste tegelik rakendamine osutuda keerukaks. Näiteks GDPR artikli 22 lõike 3 kohaselt peab andmetöötleja tagama, et andmesubjektil on õigus taotleda inimese sekkumist, oma seisukoha esitada ning otsust vaidlustada. Sellest tulenevalt peab süsteemi ülesehitus võimaldama andmesubjekti tegelikku sekkumist otsustusprotsessi, mitte piirduma pelgalt näilise kontrollivõimaluse loomisega.

Andmesubjektide jaoks peab õiguste kasutamine olema lihtne, kiire ja praktiliselt teostatav. GDPR-i artikli 7 lõike 3 kohaselt peab nõusoleku tagasivõtmine olema sama lihtne kui selle andmine. Seetõttu on soovitatud arendada kasutajasõbralikke digitaalseid liideseid, mis võimaldavad nõusoleku tühistamist kiiresti ja ilma täiendavate takistusteta, tagades andmesubjektile tegeliku kontrolli oma isikuandmete töötlemise üle. Lisaks on välja pakutud, et andmetöötlejad töötaksid välja standardiseeritud vaidlustusvormid ja juhendavad veebikeskkonnad, mis aitaksid andmesubjektil oma õigusi samm-sammult teostada.[214] Sellised mehhanismid muudavad õiguste kasutamise vähem koormavaks ja parandavad ligipääsetavust.

Täiendavalt tuleb rakendada organisatsioonilisi ja tehnilisi kaitsemehhanisme, nagu automatiseeritud süsteemide dokumenteerimine, sisekontroll, auditilogid ja selgitusmehhanismid. Kui tegemist on kõrge mõjuga automatiseeritud otsusega – st sellisega, mille tulemusel võivad andmesubjektil olla olulised tagajärjed, nagu laenust keeldumine,

[213] Wachter, Mittelstadt, Floridi, lk 98.
[214] Custers, Vrabec, lk 1-14.

tööpakkumisest keeldumine või muu sotsiaal-majanduslik mõju –, on soovitatud, et otsus ei jõustuks enne, kui inimene on selle läbi vaadanud ja kinnitanud.[215]

Olulist rolli mängib ka organisatsioonikultuur, kus andmekaitset käsitletakse väärtusena, mitte pelgalt juriidilise kohustusena. Regulaarsed koolitused, andmekaitseametnike volituste tugevdamine ja sisemised järelevalvemehhanismid aitavad kaasa vastutustundlikule andmetöötlusele.[216]

Et kaitsemeetmed ei jääks pelgalt sisekontrolli tasandile, tuleb andmekaitse järelevalveasutustele (nt andmekaitseinspektsioonid) tagada tegelik võimalus automatiseeritud otsustussüsteemide hindamiseks. Selleks tuleb tugevdada nii nende volitusi kui ka ressursse ning kaasata neid mõjuhinnangute hindamisse kõrge riskiga süsteemide puhul.[217] Samuti tuleb tagada, et järelevalveasutused saaksid nõuda dokumentatsiooni ja selgitusi ka omal algatusel, eriti juhtudel, kui süsteemid mõjutavad avalikke või ühiskondlikke huve.[218]

Andmesubjektide õiguste tagamine TI-põhistes automatiseeritud otsustusprotsessides on keeruline ja eeldab tihedat koostööd eri valdkondade vahel. Kuigi GDPR ja AI Act sätestavad mitmeid kaitsemeetmeid, näitab analüüs, et nende rakendamine on praktikas raskendatud ning vajab täiendavat selgust, sidusust ja järelevalvet. Läbipaistvuse ja selgitatavuse suurendamine, õiguskindluse tugevdamine, õiguslike aluste täpsustamine ning andmekaitse- ja eetikapõhimõtete integreerimine projekteerimisfaasi on keskse tähtsusega sammud andmesubjekti tegeliku kaitse tagamiseks. Samuti tuleb tugevdada mehhanisme, mis võimaldavad inimestel oma õigusi praktiliselt ja tõhusalt kasutada – olgu selleks vaidlustamisvõimalused, järelevalveasutuste pädevuse laiendamine või teadlikkuse tõstmine. Terviklik ja normatiivsetest põhimõtetest lähtuv lähenemine on hädavajalik, et tagada automatiseeritud otsustamise õiguspärasus ja õiglus.

[215] Chaudhary, lk 93-118.
[216] Ijaiya & Odumuwagun, lk 3368jj.
[217] Padden & Öjehag-Pettersson, lk 1-12.
[218] Mazur, Bernatt, lk 1097jj.

