ჯუზეპე დ'აკვისტო*
ლუდოვიკა დე ბენედეტი**

კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების დანერგვის ჩარჩო მონაცემთა სანდო გაზიარების მიზნით

1. მონაცემთა გაზიარების კონცეფცია

მონაცემები წარმოადგენს აუცილებელ აქტივს, რომლებიც ორგანიზაციებს ეხმარება მიაღწიონ თავიანთ დასახულ მიზნებს და შექმნან ღირებული პროდუქტი. მაგალითად, მონაცემების შეგროვება და ანალიზი შესაძლებელია მომხმარებლის გამოცდილების გაუმჯობესების, ბიზნეს ოპერაციების ოპტიმიზაციის ან ორგანიზაციის ინტერესებიდან გამომდინარე, ინოვაციების ხელშეწყობის მიზნით იყოს გამოყენებული.

თუმცა მონაცემები ხშირად სცილდება იმ ორგანიზაციების ფარგლებს, რომლებმაც თავდაპირველად შეაგროვეს და გამოიყენეს ისინი. სხვა წყაროებთან შერწყმისას მონაცემებს შეუძლიათ ახალი ინფორმაციის გენერირება, ახალი პროდუქტებისა და მომსახურების განვითარების მხარდაჭერა და როგორც სოციალური, ასევე ეკონომიკური ზრდის სტიმულირება. ამგვარად, თავდაპირველი ღირებულების მიღმა შესაძლებელია ერთი და იმავე მონაცემთა ნაკრებიდან დამატებითი ღირებულების მიღება.[1]

ამ დაკვირვების საფუძველზე, ბევრმა ორგანიზაციამ ხელი შეუწყო „მონაცემთა გაზიარების" კონცეფციას, რომელსაც შეუძლია მიიღოს მონაცემთა მართვის შიდა სტრატეგიების ფორმა ერთი კომპანიის ფარგლებში ან კანონმდებლობით განსაზღვრული სახით ეროვნულ ან საერთაშორისო დონეზე.[2] ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის ("OECD") თანახმად, მონაცემთა გაზიარება „გულისხმობს მონაცემებზე წვდომის უზრუნველყოფას სხვების მიერ გამოყენების მიზნით, შესაბამისი ტექნიკური, ფინანსური, სამართლებრივი ან ორგანიზაციული მოთხოვნების

---

* Garante per la Protezione dei Dati Personali Italian Data Protection Authority.

** Institute of International Legal Studies (ISGI), Consiglio Nazionale delle Ricerche (CNR) - Italy.

[1] According to the Organization for Economic Cooperation and Development (OECD), data access and sharing can help generate social and economic benefits worth between 0.1% and 1.5% of gross domestic product (GDP) in the case of public-sector data, and between 1% and 2.5% of GDP when also including private-sector data (https://www.oecd.org/digital/data-governance/). The EU Commission forecasts that the value of the data economy in the EU27 area is expected to reach €829 billion by 2025, up from €301 billion in 2018 with a compound annual growth rate (CAGR) of more than 14% <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en> [01.06.2024].

[2] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, 2019 <https://doi.org/10.1787/276aaca8-en> [15.09.2025].

დაცვით“.[3] „ის მოიცავს როგორც მონაცემების ხელახალ გამოყენებას კომერციული და არაკომერციული პირობითი მონაცემთა გაზიარების შეთანხმებების საფუძველზე, ასევე ღია მონაცემებს.“[4]

უფრო ფართო და მრავალფეროვანი მონაცემთა ნაკრების შეგროვებით ორგანიზაციებს შეუძლიათ ინოვაციებისა და ზრდის ხელშეწყობა უფრო ფართო, საზოგადოებრივი ინტერესებიდან გამომდინარე. მაგალითად, როდესაც ჯანდაცვის სერვისების მიმწოდებლები მონაცემებს მკვლევრებს უზიარებენ, აღნიშნულით უმჯობესდება დიაგნოზების სიზუსტე და უფრო ეფექტიანი მკურნალობის საფუძველია. ანალოგიურად, როდესაც საჯარო ხელისუფლების მიერ მონაცემების გაზიარების პროცესში უმჯობესდება კოორდინაცია და კრიზისულ სიტუაციებში რეაგირება (პანდემიები ან სტიქიური უბედურებები), მონაცემთა გაზიარებამ შეიძლება საშუალება მისცეს ორგანიზაციებს მიიღონ ახალი ინფორმაცია, შეიმუშაონ ახალი პროდუქტები და მომსახურება საზოგადოებრივი სარგებლისთვის, რომელთა შექმნასაც ისინი სხვა შემთხვევაში ვერ შეძლებდნენ. აღნიშნულმა შეიძლება გააძლიეროს კონკურენტუნარიანობა, შესაბამისად, შეიქმნას სამუშაო ადგილები. ამიტომ მონაცემთა გაზიარებას აქვს პოტენციალი, გაუმჯობესოს გადაწყვეტილების მიღების პროცესი, შედეგი და, საბოლოოდ, სარგებელი მოუტანოს საზოგადოებას.

ამავდროულად, მონაცემთა გაზიარებას შეიძლება, მოჰყვეს გარკვეული რისკი და უარყოფითი შედეგები. ინდივიდუალური ზიანის გარდა (პირადი ცხოვრების ხელშეუხებლობის დარღვევა), ერთ-ერთი ყველაზე აქტუალური პრობლემა ჯგუფური დისკრიმინაციაა.[5] ეს ხდება მაშინ, როდესაც გაზიარებული მონაცემთა ნაკრებები გამოიყენება იმგვარად, რომ იქმნება დისკრიმინაციის ახალი ფორმები ან მძაფრდება კონკრეტული სოციალური ჯგუფების მიმართ მიკერძოება (ეთნიკური კუთვნილების სქესის, ასაკის, სოციალურ-ეკონომიკური სტატუსის და სხვა მახასიათებლებთან დაკავშირებით). მაშინაც კი, როდესაც მონაცემები ანონიმურია, ნიმუშებითა და კორელაციებით შეიძლება დაიდენტიფიცირდეს ის ჯგუფები, რომლებიც შემდეგ დიფერენცირებულ მოპყრობას ექვემდებარებიან. მაგალითად, გაზიარებულ მონაცემთა ნაკრებებზე დაფუძნებული ალგორითმული გადაწყვეტილების მიღებამ შეიძლება პირთა გარკვეული წრე არახელსაყრელ მდგომარეობაში ჩააგდოს კრედიტებზე, ჯანდაცვაზე ან დასაქმების შესაძლებლობებზე წვდომის თვალსაზრისით[6]. ეს შეიძლება მოხდეს

[3] *OECD, Recommendation of the Council on Enhancing Access to and Sharing of Data, OECD/LEGAL/0463, 2021* <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463> [15.09.2025].

[4] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, 2019 <https://doi.org/10.1787/276aaca8-en> [15.09.2025].

[5] *Favaretto M., De Clercq E. & Elger B.S.,* Big Data and discrimination: perils, promises and solutions. A systematic review, J Big Data 2019, 6-12 <https://doi.org/10.1186/s40537-019-0177-4> [01.09.2025].

[6] *d'Alessandro B., O'Neil C., La Gatta T.,* Conscientious Classification: a Data Scientist's Guide to Discrimination-Aware Classification, Big Data, 2017, 5(2), 120–34. *Schermer BW.*, The Limits of Privacy in Automated Profiling

მონაცემთა „დაბინძურების“ გამო, რაც გამოწვეულია ისტორიულად დამახინჯებული მონაცემთა ნაკრებით ან მონაცემთა მაინერების მიერ შემოღებული სუბიექტური კლასობრივი ეტიკეტირებით. გარდა ამისა, შეიძლება არსებობდეს „შეგროვების მიკერძოება“, რაც გამოწვეულია კონკრეტული ჯგუფების სისტემატური არასაკმარისი ან გადაჭარბებული წარმოდგენით, რაც პოტენციურად იწვევს დისკრიმინაციულ ან არათანაბარ მოპყრობას[7].

სინამდვილეში, მონაცემთა გაზიარების შედეგად წარმოშობილი რისკები არ შემოიფარგლება მხოლოდ განზრახ ბოროტად გამოყენებით, არამედ შეიძლება, წარმოიშვას ერთი შეხედვით ნეიტრალური პრაქტიკიდანაც, როგორიცაა მონაცემთა მოდელის დიზაინი ან ტრენინგის მონაცემთა ნაკრების შერჩევა. ამიტომ სხვადასხვა ტიპის პოტენციური დისკრიმინაციის რისკის მოგვარება მოითხოვს პროაქტიული დაცვის ზომებს, მათ შორის მიკერძოების აუდიტს, სამართლიანობის შეფასებებს და ინკლუზიურ მმართველობას.

ამავდროულად, მონაცემთა გაზიარება ხშირად გულისხმობს პერსონალური მონაცემების დამუშავებას, რომლებიც ეხება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს. მონაცემთა გაზიარების პრაქტიკა ავტომატურად არ იწვევს მონაცემთა დაცვის უფლების დარღვევას, თუმცა, ვინაიდან გაზიარება გულისხმობს პერსონალური მონაცემების დამუშავებას, აუცილებელია მონაცემთა დაცვის პრინციპების მკაცრი დაცვა. ამ პრინციპების დაცვა უზრუნველყოფს მონაცემთა მწარმოებლებსა და მომხმარებლებს შორის ნდობის განმტკიცებას, რაც მნიშვნელოვანი ეკონომიკური ღირებულების გენერირების წინაპირობაა. გარდა ამისა, პერსონალური მონაცემების „საზოგადოებრივი სარგებლისთვის“ დამუშავებისას უმნიშვნელოვანესია იმის უზრუნველყოფა, რომ ამგვარი დამუშავება პროპორციული იყოს ძირითად საზოგადოებრივ ინტერესთან მიმართებით.

მონაცემთა დაცვის პრინციპების გათვალისწინებით, ორგანიზაციები არა მხოლოდ ამცირებენ მონაცემთა ბოროტად გამოყენების რისკებს, არამედ ქმნიან ხელსაყრელ გარემოს ინოვაციური თანამშრომლობისთვის.

მონაცემთა სათანადო დამუშავება გადამწყვეტია მონაცემთა სრული მნიშვნელობის გამოსავლენად, რადგან მას შეუძლია საზოგადოებაში ნდობის ჩამოყალიბება. მონაცემთა გაზიარების პროცესში ჩართულ პირებს სურთ ჰქონდეთ გონივრული მოლოდინი, რომ მათი მონაცემები გამოყენებული იქნება ეთიკური და ლეგიტიმური მიზნებისთვის.

ამ მხრივ, მნიშვნელოვანი სტრატეგიაა "by-design" მიდგომა,[8] რომელიც სისტემების დიზაინში თავიდანვე მონაცემთა დაცვისა და ეთიკური

and Data Mining, Comput Law Secur Rev. 2011, 27(1), 45–52. *Kroll JA., Huey J., Barocas S., Felten EW., Reidenberg JR., Robinson DG., Yu HL*., Accountable algorithms, Univ Pa Law Rev. 2017, 165(3), 633–705.

[7] *Brayne S.,* Big Data surveillance: the case of policing, Am Sociol Rev. 2017, 82(5), 977–1008. *Barocas S., Selbst AD.,* Big Data's disparate impact. California Law Rev. 2016, 104(3), 671–732.

[8] Art. 25, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR).

მოსაზრებების ინტეგრირებას ითვალისწინებს. ამ მიდგომის გამოყენებით, ორგანიზაციებს შეუძლიათ გააძლიერონ მონაცემთა მართვის პრაქტიკა და უზრუნველყონ მონაცემთა პასუხისმგებლიანი და ეფექტიანი გაზიარება.

ამ მიდგომის მიხედვით, ტექნიკური და ორგანიზაციული ზომების ერთობლიობა (კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები, "PET"), ხელმისაწვდომია სხვადასხვა დონეზე.[9] ეს ტექნოლოგიები მიზნად ისახავს კონფიდენციალობის რისკების შემცირებას მონაცემების გაზიარებისას, მათ შორის, განსაკუთრებული კატეგორიის ან კონფიდენციალური ინფორმაციის, რითაც ხელი ეწყობა ინოვაციებს.

წინამდებარე სტატია მიმოიხილავს სამართლებრივ ინსტრუმენტებს, რომლებიც ხელს უწყობს მონაცემთა გაზიარებას, დაკავშირებულ რისკებს და მონაცემთა დაცვის კანონმდებლობით გათვალისწინებულ დამცავ ზომებს. განსაკუთრებული ყურადღება ეთმობა კონფიდენციალობის გამაძლიერებელ ტექნოლოგიებს როგორც სანდო მონაცემთა გაზიარების სამართლებრივ, ასევე ტექნიკურ ინსტრუმენტებსა და რეკომენდაციებს.

2. მონაცემთა გაზიარების ხელშემწყობი სამართლებრივი ინსტრუმენტები

მსოფლიოში კანონმდებლებს შორის მზარდი ინტერესი არსებობს მონაცემთა გაზიარების რეგულირების მიმართ, რაც აისახება როგორც ეროვნულ, ასევე საერთაშორისო დონეზე. ეს ტენდენცია ინოვაციის, ეკონომიკური კონკურენტუნარიანობისა და საზოგადოებრივი კეთილდღეობის ძირითადი ხელშემწყობი ფაქტორებია, მაგრამ მათი გაზიარება მნიშვნელოვან სამართლებრივ, ეთიკურ და სოციალურ გამოწვევებს წარმოშობს. ჯერ კიდევ 2019 წელს ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციამ ("OECD") 30-ზე მეტ ქვეყანაში 200-ზე მეტი მთავრობის ხელმძღვანელობით გამოავლინა ინიციატივა, რომელიც მიზნად ისახავდა მონაცემთა გაზიარების ხელშეწყობას. ამ ინიციატივების უმეტესობა (თითქმის 65%) საჯარო სექტორის მიერ შენახული მონაცემების გაზიარებაზეა ორიენტირებული, მაგრამ მნიშვნელოვანი ნაწილი (დაახლოებით 15%) კერძო სექტორში მონაცემთა გაზიარების ხელშეწყობის მიზანს ისახავს. აღსანიშნავია, რომ ამ ინიციატივების თითქმის ნახევარი პერსონალური მონაცემების გაზიარებას გულისხმობდა, რაც მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის ჩარჩოსთან შესაბამისობის თვალსაზრისით პრობლემას ქმნიდა[10].

[9] The United Nations guide on Privacy-Enhancing Technologies for official statistics. United nations Big Data 2023 <https://unstats.un.org/bigdata/task-teams/privacy/guide/2023_UN%20PET%20Guide.pdf> [25.09.2025].

[10] *The World Economic Forum*, *Good Data: Sharing Data and Fostering Public Trust and Willingness*, p. 6, 2021 <www.weforum.org/whitepapers/good-data-sharing-data-and-fostering-public-trust-and-willingness/> [10.09.2025] and *Organization for Economic Co-operation and Development, Economic and social benefits of data access and sharing* - in *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, Chapter 3, OECD Publishing, 2019 <www.oecd-ilibrary.org//sites/276aaca8-

ქვემოთ წარმოგიდგენთ ბოლოდროინდელი ინიციატივების მაგალითს, რომლებიც მიზნად ისახავს (ეროვნული) მონაცემთა ნაკრებების შეგროვების, დამუშავებისა და გადაცემის რეგულირებას:

- ევროკავშირის მიერ ცოტა ხნის წინ განხორციელდა ორი საკანონმდებლო ინიციატივა, „მონაცემთა მმართველობის შესახებ ევროპული აქტი"[11] და „მონაცემთა შესახებ ევროკავშირის აქტი"[12], რომლებიც მიზნად ისახავს მონაცემთა გაზიარების ხელშეწყობას საჯარო და კერძო სექტორებში. „მონაცემთა მმართველობის შესახებ ევროპული აქტი" ხელს უწყობს მონაცემთა გაზიარებას ზომების ერთობლიობის დადგენით, ასევე, საჯარო სექტორსა და ხელახლა მომხმარებელს შორის ახალ სახელშეკრულებო შეთანხმებებს. ანალოგიურად, „მონაცემთა შესახებ ევროკავშირის აქტი" ადგენს მონაცემთა გაცვლის წესებს, ხსნის სახელშეკრულებო დისბალანსს და განსაზღვრავს იმ გარემოებებს, რომელთა არსებობის შემთხვევაშიც საჯარო სექტორის ორგანოებს შეუძლიათ წვდომა და მათზე კერძო კომპანიების მიერ შენახული მონაცემების გამოყენება ზოგადი მიზნებისთვის;
- „მონაცემთა ხელმისაწვდომობისა და გამჭვირვალობის შესახებ 2022 წლის კანონი" (ავსტრალია)[13] ადგენს მონაცემთა გაზიარების სქემას, რომლის მიხედვითაც ორგანოები უფლებამოსილნი არიან, გაუზიარონ საჯარო სექტორის მონაცემები აკრედიტებულ მომხმარებლებს, ხოლო აკრედიტებულ მომხმარებლებს უფლებამოსილება აქვთ, შეაგროვონ და გამოიყენონ მონაცემები კონტროლირებადი გზით;[14]
- „მონაცემთა გაზიარების მმართველობის ჩარჩო" (2022, დიდი ბრიტანეთი)[15] ადგენს დიდი ბრიტანეთის საჯარო სექტორის ორგანოებს შორის მონაცემთა გაზიარების სახელმძღვანელო პრინციპებს, ამასთან, ითვალისწინებს ასეთი გაზიარების ტექნიკურ (თანამედროვე სისტემებთან თავსებადობა, მონაცემთა განსხვავებული ფორმატები) და ორგანიზაციულ ბარიერებს;

---

en/1/2/3/index.html?itemId=/content/publication/276aaca8-en&_csp_=a1e9fa54d39998ecc1d83f19b8b0fc34&itemIGO=oecd&itemContentType=book> [15.09.2025].

[11] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, p. 1–44. <https://eur-lex.europa.eu/eli/reg/2022/868/oj> [15.09.2025].

[12] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 22.12.2023, p. 1-71. <https://eur-lex.europa.eu/eli/reg/2023/2854> [15.09.2025].

[13] Australian Data Availability and Transparency Act 2022 <www.datacommissioner.gov.au/law/dat-act> - Legal-Text available at: <www.legislation.gov.au/C2022A00011/latest/text> [01.06.2025].

[14] Sections 8 – 13 of the complementary "Data Availability and Transparency Act 2022" list "circumstances in which (data) sharing is barred"

[15] Uk, Data Sharing Governance Framework, 2022 <www.gov.uk/government/publications/data-sharing-governance-framework/data-sharing-governance-framework> [01.06.2025].

- „კონფიდენციალობის დაცვისა და მონაცემთა გაზიარებისა და ანალიტიკის ხელშეწყობის ეროვნული სტრატეგია“ (2023, აშშ) მიზნად ისახავს აშშ-ის ფედერალური მთავრობის საჯარო სექტორის ორგანოებს შორის მონაცემთა გაზიარებისა და ანალიტიკის მნიშვნელოვან განვითარებას;[16]
- ამის საპირისპიროდ, ჩინეთის მიერ ცოტა ხნის წინ იქნა მიღებული რიგი ზომები, რომლებიც ორიენტირებულია ტრანსასაზღვრო მონაცემთა ნაკადების რეგულირებაზე. ესენია: პერსონალური ინფორმაციის გადაცემის ხელშეკრულების სტანდარტული პირობები (ძალაშია 2023 წლის 1 ივნისიდან)[17], ტრანსასაზღვრო მონაცემთა გადაცემის ხელშეწყობისა და რეგულირების შესახებ რეგულაციები (ძალაშია 2024 წლის 22 მარტიდან)[18] და ქსელურ მონაცემთა უსაფრთხოების მართვის რეგულაცია (ქსელური მონაცემების რეგულაცია) (ძალაშია 2025 წლის 1 იანვრიდან)[19]. აღნიშნული ინსტრუმენტების ერთობლიობა ასახავს შემზღუდველ და სუვერენიტეტზე ორიენტირებულ მიდგომას, რომელიც ცდილობს მონაცემებზე სახელმწიფო კონტროლის დამყარებას;
- საუდის არაბეთის მონაცემთა გაზიარების პოლიტიკა (مشاركة سياسة البيانات)[20] 2024 წელს დამტკიცდა და გამოიცა საუდის არაბეთის მონაცემებისა და ხელოვნური ინტელექტის ორგანოს (“SDAIA”) მიერ. იგი მონაცემთა უსაფრთხო გაზიარების ყოვლისმომცველ ჩარჩოს ადგენს და განსაზღვრავს მთავრობის მიერ მონაცემთა გაცვლის მკაფიო წესებს “Government Service Bus”-ისა და “Data Marketplace”-ის მეშვეობით, აწესებს მკაცრი ავტორიზაციისა და კლასიფიკაციის მოთხოვნებს და აფასებს კანონიერების, უსაფრთხოების, გამჭვირვალობისა და ეთიკური გამოყენების გარანტიებს. ასევე, პოლიტიკა აწესებს მოთხოვნის დამუშავებისთვის სავალდებულო ვადებს, ავალდებულებს ჩანაწერების წარმოებას და პირადი მონაცემების დაცვის კანონის დაცვის

[16] Table 1 on Page 15 of this National Strategy lists technologies suitable for Privacy Preserving Data Sharing and Analytics.