KOKKUVÕTE

Käesoleva magistritöö eesmärk oli analüüsida, kuidas GDPR-i artikkel 22 reguleerib tehisintellektil (TI) põhinevaid automatiseeritud otsuseid, millised on selle regulatsiooni piirangud ja rakendusprobleemid ning kuidas tagada andmesubjektide õiguste tõhus kaitse TI-ajastul.

Töö esimeses peatükis käsitleti GDPR-i artikli 22 reguleerimisala ja piiranguid tehisintellekti kontekstis. Artikkel 22 toimib olulise kaitsemehhanismina, piirates automatiseeritud otsustusprotsesside kasutamist, mis võivad andmesubjektile kaasa tuua õiguslikke tagajärgi või avaldada talle märkimisväärset mõju. GDPR reguleerib neid protsesse laiemas andmekaitsepõhimõtete raamistikus, hõlmates mitte ainult artikli 22 keelde ja erandeid, vaid ka üldpõhimõtteid, nagu seaduslikkus, läbipaistvus, täpsus ja andmete minimaalsus, samuti nõudeid andmesubjektide õiguste tagamise ja järelevalveasutuste rolli kohta. Vastutavad töötlejad võivad kasutada profiilianalüüsi ja automatiseeritud otsustamist ainult juhul, kui nad järgivad kõiki GDPR-i nõudeid, omavad seaduslikku töötlemisalust ja rakendavad sobivaid kaitsemeetmeid, mis kaitsevad andmesubjektide õigusi ka osaliselt automatiseeritud töötlemise korral.

Artikkel 22 seab olulisi piiranguid automatiseeritud otsustusprotsessidele. See säte on tekitanud arutelu, kas artiklit tuleks käsitleda kui andmesubjekti õigust mitte olla üksnes automatiseeritud otsuse subjekt või kui üldist keeldu selliste otsuste tegemiseks. Mõlemal lähenemisel on veenvaid argumente. Süsteemne ja objektiiv-teleoloogiline tõlgendus, mis arvestab GDPR-i ülesehitust, üldpõhimõtteid ja eesmärki kaitsta andmesubjektide õigusi, toetab seisukohta, et tegemist on üldise keeluga. Selline tõlgendus tugevdab isikuandmete kaitset ja aitab vältida TI-põhiste otsuste liigset kasutamist ilma andmesubjektide selgesõnalise nõusoleku ja piisava teavitamiseta. Samuti pakub see suuremat selgust vastutavatele töötlejatele, kes peavad järgima rangemaid vastavusnõudeid.

Artikli 22 lõike 1 kohaldamiseks peavad olema täidetud kolm tingimust. Kui esimese tingimuse – otsuse mõiste – tõlgendamisel on kujunenud suhteliselt ühtne praktika, siis „üksnes automatiseeritud töötlemise“ ja „õiguslike või märkimisväärsete mõjude“ mõistete sisustamine on olnud keerulisem. Tuginedes Euroopa Kohtu ja andmekaitseasutuste viimaste

aastate otsustele, on märgata järjest põhjalikumat ja kontekstitundlikumat lähenemist. „Üksnes automatiseeritud töötlemise“ hindamisel ei piirduta tehnilise protsessi analüüsiga, vaid hinnatakse kogu organisatsiooni ülesehitust, töötajate väljaõpet ja otsustuskohustuse tegelikku sisu. Sisuline inimsekkumine eeldab süstemaatilist ja dokumenteeritud lähenemist, mitte ainult vahepealset inimlikku kohalolekut.

Töös analüüsitud Uberi, Deliveroo ja Ola juhtumid näitavad, et GDPR-i artikli 22 kohaldamisel tuleb hinnata automatiseeritud otsuste mõju sisuliselt ja juhtumipõhiselt, mitte ainult formaalsete tunnuste alusel.

Töö teises peatükis analüüsiti automatiseeritud otsuste peamisi õiguslikke probleeme GDPR-i põhimõtete rakendamisel. GDPR nõuab, et isikuandmete töötlemine, sealhulgas automatiseeritud otsuste tegemine, oleks seaduslik, õiglane ja läbipaistev (art 5 lg 1 p a). Andmesubjektidele ette nähtud õigused on olemas, kuid nende praktiline rakendamine toob kaasa olulisi väljakutseid. Läbipaistmatud algoritmid raskendavad andmesubjektide õigust saada teavet. Kuigi GDPR ei täpsusta, kui põhjalik peab olema esitatav selgitus, on regulatiivne suundumus liikumas suurema läbipaistvuse poole. Andmesubjektile tuleb anda arusaadavat ja sisulist teavet kasutatud loogika ning otsuste võimalike tagajärgede kohta.