[17] China, Measures for the Standard Contract for the Outbound Transfer of Personal Information, Cyberspace Administration of China, Decree No. 13 (effective 1 June 2023). Text available at the following link: <https://appinchina.co/government-documents/measures-for-the-standard-contract-for-outbound-transfer-of-personal-information/?utm_source=chatgpt.com> [20.09.2025].

[18] China, Provisions on Facilitating and Regulating Cross-Border Data Flow (effective 22 March 2024). Text and commentary available at: <www.chinalawupdate.cn/2024/04/articles/data-privacy/china-issues-regulations-on-facilitating-and-regulating-cross-border-data-flow/?utm_source=chatgpt.com> and <www.loc.gov/item/global-legal-monitor/2024-05-13/china-new-rules-on-cross-border-data-transfers-released/?utm_source=chatgpt.com> [20.09.2025].

[19] Regulation on Network Data Security Management (effective 1 January 2025), State Council Decree No. 790. Text available at the following link: <https://appinchina.co/government-documents/regulation-on-network-data-security-management/?utm_source=chatgpt.com> [20.09.2025]; official translation in English <https://english.www.gov.cn/policies/latestreleases/202409/30/content_WS66fab6c8c6d0868f4e8eb720.html?utm_source=chatgpt.com> [20.09.2025].

[20] SDAIA, Data Sharing Policy, 2024 <https://sdaia.gov.sa/en/SDAIA/about/Documents/DataSharingPolicyEN.pdf> [22.09.2025].

უზრუნველყოფას და "SDAIA"-ს ანიჭებს იმპლემენტაციისა და აღსრულების ზედამხედველობის უფლებამოსილებას.

აღნიშნული ინიციატივების ერთობლიობა მონაცემთა გაზიარების გლობალური მიდგომების განსხვავებულ მხარეებს ასახავს. მიუხედავად იმისა, რომ ევროკავშირი და ავსტრალია ფოკუსირებულია ნდობის განმტკიცებასა და მონაცემთა ხელახალი გამოყენების რეგულირებადი მექანიზმების შექმნაზე, დიდი ბრიტანეთი ხაზს უსვამს მმართველობასა და მოქნილობას, აშშ - კონფიდენციალობის დაცვის გაზიარების ტექნოლოგიურ გადაწყვეტილებებს, ჩინეთი იღებს სუვერენიტეტზე დაფუძნებულ მოდელს, რომელიც პრიორიტეტს ანიჭებს სახელმწიფო ზედამხედველობას, ხოლო საუდის არაბეთი ხაზს უსვამს წესებზე დაფუძნებულ, პრინციპებზე ორიენტირებულ სისტემას, რომელიც ორიენტირებულია უსაფრთხოებაზე, ეთიკურ გამოყენებასა და "SDAIA"-ს მეშვეობით სამთავრობათაშორისო კოორდინაციაზე. ამ განსხვავებების მიუხედავად, საერთო მნიშვნელია იმის აღიარება, რომ მონაცემთა გაზიარება აქტიურად უნდა იყოს რეგულირებული არა მხოლოდ ინოვაციისა და ზრდის პოტენციალის თვალსაზრისით, არამედ კონფიდენციალობის, სამართლიანობისა და ეროვნული უსაფრთხოების რისკების მოსაგვარებლად.

მიუხედავად ამისა, ქვეყნებს შორის ჰარმონიზებული მიდგომების ნაკლებობა, განსაკუთრებით პერსონალურ და კონფიდენციალურ მონაცემებთან დაკავშირებით, კვლავ ზღუდავს ტრანსასაზღვრო წვდომას. ეს ხარვეზი კვლავ გრძელდება საერთაშორისო მოწოდებების მიუხედავად, როგორებიცაა ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის რეკომენდაცია საჯარო სექტორის ინფორმაციაზე გაძლიერებული წვდომისა და უფრო ეფექტური გამოყენების შესახებ (2008)[21], ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის კანკუნის დეკლარაცია ციფრული ეკონომიკის შესახებ (2016)[22] და G20 ციფრული ეკონომიკის მინისტრთა დეკლარაცია (2024)[23], რომლებიც ხაზს უსვამს საერთაშორისო შეთანხმებებისა და თავსებადი კონფიდენციალობის ჩარჩოების შემუშავების მნიშვნელობას, რათა ხელი შეუწყოს იურისდიქციებს შორის მონაცემთა უსაფრთხო და სანდო ნაკადებს.

3. მონაცემთა გაზიარების სამართლებრივი არქიტექტურა

პერსონალური მონაცემების დამუშავების ფარგლებში მონაცემთა გაზიარება არ წარმოადგენს დაურეგულირებელ პროცესს. პირიქით, ის ინტეგრირებულია საერთაშორისო და რეგიონული სამართლებრივი ნორმების

[21] *OECD, Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information, OECD, Paris, 2008* <https://legalinstruments.oecd.org/public/doc/122/122.en.pdf> [22.09.2025].
[22] *OECD, Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration), OECD, Paris, 2016* <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0426> [22.09.2025].
[23] G20 Digital Economy Ministerial Conference, 2024 <https://www.g20.utoronto.ca/2024/240913-digital-ministerial-declaration.html> [15.09.2025].

ქსელში, რომელიც მოითხოვს, რომ მონაცემთა გაზიარების ნებისმიერი პრაქტიკა უზრუნველყოფდეს მონაცემთა დაცვის ძირითადი პრინციპებისა და პირთა უფლებების დაცვას. აღნიშნული ვალდებულებები შეიძლება გამომდინარეობდეს რამდენიმე საერთაშორისო ინსტრუმენტიდან, განსაკუთრებით ევროპის საბჭოს კონვენციიდან პერსონალური მონაცემების ავტომატური დამუშავების დროს ფიზიკური პირების დაცვის შესახებ (108-ე კონვენცია), ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის სახელმძღვანელო პრინციპებიდან პერსონალური მონაცემების კონფიდენციალობისა და ტრანსსასაზღვრო ნაკადების დაცვის შესახებ (1980, გადაიხედა 2013 წელს) და, ზოგადად, კონფიდენციალობის უფლებიდან, რომელიც გათვალისწინებულია სამოქალაქო და პოლიტიკური უფლებების შესახებ საერთაშორისო პაქტის (“ICCPR”) მე-17 მუხლითა და ადამიანის უფლებათა ევროპული კონვენციის (“ECHR”) მე-8 მუხლით.

გლობალურ დონეზე ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის (“OECD”) სახელმძღვანელო პრინციპები კონფიდენციალობის დაცვისა და პერსონალური მონაცემების ტრანსსასაზღვრო ნაკადების შესახებ (პირველად მიღებული 1980 წელს და განახლებული 2013 წელს) კვლავ ერთ-ერთ პირველ და ყველაზე გავლენიან მცდელობად რჩება ტრანსასაზღვრო მონაცემთა ნაკადების თანმიმდევრული ჩარჩოს უზრუნველყოფის მიმართულებით. ეს სახელმძღვანელო პრინციპები ადგენს ისეთ ძირითად პრინციპებს, როგორებიცაა მიზნის განსაზღვრა, მონაცემთა მინიმიზაცია და ანგარიშვალდებულება და კვლავაც წარმოადგენს როგორც ეროვნული კანონმდებლობის, ასევე საერთაშორისო მოლაპარაკებების ინფორმირების საშუალებას[24].

ანალოგიურად, გაერთიანებული ერების ორგანიზაციის ფარგლებში, სამოქალაქო და პოლიტიკური უფლებების შესახებ საერთაშორისო პაქტის (“ICCPR”) მე-17 მუხლით გათვალისწინებული პირადი ცხოვრების ხელშეუხებლობის უფლება სულ უფრო ხშირად განიმარტება, როგორც ციფრული გარემოს იმგვარი გავრცობა, რომლითაც იზღუდება პერსონალური მონაცემების გაზიარების ან გადაცემის გზები იურისდიქციებს შორის.[25] ასევე, გაეროს გენერალურმა ასამბლეამ მიიღო მრავალი რეზოლუცია, რომლებიც აღიარებს პირადი ცხოვრების ხელშეუხებლობის დაცვის მნიშვნელობას ციფრული კომუნიკაციებისა და ტრანსასაზღვრო მეთვალყურეობის კონტექსტში, რაც ირიბად აყალიბებს მონაცემთა მმართველობის შესახებ გლობალურ სტანდარტებს.[26]

რეგიონულ დონეზე ევროპა მარეგულირებელი ცვლილებების სათავეში იდგა. ევროპის საბჭოს 108-ე კონვენცია (1981 წელი, გადაიხედა 2018 წელს)

[24] *OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013 Revision. OECD, Explanatory memoranda of the OECD Privacy Guidelines, 2022, PP 11-12.*

[25] International Covenant on Civil and Political Rights (Adopted by General Assembly resolution 2200 (XXI) of 16 December 1966) (ICCPR), Art. 17: Right to privacy.

[26] UN General Assembly Resolutions on the right to privacy in the digital age, e.g., A/RES/68/167 (2013).

მონაცემთა დაცვის შესახებ ერთადერთი სავალდებულო საერთაშორისო ხელშეკრულებაა და ცალსახად მოიცავს მონაცემთა ტრანსსასაზღვრო ნაკადებს, ამავდროულად მოითხოვს მხარეებისგან, უზრუნველყონ შესაბამისი დაცვის სტანდარტები ტრანსასაზღვრო გადაცემების შემთხვევაში[27]. ევროკავშირის ფარგლებში „მონაცემთა დაცვის ძირითადი რეგულაცია" ("GDPR", რეგულაცია (EU) 2016/679) უზრუნველყოფს მონაცემთა დამუშავების ყოვლისმომცველ ჩარჩოს და ადგენს მკაცრ პირობებს მონაცემთა საერთაშორისო გადაცემისთვის. აღსანიშნავია, რომ, ევროპის მიღმა, სხვა რეგიონულ ორგანიზაციებსაც აქვთ განვითარებული მარეგულირებელი ჩარჩოები.[28]

წინამდებარე ინსტრუმენტები ცხადყოფს, რომ მონაცემთა გაზიარება აღარ რეგულირდება მხოლოდ ეროვნულ დონეზე, არამედ სულ უფრო მეტად ინტეგრირდება საერთაშორისო, რეგიონული და საერთაშორისო ჩარჩოების რთულ ქსელში. ეს ნორმატიული არქიტექტურა არა მხოლოდ აყალიბებს ეროვნულ კანონმდებლობას, არამედ უზრუნველყოფს ძირითად პრინციპებს (კანონიერება, სამართლიანობა, ანგარიშვალდებულება, უსაფრთხოება და პროპორციულობა), რომლებიც სახელმწიფოებმა უნდა გაითვალისწინონ საკუთარი პოლიტიკის შემუშავებისას.

წინამდებარე საერთაშორისო სტანდარტები მოიცავს მონაცემთა დამუშავებისთვის პასუხისმგებელი პირებისთვის მოთხოვნების სერიას. უპირველესად, მათ მოეთხოვებათ შექმნან მონაცემთა მართვის თანმიმდევრული და ძლიერი ჩარჩოები, რათა უზრუნველყონ პერსონალური მონაცემების მართვა პასუხისმგებლიანი და ეთიკური მიდგომით.[29] ასეთ ჩარჩოებს თან უნდა ახლდეს ყოვლისმომცველი რისკების შეფასებები, რომლებიც მიზნად ისახავს მონაცემთა გაზიარებასთან დაკავშირებული პოტენციური რისკების იდენტიფიცირებას. ეს მოიცავს კონფიდენციალობისა და მონაცემთა დაცვაზე ზეგავლენის შეფასებებს (PIAs/DPIAs), რაც ხელს უწყობს კონფიდენციალობასთან დაკავშირებული პოტენციური რისკების შეფასებას და შესაბამისი შემარბილებელი ზომების იდენტიფიცირებას.[30]

---

[27] Council of Europe, Convention 108, 1981; modernized as Convention 108+, 2018, Arts. 5–7.

[28] აფრიკის კავშირის კიბერუსაფრთხოებისა და პერსონალური მონაცემების დაცვის შესახებ კონვენცია (მალაბოს კონვენცია, 2014) ადგენს წევრი სახელმწიფოების ვალდებულებებს მონაცემთა გაზიარებისა და გადაცემის შესახებ, ხოლო აზია-წყნარი ოკეანის რეგიონში APEC-ის ტრანსასაზღვრო კონფიდენციალობის წესების (CBPR) სისტემა ადგენს ნებაყოფლობით, აღსრულებად მექანიზმს მონაწილე ეკონომიკებს შორის სანდო მონაცემთა ნაკადის ხელშეწყობის მიზნით. ორმხრივ და პლურილტერალურ დონეზე რამდენიმე სავაჭრო შეთანხმება, როგორებიცაა ტრანს-წყნარი ოკეანის პარტნიორობის ყოვლისმომცველი და პროგრესული შეთანხმება (CPTPP) და USMCA (ამერიკის შეერთებული შტატები-მექსიკა-კანადის შეთანხმება), მოიცავს დებულებებს ტრანსასაზღვრო მონაცემთა ნაკადების შესახებ, რომლებიც ირიბად არეგულირებენ მონაცემთა გაზიარებას გაუმართლებელი შეზღუდვების აკრძალვით და ამავდროულად პერსონალური ინფორმაციის დაცვის მოთხოვნით.

[29] Convention 108+ (Art. 10) explicitly requires controllers to adopt appropriate safeguards, while the GDPR (Art. 24) imposes the principle of accountability, obliging controllers to demonstrate compliance.

[30] როგორც 108-ე კონვენცია (მუხლი 10(3)), ასევე GDPR (მუხლი 35) ავალდებულებს მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) გამოყენებას იმ შემთხვევებში, როდესაც დამუშავება, სავარაუდოდ, დარღვევის მაღალ რისკებს შეუქმნის ინდივიდების უფლებებსა და თავისუფლებებს. ეკონომიკური

მონაცემთა დამუშავებისთვის პასუხისმგებელი პირები ასევე ვალდებულნი არიან, მიიღონ მონაცემთა შენახვისა და განადგურების მკაფიო პოლიტიკა და პროცედურები, რათა უზრუნველყონ, რომ პერსონალური მონაცემები არ შეინახოს საჭიროზე მეტხანს და უსაფრთხოდ განადგურდეს. ანგარიშვალდებულების უზრუნველსაყოფად მათ უნდა ჩაატარონ მონაცემთა გაზიარების პროცესის რეგულარული შემოწმება და მიმოხილვა, რათა დაადასტურონ სამართლებრივ და მარეგულირებელ მოთხოვნებთან შესაბამისობა.

კიდევ ერთი მნიშვნელოვანი ელემენტია გამჭვირვალობა ფიზიკური პირების მიმართ, რაც გულისხმობს მონაცემთა სუბიექტების ინფორმირებას მათი პერსონალური მონაცემების გაზიარების შესახებ და მათთვის ინფორმაციის მიწოდებას უფლებების შესახებ, მათ შორის მონაცემებზე წვდომისა და მათი შესწორების უფლების შესახებ. ამავდროულად, მონაცემთა სიზუსტე და ხარისხი უნდა გაუმჯობესდეს ისეთი მექანიზმების მეშვეობით, როგორებიცაა მონაცემთა ვალიდაცია ან, საჭიროების შემთხვევაში, ასაკის დადასტურება.

გარდა ამისა, მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა ჩაატარონ აუცილებლობისა და პროპორციულობის ტესტები, რათა მინიმუმამდე დაიყვანონ სხვა ორგანიზაციებისთვის გადაცემული პერსონალური მონაცემების მოცულობა, რითაც შემცირდება დარღვევებისა და კონფიდენციალობის დარღვევის რისკი. ასევე, მათ უნდა დაადგინონ პროცედურები მონაცემთა უსაფრთხოების დარღვევების პრევენციისა და მათზე რეაგირების მიზნით დაზარალებული პირების დასაცავად, შემამსუბუქებელი ზომების გატარების პარალელურად.

არანაკლებ მნიშვნელოვანია მონაცემთა გაზიარების შესახებ მრავალმხრივი შეთანხმებების მიღება, რომლებიც მკაფიოდ განსაზღვრავს გაზიარების მიზანს, ფარგლებს და პირობებს, მათ შორის, გაზიარებული მონაცემების გამოყენების შეზღუდვებს, კონფიდენციალობის ვალდებულებებსა და არაავტორიზებული ხელახალი იდენტიფიცირების შესახებ აკრძალვებს. ეს შეთანხმებები უნდა იყოს მხარდაჭერილი სასწავლო პროგრამებით, რომლებიც ხელს შეუწყობს მონაცემთა გაზიარებასთან დაკავშირებული რისკების შესახებ ცნობიერების ამაღლებას და საჭირო ცოდნისა და უნარების განვითარებას.

დაბოლოს, დამუშავებისთვის პასუხისმგებელი პირებისგან მოსალოდნელია მონაცემთა პორტირების მექანიზმების დანერგვა, რომლებიც მონაცემთა სუბიექტებს საშუალებას მისცემს, მიიღონ თავიანთი პერსონალური მონაცემები სტრუქტურირებული ფორმით, ან პირდაპირ გადასცენ ეს მონაცემები დამუშავებისთვის პასუხისმგებელ სხვა პირს.

თანამშრომლობისა და განვითარების ორგანიზაციის სახელმძღვანელო პრინციპები ანალოგიურად ხაზს უსვამს პერსონალური მონაცემების ნაკადების მიმართ რისკზე დაფუძნებულ მიდგომებს.

4. მონაცემთა დაცვის რისკები მონაცემთა გაზიარებისას

თანამშრომლობის პოტენციური მნიშვნელობა ყოველთვის ყურადღებით უნდა შეფასდეს კონფიდენციალობის, მონაცემთა უსაფრთხოებისა და განსაკუთრებული კატეგორიის მონაცემების კონტროლის კუთხით. მონაცემთა გაზიარების კონცეფციასთან დაკავშირებულია რამდენიმე რისკი, რომელთა გათვალისწინებაც აუცილებელია პერსონალური მონაცემების დაცვის კონტექსტში არა მხოლოდ ინდივიდების უფლებების დასაცავად, არამედ ორგანიზაციებს შორის მდგრადი თანამშრომლობისთვის აუცილებელი ნდობის უზრუნველსაყოფად.[31]

ერთ-ერთი მთავარი გამოწვევა მონაცემთა სუბიექტებისა და საზოგადოების მხრიდან არასაკმარისი ცნობიერებაა იმის შესახებ, თუ რა ხდება მონაცემთა დამუშავებისას, რა არის მიზანი, სამართლებრივი საფუძველი, ბიზნეს მოდელი (რომელი გამოყენების შემთხვევებია გათვალისწინებული „მონაცემთა სივრცის"/„მონაცემთა გაზიარებისთვის", მათ შორის, საზოგადოებაზე ეკონომიკური ინკლუზიურობისა და ურთიერთგაზიარების ხელშეწყობის თვალსაზრისით[32]).

ცნობიერების ნაკლებობა, რომელიც ძირითადად გამჭვირვალობის პრობლემატიკით არის გამოწვეული, ეწინააღმდეგება სამართლიანობისა და კანონიერების პრინციპებს საერთაშორისო და რეგიონულ დონეზე[33], რომლებიც მოითხოვს, რომ მონაცემთა სუბიექტები მკაფიოდ იყვნენ ინფორმირებულნი მათთან დაკავშირებული დამუშავების პროცესის შესახებ. ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის სახელმძღვანელო პრინციპები კონფიდენციალობის დაცვისა და პერსონალური მონაცემების ტრანსსასაზღვრო ნაკადების შესახებ ასევე ითვალისწინებს გამჭვირვალობას, როგორც მონაცემთა ტრანსსასაზღვრო ნაკადების ძირითად პრინციპებს[34].

კიდევ ერთი გამოწვევა მონაცემთა დამუშავების პროცესში სამართლიანობის ნაკლებობაა, რაც ხშირად არასაკმარისი ტექნოლოგიური ან ორგანიზაციული დაცვის შედეგია. შესაბამისი მექანიზმების გარეშე პირები შეიძლება დაექვემდებარონ არაგამჭვირვალე მონაცემთა დამუშავების პრაქტიკას, რაც ხელს უშლის მათ კონტროლის განხორციელებაში. ამასთან მჭიდრო კავშირშია მიზნის შეზღუდვის არარსებობა. მონაცემთა გაზიარების კონტექსტში დამუშავების ფარგლები ბუნდოვნად არის განსაზღვრული, აქტივობები განპირობებულია შემთხვევითი აღმოჩენით და არა სტრუქტურირებული, ჰიპოთეზებზე დაფუძნებული ან სამეცნიერო მიდგომით.

[31] *OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2019* <https://doi.org/10.1787/276aaca8-en> [20.09.2025].

[32] იხ.: for instance *Assessment of current and future impact of Big Data on Financial Services*, 2016, available at <https://finance.ec.europa.eu/system/files/2016-12/1606-big-data-on-financial-services_en_0.pdf> [06.09.2025].

[33] მაგალითად: 108-ე კონვენციის 5(4)(a) მუხლი და, რეგიონულ დონეზე, მონაცემთა დაცვის ზოგადი რეგულაციის 2016/679 (GDPR) 5(1)(a) მუხლი.