Algoritmilise läbipaistvuse eesmärk ei piirdu üksnes TI-süsteemide toimimise mõistmisega, vaid hõlmab ka õigluse ja võrdse kohtlemise tagamist. Läbipaistmatud otsustusprotsessid takistavad varjatud diskrimineerimise avastamist. Kuigi GDPR nõuab õiglast kohtlemist, on selle mõiste täpsem sisu määruses avamata, mistõttu on õiglane töötlemine võimalik vaid töötlemise tegelike mõjude analüüsi, süsteemsete riskide tuvastamise ja tõhusate läbipaistvuse ning auditeerimise meetmete kaudu.

Artikli 22 lõige 2 loetleb kolm erandit, mille korral automatiseeritud otsuste tegemine on lubatud, kuid nende rakendamine eeldab põhjalikku õiguslikku kaalutlust ja dokumenteeritud põhjendusi.

Kuigi GDPR annab andmesubjektidele mitmeid õigusi, on nende praktiline rakendamine sageli piiratud. Teadmatus õiguste olemasolust, tehniline keerukus, institutsionaalsed takistused ja raskesti mõistetav teave vähendavad andmesubjektide tegelikku mõjuvõimu oma andmete kasutamise üle.

Töö kolmandas peatükis käsitleti andmesubjektide õiguste kaitset TI-põhistes otsustusprotsessides ning analüüsiti GDPR-i ja AI Act-i koostoimet. AI Act täiendab GDPR-i, sest selle kohaldamisala on laiem: see reguleerib kõiki kõrge riskiga TI-süsteeme sõltumata andmetüübist. AI Act sätestab õiguse saada arusaadav selgitus TI-süsteemi rolli ja otsuste peamiste elementide kohta ning kehtestab kõrge riskiga süsteemidele jälgitavuse, läbipaistvuse ja inimjärelevalve nõuded. Tähelepanu pööratakse ka andmekvaliteedile ja algoritmilise kallutatuse ennetamisele. Siiski jäävad mõned probleemid lahendamata, näiteks piiratud kohaldamisala ja automatiseeritud otsuste sisuline hindamine.

Magistritöö tulemusena pakuti välja süstemaatiline ja objektiiv-teleoloogiline tõlgendus GDPR-i artiklile 22, käsitledes seda üldise keeluna automatiseeritud otsustele koos piiratud eranditega. See lähenemine tugevdab andmesubjektide õiguste kaitset TI-ajastul ja loob suurema õigusselguse vastutavatele andmetöötlejatele. Samuti toodi esile, et automatiseeritud otsuste sisuline hindamine peab hõlmama kogu organisatsiooni ülesehitust ja tööprotsesse, mitte ainult tehnoloogilist analüüsi. Lisaks pakuti välja uuendatud arusaam „üksnes automatiseeritud töötlusel“ ja „märkimisväärse mõju“ mõistete sisust, rõhutades inimsekkumise kvaliteedi ja dokumenteerituse tähtsust. Töö integreeris GDPR-i ja AI Act-i põhimõtted ühtseks raamistikuks, mis aitab tõhusamalt tuvastada ja lahendada TI-põhiste otsustusprotsesside riskikohti, pakkudes seeläbi õigusteadusele sisulist lisandväärtust andmekaitse ja automatiseeritud otsustamise õiguspärasuse alal.

Kokkuvõttes näitab analüüs, et andmesubjektide õiguste tagamine TI-põhistes otsustusprotsessides eeldab eri valdkondade koostööd ning suuremat läbipaistvust, õiguskindlust ja sidusust õigusaktide rakendamisel. Läbipaistvuse ja selgitatavuse suurendamine, õigusaluste täpsustamine ning andmekaitse- ja eetikapõhimõtete integreerimine projekteerimisfaasi on kesksed sammud, et tagada TI-põhiste otsuste õiguspärasus ja õiglus.

SUMMARY

Artificial Intelligence-Based Automated Decisions: Problems and Solutions in the Application of the General Data Protection Regulation (GDPR)

Automated decision-making is becoming increasingly common in the digital society, as big data and artificial intelligence enable fast and efficient data processing. This not only improves the efficiency of data processing operations and reduces resource consumption, but also allows for better personalization of services and products. Consequently, automated decisions are increasingly used across various sectors, offering more efficient and user-tailored services. However, they also introduce new data protection and transparency risks.