[34] *OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013, Part Two: Basic Principles of National Application.*

ეს პრაქტიკა ეწინააღმდეგება მიზნის შეზღუდვის პრინციპს, რომლისთვისაც მონაცემები შეიძლება დამუშავდეს მხოლოდ განსაზღვრული, მკაფიო და ლეგიტიმური მიზნებისთვის და არ უნდა დამუშავდეს შემდგომში ისე, რომ არ შეესაბამებოდეს ამ მიზნებს[35].

მაშინაც კი, როდესაც ფიზიკური პირები და ორგანიზაციები ცალსახად თანხმდებიან მონაცემთა გაზიარებისა და ხელახალი გამოყენების კონკრეტულ პირობებზე, მათ შორის იმ მიზნებზე, რომელთათვისაც ლეგიტიმურად შეიძლება მონაცემების ხელახალი გამოყენება, კვლავ არსებობს მნიშვნელოვანი რისკი, რომ მესამე მხარეებმა, შეგნებულად ან უნებლიეთ, შეთანხმებული ჩარჩოდან გადახვევის გზით, მონაცემები ხელახლა გამოიყენონ. ფართოდ განხილული “Cambridge Analytica”-ს საქმე ამ რისკის ნათელი მაგალითია: “Facebook”-ის მომხმარებლების პერსონალური მონაცემები, რომლებიც თავდაპირველად შეგროვდა კვლევისთვის მიზნებისთვის, ხოლო შემდგომში გამოყენებული იქნა პოლიტიკური კამპანიისთვის. აღნიშნული განხორციელდა “Facebook”-ის მიერ მონაცემების „ნებისმიერი სარეკლამო ქსელისთვის, მონაცემთა ბროკერისთვის ან სხვა სარეკლამო ან მონეტიზაციასთან დაკავშირებული სერვისისთვის“, გაყიდვის ან გადაცემის ცალსახა აკრძალვის მიუხედავად.[36]

“Cambridge Analytica”-ს ინციდენტი მხოლოდ ერთ-ერთია იმ მრავალ შემთხვევას შორის, როდესაც მონაცემების ხელახლა იქნა გამოყენებული. მნიშვნელოვანია, რომ ასეთი დარღვევები ყოველთვის არ არის ბოროტი განზრახვის შედეგი. მონაცემთა გაზიარება გულისხმობს მონაცემების ამოღებას ერთი კონტექსტიდან და მათ მეორეში გადატანას. როგორც ეს შეიძლება გავიგოთ ნისენბაუმის კონფიდენციალობის თეორიის[37], როგორც კონტექსტური მთლიანობის მითითებით. კონტექსტში ნებისმიერი ცვლილება ართულებს არსებული უფლებებისა და ვალდებულებების შენარჩუნების უზრუნველყოფას. მაგალითად, მონაცემთა თავდაპირველი გამოყენებისას ნაგულისხმევი კონფიდენციალობის მოლოდინები შესაძლოა, აღარ გავრცელდეს შემდგომ ხელახალ გამოყენებაზე. მონაცემთა ხელახალ გამოყენებასთან დაკავშირებული რისკები დამოკიდებულია იმ კონტექსტზე, რომელშიც შეგროვდა მონაცემები და იმ ახალ კონტექსტზე, რომელშიც ისინი იქნება გამოყენებული. ამიტომ მონაცემთა გაზიარება და მისი გამოყენება დამატებითი მიზნებისთვის უნდა იყოს ინტეგრირებული გამჭვირვალობის, ანგარიშვალდებულებისა და დაცვის მყარ ჩარჩოში.

ასევე, რისკები ვრცელდება მონაცემთა დუბლირებასა და გავრცელებაზე კანონიერი ან ლეგიტიმური მიზნების მიღმა, რამაც შეიძლება დაარღვიოს

[35] ეს პრინციპი, მაგალითად, გათვალისწინებულია ეკონომიკური თანამშრომლობისა და განვითარების ორგანიზაციის სახელმძღვანელო პრინციპებში, 108-ე კონვენციის 5(4)(a) მუხლსა და GDPR-ის 5(1)(b) მუხლში.

[36] *Granville K.,* Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens, The New York Times, 2018; *Isaak J. and Hanna M.*, User data privacy: Facebook, Cambridge Analytica, and Privacy Protection, Computer, Vol. 51/8, pp. 56-59, 2018.

[37] *Nissenbaum H*., Privacy as Contextual Integrity, Washington Law Review, Vol. June, 2004.

როგორც შენახვის შეზღუდვის, ასევე მიზნის შეზღუდვის პრინციპები. გარდა ამისა, ხშირად ხდება მონაცემების არაეფექტიანი ან არასაჭირო გამოყენება. ეს ფენომენი, რომელიც შეიძლება შეფასდეს, როგორც „მონაცემთა ფლანგვა", არა მხოლოდ იწვევს რესურსების არაეფექტურ განაწილებას, არამედ არღვევს მონაცემთა მინიმიზაციის პრინციპს[38] და მჭიდროდ უკავშირდება მონაცემთა უსაფრთხოების გაზრდილ რისკებს.

ფაქტობრივად, უსაფრთხოება კიდევ ერთი საზრუნავია. მასშტაბური მონაცემთა გაზიარება ხშირად გულისხმობს მონაცემების გადაცემას მრავალ ქსელსა და სისტემას შორის, რომელთაგან თითოეულს სხვადასხვა ორგანიზაცია მართავს განსხვავებული პოლიტიკით. აღნიშნული ზრდის უსაფრთხოების ინციდენტებისა და მონაცემთა დარღვევის ალბათობას, რაც პოტენციურად საფრთხეს უქმნის კონფიდენციალობას, მთლიანობას და ხელმისაწვდომობას.[39] გარდა ამისა, უკანონო წვდომა ან გამჟღავნება გაზრდილ რისკს წარმოადგენს, რადგან მონაცემები იცვლება მრავალ ორგანიზაციასა და სისტემას შორის და ამ შემთხვევებში, იურისდიქციებსა თუ სექტორებს შორის თანმიმდევრული მმართველობითი ჩარჩოების შექმნის სირთულემ შეიძლება კიდევ უფრო შელახოს დამუშავების კანონიერება.[40]

მონაცემთა ხარისხის შემცირება ("reduction in data quality") არანაკლებ პრობლემურია, რადგან შეიძლება გამოიწვიოს არასწორი გადაწყვეტილებები და დისკრიმინაციული შედეგები. მონაცემთა წყაროების ჰეტეროგენულობამ, თუ სათანადოდ არ იქნება მოგვარებული, შეიძლება გამოიწვიოს შეუსაბამობები და შეცდომები, რომლებითაც დაირღვევა მონაცემთა სიზუსტის პრინციპი.[41] ამ უზუსტობამ ასევე შეიძლება გავლენა იქონიოს სამართლიანობაზე, განსაკუთრებით მაშინ, როდესაც საქმე ეხება ავტომატიზებული გადაწყვეტილების მიღებას, რაც პოტენციურად გაამძაფრებს მიკერძოებას და დისკრიმინაციას.

ანგარიშვალდებულების პრინციპი, რომელიც მოითხოვს პროაქტიულ ქცევას და პერსონალური მონაცემების დაცვის უზრუნველსაყოფად კონკრეტული ზომების დემონსტრირებას, ასევე უფრო რთული ხდება მონაცემთა გაზიარების კონტექსტში განსახორციელებლად. როდესაც დამუშავების რთულ ოპერაციებში მრავალი ორგანიზაცია მონაწილეობს, ხშირად გაურკვეველია, თუ როგორ ნაწილდება პასუხისმგებლობა მონაცემთა დამუშავებისთვის პასუხისმგებელ და უფლებამოსილ პირებს შორის.[42] აღნიშნული გაურკვევლობა ართულებს რეგულაციების აღსრულებას და ასუსტებს ანგარიშვალდებულების მარეგულირებელი ჩარჩოების ეფექტიანობას.[43]

[38] Convention 108, Art. 5(4)(c) and GDPR, Art. 5(1)(c).

[39] OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2019.

[40] Convention 108+, Art. 5(4)(a); GDPR, Art. 5(1)(a).

[41] Article 5(4)(d) Convention 108 ; Article 5(1)(d) GDPR.

[42] *European Data Protection Board (EDPB), Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 2.0, 7 July 2021.*

[43] Convention 108+, Art. 10; GDPR, Arts. 24–28.

საბოლოოდ, მონაცემთა გაზიარება მოიაზრებს მონაცემთა დაცვის ყველა პრინციპს. თუ აღნიშნული სწორად განხორციელდება და არა მხოლოდ ფორმალურად, მონაცემთა დაცვის პრინციპები დაბრკოლებას კი არ წარმოადგენს, არამედ პასუხისმგებლიანი გაზიარების ხელშემწყობ ფაქტორს. აუცილებლობისა და პროპორციულობის პრინციპი უზრუნველყოფს სამართლებრივ საფუძველს ინოვაციისა და ფუნდამენტური უფლებების შეთავსებისთვის. აღნიშნული მოითხოვს, ერთი მხრივ, მონაცემთა გაზიარების ეფექტიანობის დაბალანსებას დასახული მიზნის მისაღწევად, ხოლო, მეორე მხრივ, ჩარევას კონფიდენციალობასა და მონაცემთა დაცვაში.[44]

კონკრეტული რისკის შემცირების ზომა, როგორიცაა კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების დანერგვა, მიზნის მკაცრი შეზღუდვა ან მყარი სახელშეკრულებო ჩარჩოები, ამ ბალანსის ნაწილია. საერთაშორისო და რეგიონულ მონაცემთა დაცვის სტანდარტებთან შესაბამისობის უზრუნველყოფით, მონაცემთა გაზიარებას შეუძლია ხელი შეუწყოს ინოვაციის დანერგვას და ამავდროულად დაამყაროს ნდობა, რაც აუცილებელია თანამშრომლობისთვის, ღირებულების შექმნისა და საზოგადოებრივი სარგებლისთვის. ამ თვალსაზრისით, მონაცემთა დაცვის კანონმდებლობა მოქმედებს არა როგორც დაბრკოლება, არამედ როგორც მონაცემთა გაზიარების ხელშემწყობი ფაქტორი, რომელიც გვთავაზობს პრინციპულ და პროგნოზირებად ჩარჩოს ტექნოლოგიური პროგრესის პირთა ძირითად უფლებებთან შეთავსებისთვის.

5. კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები, როგორც სამართლებრივი და ტექნიკური ინსტრუმენტები

კონსოლიდირებულ ტექნოლოგიებს, ე.წ. კონფიდენციალობის გამაძლიერებელ ტექნოლოგიებს (“PETs”), გააჩნია პოტენციალი, ფუნდამენტურად შეცვალოს მონაცემთა გაზიარების დინამიკა რისკების აღმოფხვრისა თუ შემცირების საშუალებით. აღნიშნული რისკები დაკავშირებულია მონაცემთა გაზიარებასთან. დღევანდელ რეალობაში უკვე შესაძლებელია ტექნოლოგიებთან მიმართებით არსებულ კითხვებზე პასუხის გაცემა.[45]

მონაცემთა გაზიარების პროცესში მხარეთა შორის თანამშრომლობის სტანდარტული ფორმა, როგორც წესი, მოიაზრებს მონაცემთა გაერთიანებას ერთ ნაკრებად, რომელიც შემდეგ ყველასთვის ხელმისაწვდომი ხდება. თუმცა

[44] ეს პრინციპი ნათლად არის ასახული ადამიანის უფლებათა ევროპულ კონვენციაში, რომი, 1950 წლის 4 აპრილი, მე-8(2) მუხლი (ECHR) და სამოქალაქო და პოლიტიკური უფლებების შესახებ საერთაშორისო კონვენციის მე-17 მუხლში და შემდგომში განხორციელდა ევროკავშირის სამართალში GDPR-ის დებულებების მეშვეობით.

[45] PETs-ის საკითხებთან დაკავშირებით იხ. *OECD-ის სახელმძღვანელო, სახელწოდებით: Emerging privacy-enhancing technologies: Current regulatory and policy approaches, OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, 2023* <https://doi.org/10.1787/bf121be4-en> [01.10.2025] and *Asrow K. and Samonas S.,* Privacy Enhancing Technologies: Categories, Use Cases and Considerations, Federal Reserve Bank of San Francisco, CA, 2021.

თანამედროვე ტექნოლოგიები მონაცემთა გაზიარების გამარტივებულ ფორმაზე გადასვლის საშუალებას იძლევა. თანამედროვე მიდგომების მეშვეობით, წინასწარი გამოთვლის და ლოგიკური ოპერაციების განხორციელების გზით, შესაძლებელია გასაზიარებელი მონაცემების მინიმიზაცია. ამავდროულად, წინასწარი მოქმედებების განხორციელების შედეგად შესაძლებელია მონაცემთა სათანადო დაცვის უზრუნველყოფა. ამდენად, კონფიდენციალობის გამაძლიერებელი ტექნოლოგიებით მონაცემთა დაცვა შესაძლებელია როგორც ტექნოლოგიებით სარგებლობის, ასევე ტექნოლოგიების გამოყენების შემდგომ ეტაპებზე.

კონფიდენციალობის შიდა სისტემური უზრუნველყოფისთვის კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები უკვე ხელმისაწვდომია. მათში მოიაზრება: კერძო ნაკრების მოდელი,[46] ჰომომორფული დაშიფვრა,[47] მრავალმხრივი გამოთვლა დაცული საშუალებებით[48] და მტკიცებულებები ცოდნის გარეშე.[49] აღნიშნულის სანაცვლოდ, სისტემის მიღმა გამჟღავნებული მონაცემების დაცვა შესაძლებელია კონფიდენციალობის გამაძლიერებელი ორი დამატებითი ზომით: რანდომიზაცია[50] და განზოგადება[51].

კონფიდენციალობის გამაძლიერებელმა ტექნოლოგიებმა შეიძლება მნიშვნელოვნად შეამციროს იმ პირთა რაოდენობა, რომლებსაც წვდომა აქვთ პერსონალურ ინფორმაციაზე. კონკრეტულად, მხარეს, რომელიც პერსონალურ მონაცემებთან მიმართებით ახორციელებს რიცხობრივ თუ ლოგიკურ მოქმედებებს, არ შეუძლია: ღია, დაუშიფრავი სახით მონაცემების დანახვა; მონაცემთა დამუშავების პროცესში წვდომა ჰქონდეს შუალედურ მნიშვნელობებზე ან სტატისტიკურ შედეგებზე (გარდა იმ შემთხვევისა, თუ მონაცემი სპეციალურად არის განკუთვნილი გასაზიარებლად); გამოიყენოს ისეთი ტექნიკა, როგორიცაა შეტევა სხვა საშუალებებით ("side-channel attacks"), რათა დამუშავების პროცესში გამოვლენილი ცვლილებების, მაგალითად,

[46] კერძო ნაკრების მოდელი ("PSI"): დაცული მრავალმხრივი კომპიუტერული კრიპტოტექნიკა, რომელიც ნებას რთავს ორ მხარეს, შეადარონ დაშიფრული ვერსიები აღნიშნული კერძო ნაკრების გამოყენებით. ამ პროცესში, კერძო ნაკრების გარდა, მხარეები ერთმანეთს სხვა ინფორმაციას არ უზიარებენ.

[47] ჰომომორფული დაშიფვრა ("HE"): საშუალებას იძლევა, რომ გამოთვლები განხორციელდეს უშუალოდ დაშიფრულ მონაცემებზე, რომლის შედეგად მონაცემები დაშიფრული სახით გენერირდება და მათი გაშიფვრა შესაძლებელია მოგვიანებით, ძირითადი, თავდაპირველი მონაცემების გამჟღავნების გარეშე.

[48] მრავალმხრივი გამოთვლა დაცული მეთოდებით ("SMPC") საშუალებას აძლევს სხვადასხვა მხარეს, რომ ერთობლივად გამოთვალონ მონაცემები კონფიდენციალური სახით.

[49] მტკიცებულებები ცოდნის გარეშე (ZKPs) წარმოადგენს პროტოკოლს, რომლის შესაბამისად ერთ მხარეს შეუძლია მეორე მხარეს დაუსაბუთოს, რომ კონკრეტული მტკიცება არის სწორი (მაგალითად, ისინი აკმაყოფილებს განსაზღვრულ პირობებს), სხვა დამატებითი ინფორმაციის გაზიარების გარეშე.

[50] რანდომიზაციის საშუალებით შესაძლებელია ინდივიდუალური ჩანაწერების დაფარვა, თუმცა, ამავდროულად, მონაცემთა ანალიზი.

[51] მონაცემთა განზოგადება წარმოადგენს მონაცემების შემცირების ან შეჯამების პროცესს, რომლის საშუალებითაც არსებული მონაცემები დაცულია, თუმცა ზოგადი დასკვნების გამოტანა შესაძლებელია.

მოთხოვნის შესრულების დროის ან ენერგომოხმარებისას, ანალიზით მოიპოვოს მონაცემები.

ქსელური კონფიდენციალობის ტექნიკა, როგორც წესი, გულისხმობს მონაცემთა ტრანსფორმაციას და გამოთვლებს დაშიფვრის მექანიზმის მეშვეობით. მაგალითად, დაცული მრავალმხრივი გამოთვლის ("SMPC") ტექნიკის გამოყენებისას მონაცემები იყოფა მრავალ კომპონენტად, რომლებიც შემდეგ ეტაპზე გამოთვლების შესასრულებლად ერთიანდება.[52]

კონფიდენციალობის დაცვის თვალსაზრისით ერთ-ერთ მაგალითად შეიძლება იქნეს მოყვანილი სავაჭრო მონაცემების დამუშავება ტრანსსასაზღვრო კონტექსტში. დაცული მრავალმხრივი გამოთვლის ტექნიკის გამოყენებით შესაძლებელი ხდება იმპორტის მონაცემების შედარება ექსპორტის მონაცემებთან. ამ გზით ორივე მხარეს შეუძლია შესაბამისობის თუ ხარვეზების გამოვლენა სავაჭრო მონაცემების გამჟღავნების გარეშე. აღნიშნული საშუალებით მხარეთა შორის ხორციელდება მნიშვნელოვანი მონაცემების მიმოცვლა განსაკუთრებული კატეგორიის მონაცემების გამჟღავნების გარეშე. სისტემური კონფიდენციალობის ტექნიკა, როგორიცაა დაცული მრავალმხრივი გამოთვლა, ფსევდონიმიზაციის საუკეთესო ფორმად შეიძლება იქნეს მიჩნეული, როდესაც ტექნოლოგიაში ასახული მონაცემები პირადი ხასიათისაა.[53]

კონფიდენციალობის სხვა ტექნიკა შეიძლება გულისხმობდეს იმგვარ სანდო გარემოს შექმნას, როდესაც გამოთვლები უსაფრთხო ტექნოლოგიურ სისტემაში ხორციელდება. აღნიშნული ამცირებს მონაცემთა დამუშავების ოპერაციების შეცვლის რისკებს.

ტექნოლოგიებით სარგებლობის შემდგომ ეტაპზე არსებული კონფიდენციალობის ტექნიკების გამოყენებით, რომლებიც მოიცავს ხმის დამატებას ან მონაცემების კატეგორიებად დაჯგუფებას, შესაძლებელია პერსონალური მონაცემების სათანადო დაცვა. აღსანიშნავია, რომ ხმის დონის ან ინტერვალების ამპლიტუდის განსაზღვრით, მონაცემები შეიძლება დარჩეს ზუსტი. აღნიშნულის საპირისპიროდ, ხელახალი იდენტიფიკაციის მცდელობები შეიძლება იყოს არაგონივრული, მაგალითად, "GDPR"-ის პრეამბულის 26-ე პუნქტით[54] გათვალისწინებული იდენტიფიცირებადობის

[52] დაცული მრავალმხრივი გამოთვლის მიმართულებით საინტერესოა JOCONDE-ის (Joint On-demand COmputation with No Data Exchange) ინიციატივა, რომელიც ევროსტატმა 2024 წლის აპრილში წამოიწყო PET-ების ევროპულ სტატისტიკურ სისტემაში დანერგვის ხელშეწყობის მიზნით, <https://cros.ec.europa.eu/joconde> [05.09.2025].

[53] *ENISA Data Pseudonymisation: Advanced Techniques & Use Cases Technical analysis of cybersecurity measures in data protection and privacy - January 2021.*

[54] "GDPR"-ის პრეამბულის 26-ე პუნქტი: „იმისათვის, რომ განისაზღვროს, შესაძლებელია თუ არა ფიზიკური პირის იდენტიფიცირება, მხედველობაში უნდა იქნეს მიღებული ყველა გონივრული შესაძლო საშუალება, მაგალითად, ფიზიკური პირის ამოცნობა, რაც შესაძლოა გამოყენებულ იქნეს დამუშავებისთვის პასუხისმგებელი პირის ან სხვა პირის მიერ პირის პირდაპირ ან არაპირდაპირ იდენტიფიცირების მიზნით. იმის დასადგენად, მოხდება თუ არა გონივრული საშუალებების გამოყენება ფიზიკური პირების იდენტიფიცირების მიზნით, მხედველობაში უნდა იქნეს მიღებული

კრიტერიუმის შესაბამისად. სამართლებრივი თვალსაზრისით, ტექნოლოგიით სარგებლობის დასრულების შემდგომ ეტაპზე გამოყენებული კონფიდენციალობის ტექნიკა შეიძლება მიჩნეულ იქნეს ანონიმიზაციად.

კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები ამცირებს რისკს, რომ ფიზიკურმა პირებმა მონაცემების დამუშავებისას შეძლონ პერსონალური ინფორმაციის მოპოვება. აღნიშნული შედეგი დგება იმის მიუხედავად, აკმაყოფილებს თუ არა განხორციელებული გამოთვლები ან ლოგიკური ოპერაციები სისტემური კონფიდენციალობის პირობებს. "PET"-ის გამოყენება, რომელიც უზრუნველყოფს შედეგების კონფიდენციალობას, სასარგებლოა როგორც ანონიმური სტატისტიკის საჯაროდ ხელმისაწვდომობისთვის, ასევე ანალიზის შედეგების გასაზიარებლად.

ასევე, კონფიდენციალობის გამაძლიერებელი ამგვარი ტექნოლოგიები მნიშვნელოვან როლს ასრულებს შენახვის ვადის შეზღუდვისა და მონაცემთა მინიმიზაციის პრინციპების დაცვის თვალსაზრისით.[55]

კონფიდენციალობის დაცვის კონტექსტში საინტერესოა სტატისტიკის ეროვნული სამსახურის მიდგომა, რომელიც მონაცემებს მათ გამოქვეყნებამდე ამატებს კალიბრირებულ ხმას. აღნიშნული ტექნიკის გამოყენება ნათლად წარმოაჩენს ანონიმიზაციის ეფექტიანობას.[56]

ტექნოლოგიების როგორც გამოყენების, ასევე გამოყენების შემდგომ ეტაპებზე დასახელებული სტანდარტების გათვალისწინება მნიშვნელოვნად უზრუნველყოფს გაზიარებული პერსონალური მონაცემების კონფიდენციალობას. დადგენილი ტექნიკების შემუშავებით ორგანიზაციებს შეუძლიათ მონაცემები სხვადასხვა სახით დაამუშაონ, რა პროცესშიც სათანადოდ იქნება დაცული პირადი ინფორმაცია. აგრეთვე, უზრუნველყოფილი იქნება მონაცემების სანდო, სამართლებრივი და ეკონომიკური პერსპექტივიდან მომგებიანი გაზიარება, მათ შორის, საერთაშორისო გადაცემის კონტექსტში, რაც სხვა შემთხვევაში შეუძლებელი იქნებოდა.

გარდა აღნიშნულისა, არსებობს კონფიდენციალობის გამაძლიერებელი სხვა ტექნოლოგიები, რომლებიც განსხვავდება განხილული ტექნოლოგიებისგან. ისინი გულისხმობს მონაცემების უსაფრთხო დამუშავებას და ამცირებს პერსონალური მონაცემების რაოდენობას, რომლებზეც წვდომა აქვთ სხვა მხარეებს. აღნიშნული უზრუნველყოფს მონაცემთა დამუშავების პრინციპების დაცვას, მაგალითად, როგორებიცაა

ყველა ობიექტური გარემოება, როგორებიცაა იდენტიფიცირებისათვის საჭირო ხარჯები და დრო, მონაცემთა დამუშავებისას ხელმისაწვდომი ტექნოლოგიები და ტექნოლოგიის განვითარება.

[55] Information Commissioner's Office, Privacy-enhancing technologies (PETs), June 2023, <https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf> [05.09.2025].

[56] იხ., Harvard University (n.d.), Differential Privacy, Harvard University Privacy Tools Project, <https://privacytools.seas.harvard.edu/differential-privacy> [02.10.2025].

დეცენტრალიზებული (ფედერაციული) სწავლება[57] და სინთეზური მონაცემების გამოყენება.[58]

6. რეკომენდაციები

სტატიის წინა თავებში ხაზი გაესვა მონაცემთა გაზიარებასთან დაკავშირებულ პოტენციალსა და რისკებს: როდესაც ორი ან მეტი ორგანიზაცია ერთობლივად მონაწილეობენ მონაცემთა გაზიარებაში, ისინი კოლექტიურად ქმნიან უფრო ფართო და მონაცემთა მრავალფეროვან ეკოსისტემას, რომელსაც პოტენციურად დიდი სარგებელი მოაქვს საზოგადოებისთვის. აღნიშნული წარმოშობს რისკებს კონფიდენციალობის დაცვის თვალსაზრისით. ამგვარ გარემოში გამოყენებული მიდგომების საშუალებით შეიძლება გამოიკვეთოს ახალი ტენდენციები. თუმცა ტრადიციული მიდგომების გამოყენება, როგორებიცაა ნედლი მონაცემთა ნაკრებების ორმხრივი გაცვლა ან საერთო საცავში განთავსება, რომელიც ხელმისაწვდომია ყველა მხარისთვის, არ არის მიზანშეწონილი განსაკუთრებით იმ კონტექსტში, როდესაც მონაწილეები დეცენტრალიზებულნი არიან და ხორციელდება მონაცემთა ფართომასშტაბიანი მიმოცვლა.[59]

აღნიშნულის ნაცვლად, მრავალმხრივი მიდგომა, რომელიც ეფუძნება კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების დანერგვას, შეიძლება იყოს უფრო ხელსაყრელი ვარიანტი გრძელვადიან პერსპექტივაში. “PeTs”-ის გამოყენებით, დაინტერესებულ მხარეებს შეუძლიათ, შექმნან სანდო გარემო, რომელიც ორიენტირებული იქნება მონაცემთა დაცვაზე და, ამავდროულად, უზრუნველყოფს მონაცემთა დაცვის დადგენილ პრინციპებთან შესაბამისობას.[60]

მონაცემთა დამუშავებისთვის პასუხისმგებელ პირებზე დაკისრებული ორგანიზაციული ვალდებულებების, მონაცემთა გაზიარებისთვის დამახასიათებელი რისკებისა და კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების დადებითი მხარეების გათვალისწინებით, მოცემული თავი ორიენტირებულია ტექნოლოგიების მართვის პრაქტიკულ ასპექტებზე. კერძოდ, ასახულია რეკომენდაციები, რომელთა მიზანია დაინტერესებული მხარეებისთვის სათანადო ინფორმაციის მიწოდება კონფიდენციალობის დაცვის უზრუნველსაყოფად.

---

[57] *Konečnỳ J., McMahan B., Ramage D..* Federated optimization: Distributed optimization beyond the datacentre, arXiv preprint arXiv:1511.03575, 2015.

[58] *El Emam K., Mosquera L., Hoptroff R.,* Practical Synthetic Data Generation: Balancing Privacy and the Broad Availability of Data, O'Reilly Media, 2020.

[59] *Tene O.and Polonetsky J.,* Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239, 2013.

[60] European Union Agency for Cybersecurity (ENISA), Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, December 2015. European Union Agency for Cybersecurity (ENISA), ENISA’s PETs Maturity Assessment Repository, November 2018.

6.1. რეკომენდაციები დამუშავებისთვის პასუხისმგებელი პირებისთვის

დამუშავებისთვის პასუხისმგებელმა პირებმა აუცილებელია, შეაფასონ მონაცემთა გაზიარების მიზანშეწონილობა, რომლის ფარგლებშიც უნდა დააიდენტიფიცირონ მხარეები, რომლებთანაც ხორციელდება მონაცემების გაზიარება. აღნიშნულის შესახებ სათანადოდ უნდა იყვნენ ინფორმირებულნი მონაცემთა სუბიექტები. მნიშვნელოვანია, რომ მონაცემთა სუბიექტებმა მონაცემთა დამუშავებამდე, მათ შორის, მონაცემთა შეგროვებასა და გაზიარებამდე, მარტივი და გასაგები ფორმით მიიღონ სრულყოფილი ინფორმაცია მათი პერსონალური მონაცემების დამუშავების შესახებ.[61] ამგვარი ინფორმაცია არ უნდა იყოს მიწოდებული რთული ფორმით, კერძოდ, უნდა იყოს მარტივი ენით და, ასევე, მონაცემთა სუბიექტს უნდა ჰქონდეს დამატებითი განმარტებების მიღების შესაძლებლობა. რაც მთავარია, ფიზიკურ პირებს ასევე უნდა მიეცეთ საშუალება, უარი თქვან მათი პერსონალური მონაცემების გაზიარებაზე.

პერსონალური მონაცემების გაზიარებასთან დაკავშირებული ნებისმიერი მოქმედება წარმოადგენს პერსონალური მონაცემების დამუშავებას და, შესაბამისად, წარმოშობს იურიდიულ ვალდებულებებს ორგანიზაციებისთვის. დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა მიიღონ ყველა საჭირო ზომა მონაცემთა დამუშავების პროცესების კანონმდებლობასთან შესაბამისობის უზრუნველსაყოფად ყველა იურისდიქციაში, რომლებსაც გადაეცემა მონაცემები. ამისათვის აუცილებელია მონაცემთა გაზიარებისთვის სათანადო სამართლებრივი საფუძვლის განსაზღვრა.[62]

კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები მნიშვნელოვან როლს ასრულებს მონაცემთა გაზიარების თანხმლები რისკების შემცირებაში, მათ შორის, განსაკუთრებული კატეგორიის მონაცემების დამუშავების კუთხით. იურისდიქციის სპეციფიკის გათვალისწინებით, "PETs" შესაძლოა დამხმარე საშუალება იყოს მონაცემთა გაზიარების კონტექსტში, რაც სხვა შემთხვევაში შეუძლებელი იქნებოდა. ასევე, "PETs" წარმოადგენს ბიზნესის წარმართვის ხელშემწყობ საშუალებას, რაც ორგანიზაციებს ეხმარება, ისარგებლონ მონაცემთა დამუშავების უპირატესობებით ისე, რომ შემცირებული იყოს კონფიდენციალობასთან დაკავშირებული რისკები.[63] სწორედ აღნიშნულის გათვალისწინებით, ტექნოლოგიები უნდა დაინერგოს განსაკუთრებული სიფრთხილით.

[61] *OECD, Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 2013.*

[62] Article 29 Data Protection Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller, WP 217, 9 April 2014.

[63] *McCarthy N., Fourniol F.,* The role of technology in governance: The example of Privacy Enhancing Technologies, Data & Policy, 2020.