Due to these changes, there was a need for a strong and coherent data protection framework within the European Union, along with effective enforcement mechanisms. Therefore, the General Data Protection Regulation (GDPR) was established with the aim of protecting the personal data of EU citizens and residents, safeguarding their privacy, and mitigating the risks associated with decisions based on automated processing and profiling.

The aim of this research is to analyze how Article 22 of the GDPR regulates automated decision-making in artificial intelligence applications, as well as to identify its limitations and practical implementation challenges. The thesis also focuses on the key legal issues in applying the GDPR principles to automated decisions and discusses possible solutions to ensure effective protection of data subjects in the era of artificial intelligence.

To achieve the objective of the thesis, the following research questions have been formulated:

1. How does Article 22 of the GDPR regulate automated decision-making, and what are its limitations in the context of artificial intelligence?
2. What are the main legal issues related to the application of GDPR principles in automated decision-making?
3. How can the rights of data subjects be effectively protected in AI-based decision-making processes?

The first chapter of this thesis examines the scope and limitations of Article 22 of the GDPR in the context of artificial intelligence. Article 22 serves as a crucial safeguard by restricting the use of automated decision-making processes that may produce legal effects or similarly significant impacts on data subjects. These processes are regulated within the broader framework of the GDPR's data protection principles, encompassing not only the prohibitions and exceptions set out in Article 22 but also the general principles of lawfulness, transparency, accuracy, and data minimization, alongside obligations concerning the protection of data subjects' rights and the role of supervisory authorities.

Controllers may engage in profiling and automated decision-making only if they fully comply with the GDPR, possess a valid legal basis for processing, and implement appropriate safeguards to protect data subjects' rights, even in cases of partially automated processing.

Article 22 imposes significant restrictions on automated decision-making processes. It has sparked debate over whether it should be interpreted as granting data subjects a right not to be subject to solely automated decisions or as establishing a general prohibition on such decisions. Both interpretations offer compelling arguments. A systematic and objective-teleological interpretation—taking into account the GDPR's structure, general principles, and objective of safeguarding data subjects' rights—supports reading Article 22 as a general prohibition. This interpretation strengthens personal data protection and helps prevent the excessive use of AI-based decisions without explicit consent and adequate information, while also offering greater legal clarity for controllers, who must meet stricter compliance obligations.

Three conditions must be satisfied for the application of Article 22(1). While there is relatively consistent practice regarding the definition of a "decision," interpreting the concepts of "solely automated processing" and "legal or similarly significant effects" has proven more challenging. Based on recent decisions by the Court of Justice of the European Union and data protection authorities, there is a clear trend toward a more nuanced and context-sensitive interpretation.

In assessing "solely automated processing," analysis must extend beyond the technical process to encompass the organization's structure, employee training, and the substantive nature of decision-making responsibilities. Genuine human intervention requires a systematic and documented approach, not merely incidental human involvement.

The Uber, Deliveroo, and Ola cases analyzed in this thesis demonstrate that the impact of automated decisions must be assessed substantively and on a case-by-case basis, rather than solely based on formal characteristics.

The second chapter analyzes the key legal challenges associated with applying GDPR principles to automated decision-making. The GDPR requires that the processing of personal data, including through automated decision-making, be lawful, fair, and transparent (Article 5(1)(a)). While data subjects are granted certain rights, their practical realization faces significant obstacles. Opaque algorithms undermine the right to information, and although the GDPR does not specify the depth of explanation required, regulatory developments are moving toward increased transparency. Data subjects must be provided with clear, meaningful information about the logic involved and the potential consequences of decisions.

The goal of algorithmic transparency extends beyond understanding the functioning of AI systems; it also aims to ensure fairness and equality of treatment. Opaque decision-making processes hinder the detection of hidden discrimination. Although the GDPR requires fair processing, the concept of fairness is not precisely defined in the regulation, meaning that fair processing must be ensured through analysis of actual impacts, the identification of systemic risks, and the implementation of effective transparency and auditing measures.

Article 22(2) lists three exceptions under which automated decision-making is permitted; however, applying these exceptions requires careful legal reasoning and documented justification.

Although the GDPR grants data subjects several rights, the practical exercise of these rights is often limited by lack of awareness, technical complexity, institutional barriers, and the provision of incomprehensible information, all of which diminish individuals' actual control over their personal data.

The third chapter addresses the protection of data subjects' rights in AI-based decision-making processes and explores the interaction between the GDPR and the AI Act. The AI Act would complement the GDPR by covering all high-risk AI systems, regardless of the type of data processed. It establishes the right to receive understandable explanations concerning the role of the AI system and the key elements of its decision-making process, and it imposes traceability, transparency, and human oversight requirements on high-risk systems. Emphasis

is also placed on data quality and the prevention of algorithmic bias. Nevertheless, some challenges remain unresolved, particularly regarding the AI Act's limited scope and the substantive evaluation of automated decisions.

As a result of this thesis, a systematic and objective-teleological interpretation of Article 22 of the GDPR is proposed, treating it as a general prohibition on automated decision-making, subject to narrowly defined exceptions. This approach enhances the protection of data subjects' rights in the era of AI and provides greater legal certainty for controllers.

The analysis highlights that a substantive evaluation of automated decisions must consider the organizational structure and work processes, not just the technical aspects of processing. Furthermore, an updated understanding of the notions of "solely automated decision" and "significant effect" is proposed, emphasizing the quality and documentation of human intervention.

The thesis integrates the principles of the GDPR and the AI Act into a coherent framework to better identify and address risks associated with AI-based decision-making processes, thereby offering meaningful contributions to legal scholarship in the fields of data protection and the lawfulness of automated decision-making.

In conclusion, the analysis demonstrates that ensuring the rights of data subjects in AI-driven decision-making processes requires interdisciplinary cooperation as well as enhanced transparency, legal certainty, and consistency in the implementation of legal norms.

Strengthening transparency and explainability, clarifying legal bases, and integrating data protection and ethical principles into the design phase are critical steps toward achieving the lawfulness and fairness of AI-based decision-making.

KASUTATUD KIRJANDUS

1. Barros Vale, S., Zanfir-Fortuna, G. Automated Decision-Making under the GDPR: Practical Cases from Courts and Data Protection Authorities. Future of Privacy Forum 2022.
2. Camões, D. The challenges of the GDPR in the era of Artificial Intelligence: what can we expect from the future? – e-Publica 2024, Vol. 11 No. 3.
3. Castets-Renard, C. Accountability of Algorithms in the GDPR and beyond: A European Legal Framework on Automated Decision-Making. – Fordham Intellectual Property, Media & Entertainment Law Journal 2019, Vol. 30 No. 1.
4. Chaudhary, G. Unveiling the Black Box: Bringing Algorithmic Transparency to AI. – Masaryk University Journal of Law and Technology 2024, Vol. 18 No. 1.
5. Cotogni, G. The Explainability of Automated Decision-Making: A Historical Perspective through EU Legislation – Journal of Law, Market & Innovation 2024, Vol. 3 Issue 3.
6. Custers, B., Vrabec, H. Tell me something new: data subject rights applied to inferred data and profiles. – Computer Law & Security Review, 2024, Vol. 52.
7. Deck, L., Müller, J.-L., Braun, C., Zipperling, D., Kühl, N. Implications of the AI Act for Non-Discrimination Law and Algorithmic Fairness. – CEUR Workshop Proceedings, EWAF'24: European Workshop on Algorithmic Fairness, 1–3 July 2024, Mainz, Germany.
8. Euroopa Komisjoni kõrgetasemeline tehisintellekti ekspertgrupp. Ethics Guidelines for Trustworthy AI. 8. aprill 2019. Kättesaadav: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (vaadatud 26.04.2025).
9. Häuselmann, A., Custers, B. Substantive fairness in the GDPR: Fairness Elements for Article 5.1a GDPR. – Computer Law & Security Review 2024, Vol. 52.
10. Ijaiya, H., Odumuwagun, O. O. Advancing Artificial Intelligence and Safeguarding Data Privacy: A Comparative Study of EU and US Regulatory Frameworks Amid Emerging Cyber Threats. – International Journal of Research Publication and Reviews, 2024, Vol. 5, No. 12.
11. Kosinski, M., Stillwell, D., Graepel, T. Private traits and attributes are predictable from digital records of human behavior. – Proceedings of the National Academy of Sciences of the United States of America 2013, Vol. 110 No. 15. Kättesaadav: https://www.pnas.org/doi/pdf/10.1073/pnas.1218772110 (vaadatud 26.04.2025).

12. Malgieri, G. The Concept of Fairness in the GDPR: A Linguistic and Contextual Interpretation. – Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT* '20), January 27–30, 2020, ACM, New York.
13. Mazur, J., Bernatt, M. Can the Automated State Be Trusted? The Role of Rule of Law Safeguards for Governing Automated Decision-Making and Artificial Intelligence. – Georgia Law Review, 2024, Vol. 58, No. 3.
14. Metikoš, L., Ausloos, J. The right to an explanation in practice: insights from case law for the GDPR and the AI Act. – Law, Innovation and Technology, 2025.
15. Nišević, M., Cuypers, A., De Bruyne, J. Explainable AI: Can the AI Act and the GDPR go out for a date? – 2024 International Joint Conference on Neural Networks (IJCNN), IEEE, 2024.
16. Nišević, M., Sears, A. M., Fosch-Villaronga, E., Custers, B. Understanding the legal bases for automated decision-making under the GDPR. – Research Handbook on EU Data Protection, eds. Kostas, E., Leenes, R., Kamara, I., Edward Elgar Publishing 2022.
17. Padden, M., Öjehag-Pettersson, A. Digitalisation, democracy and the GDPR: The efforts of DPAs to defend democratic principles despite the limitations of the GDPR. – Big Data & Society, October–December 2024, Vol. 11, No. 4.
18. Pi, Y. Empowering Individuals in Automated Decision-Making: Explainability, Contestability and Beyond. – CSCW Companion '24, November 9–13, 2024, San Jose, Costa Rica, ACM, New York.
19. Thouvenin, F., Früh, A., Henseler, S. Article 22 GDPR on Automated Individual Decision-Making: Prohibition or Data Subject Right? – European Data Protection Law Review 2022, Vol. 8 No. 2.
20. van Bekkum, M., Zuiderveen Borgesius, F. Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception? – Computer Law & Security Review 2023, Vol. 48.
21. Wachter, S., Mittelstadt, B., Floridi, L. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. – International Data Privacy Law 2017, Vol. 7, No. 2
22. Wachter, S., Mittelstadt, B., Russell, C. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. – Harvard Journal of Law & Technology 2018, Vol. 31 No. 2
23. Wiedemann, K. Profiling and (automated) decision-making under the GDPR: A two-step approach. – Computer Law & Security Review 2022, Vol. 45.

KASUTATUD ÕIGUSAKTID JA SUUNISED

24. Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. Vastu võetud Roomas 4. novembril 1950, jõustunud 3. septembril 1953.
25. Euroopa Parlament ja Euroopa Liidu Nõukogu. Määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta ning millega tunnistatakse kehtetuks direktiiv 95/46/EÜ (isikuandmete kaitse üldmäärus), 27.04.2016. – ELT L 119, 4.5.2016.
26. Euroopa Parlament ja Euroopa Liidu Nõukogu. Määrus (EL) 2024/1689 tehisintellekti käsitlevate ühtlustatud õigusnormide kohta, 13.06.2024. – ELT L 2024/1689, 12.07.2024.
27. European Data Protection Board (EDPB). Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, version 2.0, 8 October 2019.
28. European Data Protection Board (EDPB). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251 rev.01, endorsed by the EDPB on 6 July 2018, initially adopted by the Article 29 Working Party in 2018.
29. European Data Protection Board (EDPB). Guidelines on Transparency under Regulation 2016/679, WP260 rev.01, endorsed by the EDPB on 11 April 2018, initially adopted by the Article 29 Working Party on 29 November 2017.

KASUTATUD KOHTUPRAKTIKA JA ANDMEKAITSEASUTUSTE OTSUSED

30. Berliini Andmekaitseamet. Otsus 31. mai 2023. Kättesaadav: https://gdprhub.eu/index.php?title=BlnBDI_(Berlin)_-_31.05.2023 (vaadatud 26.04.2025).
31. District Court of The Hague, 5. veebruar 2020, NJCM et al. v. the State of the Netherlands, ECLI:NL:RBDHA:2020:865
32. EKo C-524/06, Heinz Huber vs. Saksamaa, ECLI:EU:C:2008:724.
33. EKo C-634/21, SCHUFA Holding AG, ECLI:EU:C:2023:957.
34. Gerechtshof Amsterdam, 24. aprill 2023, Uber, ECLI:NL:GHAMS:2023:793.

35. Itaalia Andmekaitseamet. Decision against Deliveroo Italy S.r.l. 22. juuli 2021. Kättesaadav: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9685994 (vaadatud 26.04.2025).
36. Rechtbank Amsterdam, 11. märts 2021, Ola, ECLI:NL:RBAMS:2021:1019.
37. Rechtbank Amsterdam, 3. veebruar 2021, Uber, ECLI:NL:RBAMS:2021:1018.