6.2. რეკომენდაციები კანონმდებლებისა და მთავრობებისათვის

კანონმდებლებმა და მთავრობებმა უნდა შეიმუშაონ მონაცემთა გაზიარების შესახებ სამართლებრივი სისტემა, რომელიც გასცდება ორგანიზაციებს შორის მონაცემთა მარტივი გადაცემის ფარგლებს და, ამავდროულად, შეიზღუდება მონაცემთა გადამეტებული ცენტრალიზაცია.[64] ამგვარი მიდგომით, მხედველობაში უნდა იქნეს მიღებული მონაცემთა გაზიარების სოციალური და ეკონომიკური ფაქტორები, ისევე როგორც კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების პოტენციალი წარმოქმნილი რისკების შესამცირებლად.[65] "PETs"-მა, ბაზარზე შესვლის ბარიერების შემცირებითა და ახალი აქტორებისთვის ციფრული ბაზრების გახსნით შეიძლება ხელი შეუწყოს კონკურენციას.[66]

ამდენად, საკანონმდებლო ინიციატივები მიზნად უნდა ისახავდეს სამართლებრივი ჩარჩოების ჩამოყალიბებას, რომლებიც ხელს შეუწყობს "PETs"-ის დანერგვას და ორგანიზაციების წახალისებას კონფიდენციალობის დამცავი ტექნოლოგიების გამოყენების თვალსაზრისით. ამავდროულად, ინსტიტუტებმა მნიშვნელოვანი ინვესტიცია უნდა ჩადონ კვლევასა და განვითარებაში, რათა გაუმჯობესდეს "PETs"-ის გამოყენებადობა, მასშტაბურობა და ეფექტიანობა.[67] დამატებით, მთავრობებს შეუძლიათ მიზნობრივი სუბსიდიებით და სათანადო ნაბიჯების გადადგმით დააჩქარონ კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების დანერგვა.[68]

სტრატეგიულ დონეზე, სამთავრობო მონაცემთა პოლიტიკის შესაბამისად, პრიორიტეტული უნდა იყოს მონაცემთა დაცვის რეგულაციებთან შესაბამისობის უზრუნველყოფა და, ასევე, გამოთვლითი ინფრასტრუქტურის შექმნა აღსრულების სათანადო გარანტიებით. ამ თვალსაზრისით, კერძო და საჯარო სექტორების თანამშრომლობა და მარეგულირებელი "sandboxes"-ის შექმნა მნიშვნელოვან როლს ასრულებს დაინტერესებულ მხარეთა შორის ნდობის ჩამოყალიბებაში, ინოვაციების წახალისებისა და მონაცემთა დაცვის მაღალი სტანდარტების შენარჩუნებაში.[69]

---

[64] *Organisation for Economic Co-operation and Development (OECD), Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches, OECD Digital Economy Papers No. 351, 2023.*

[65] *Organisation for Economic Co-operation and Development (OECD), Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches, OECD Digital Economy Papers No. 351, 2023.*

[66] *Organisation for Economic Co-operation and Development (OECD), Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches, OECD Digital Economy Papers No. 351, 2023.*

[67] *OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2021.*

[68] European Commission, Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM(2022) 68 final.

[69] *Truby J. et al.*, "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications", European Journal of Risk Regulation, 2021 <www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/sandboxapproach-to-regulating-highrisk-artificial-intelligenceapplications/C350EADFB379465E7F4A95B973A4977D> [05.09.2025]

გარდა აღნიშნულისა, აუცილებელია მონაცემთა გაზიარების შესახებ ჰარმონიზებული საერთაშორისო მარეგულირებელი ჩარჩოს შემუშავება. ტრანსსასაზღვრო დონეზე, შემუშავებული ჩარჩოს საშუალებით, მონაცემთა გაცვლა გახდება მეტად მარტივი და განჭვრეტადი. აგრეთვე, შეიქმნება ძლიერი და ეფექტიანი გარანტიები ინდივიდთა უფლებების დასაცავად.

6.3. რეკომენდაციები ტექნოლოგიების გამოყენების შესახებ გადაწყვეტილების მიმღებ პირთათვის

ტექნოლოგიების გამოყენების შესახებ გადაწყვეტილების მიმღებმა პირებმა, გამჭვირვალობის უზრუნველსაყოფად, ხელი უნდა შეუწყონ დანერგილი ტექნოლოგიის ფუნქციონირების შესახებ ინფორმაციის გასაჯაროებას, რომლის საშუალებითაც მონაცემთა სუბიექტები მათი პერსონალური მონაცემების დამუშავების შესახებ სრულ ინფორმაციას მიიღებენ.[70] ამასთან, საზოგადოებას უნდა ჰქონდეს მათ შესახებ ალგორითმების შემოწმების შესაძლებლობა ხელმისაწვდომობის უზრუნველყოფით. აღნიშნული ხელს შეუწყობს ნდობის გაზრდასა და სამართლიანობის დაცვას.

ამასთან, უნდა შეიქმნას მხარეთა თანამშრომლობის ფორმატი, რომლის საშუალებითაც მონაცემების გაზიარება მოხდება მკაფიოდ განსაზღვრული წესების საფუძველზე, რა პროცესშიც მონაცემთა დაცვას მიენიჭება უპირატესობა.

თავის მხრივ, უპირატესობა უნდა მიენიჭოს სტანდარტიზებულ გადაწყვეტილებებს, რათა თავიდან იქნეს აცილებული სხვადასხვა იურისდიქციით გათვალისწინებული შეუსაბამობები მონაცემთა უკანონო დამუშავების პრევენციისთვის. გარდა სამართლებრივი ვალდებულებებისა, სექტორულ დონეზე უნდა შემუშავდეს ქცევის წესები მონაცემთა კონფიდენციალობის უზრუნველსაყოფად.[71]

6.4. რეკომენდაციები სამეცნიერო საზოგადოებისთვის

მკვლევრებმა და აკადემიურმა წრეებმა მიზანშეწონილია, ყურადღება გაამახვილონ კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების გამოყენებასთან დაკავშირებულ საკითხებზე. აღნიშნული ხელს შეუწყობს "PETs"-ის პრაქტიკულ გამოყენებას და მათი პოტენციური უპირატესობების დემონსტრირებას სხვადასხვა სფეროში.[72]

---

[70] *United Nations, Roadmap for Digital Cooperation, 2020*, available at: <www.un.org/en/content/digital-cooperation-roadmap> [20.09.2025].

[71] აგრეთვე, მისასალმებელი იქნება სახელმძღვანელო რეკომენდაციების შემუშავება, რომლებიც განკუთვნილი იქნება პროდუქტის მწარმოებლებისთვის, რა პროცესშიც ხორციელდება სენსიტიური ინფორმაციის გაზიარება, მაგალითად: *CDEI (n.d.), PETs Adoption Guide,* <https://cdeiuk.github.io/pets-adoption-guide/adoption-guide> [02.10.2025].

[72] *Wang Y. & Kobsa A.,* Privacy-Enhancing Technologies: Classification and Applications, in The Handbook of Privacy and Privacy-Enhancing Technologies, 2018.

გარდა აღნიშნულისა, სახელმძღვანელო რეკომენდაციების საშუალებით, დამუშავებისთვის პასუხისმგებელ პირებს უფრო მეტი ინფორმაცია უნდა მიეწოდოთ იმისათვის, რომ მაქსიმალურად შემცირდეს ტექნოლოგიების გამოყენებასთან დაკავშირებული რისკები.[73]

მკვლევრები და აკადემიური წრეების წარმომადგენლები აქტიურად უნდა ჩაერთონ ინდუსტრიის მიერ წარმოდგენილი გადაწყვეტილებების კრიტიკული შეფასების პროცესში. აღნიშნულის მიზანია მონაცემთა დაცვა დადგენილი სტანდარტების შესაბამისად.[74]

6.5. რეკომენდაციები მონაცემთა დაცვის საზედამხედველო ორგანოებისთვის

მონაცემთა დაცვის საზედამხედველო ორგანოებმა ხელი უნდა შეუწყონ კონფიდენციალობის გამაძლიერებელი ტექნოლოგიებით სარგებლობას და უზრუნველყონ მათი გამოყენება პრაქტიკაში.

ამასთან, საზედამხედველო ორგანოებმა უნდა დაიცვან კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების გამოყენების კონტექსტში ტაქსონომიისა და საზღვრების ბალანსი იმისათვის, რომ უკეთ იქნეს გააზრებული მონაცემთა გაზიარების და ამ პროცესში თანამშრომლობის მნიშვნელობები. აგრეთვე, უნდა მიიღონ ზომები ცნობიერების ამაღლების უზრუნველსაყოფად.[75]

მონაცემთა დაცვის საზედამხედველო ორგანოებმა უნდა წაახალისონ ორგანიზაციები, რომ ტექნოლოგიების გამოყენებისას დანერგონ მონაცემთა დაცვის სტანდარტები, რა პროცესშიც არსებითად მნიშვნელოვანია მონაცემთა დაცვის ექპერტებსა და ტექნოლოგიების სფეროში მომუშავე პირებს შორის თანამშრომლობა. აღნიშნული საშუალებით პასუხები გაეცემა კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების გამოყენებასთან დაკავშირებულ კითხვებს.[76]

[73] *Danezis G. et al.,* Privacy and Data Protection by Design – From Policy to Engineering, Computer Law & Security Review, Vol. 34, Issue 2, 2018.

[74] *van Blarkom J.J., van Eck B.M.A. & Verhaar P.,* Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents, College bescherming persoonsgegevens, 2003.

[75] *Jurcys P., Corrales Compagnucci M., Fenwick M.,* The Future of International Data Transfers: Managing Legal Risk with a User-Held Data Model, Computer Law & Security Review, Volume 46, September 2022, 105691.

[76] *Gregory Voss W.,* "Cross-Border Data Flows, the GDPR, and Data Governance," Washington International Law Journal, Vol. 29, No. 3, 2020.

7. დასკვნა

მონაცემთა გაზიარებით შესაძლებელია მნიშვნელოვანი ეკონომიკური ღირებულების შექმნა საზოგადოებისთვის ინოვაციების დანერგვის ხელშეწყობით და თანამშრომლობის წახალისებით; თუმცა აღნიშნული მოიცავს რისკებს, როგორებიცაა: მონაცემებზე არასანქცირებული წვდომა; მონაცემთა დამუშავების პროცესში გამჭვირვალობის არარსებობა; მონაცემთა სუბიექტების უფლებების განხორციელების თვალსაზრისით ბარიერების შექმნა (მონაცემთა სუბიექტმა შეიძლება არ იცოდეს, ვინ აკონტროლებს მის პერსონალურ ინფორმაციას); მონაცემთა დამუშავების მიზნის ცვლილება ("Purpose creep"). თითოეული ეს გამოწვევა უნდა მოგვარდეს ეფექტიანი რეაგირებით. ნებისმიერ შემთხვევაში პერსონალური მონაცემების, განსაკუთრებით სავალდებულო მონაცემების, შეგროვება და გამოყენება უნდა შეესაბამებოდეს აუცილებლობისა და პროპორციულობის პრინციპებს. კერძო სუბიექტების მიერ მონაცემთა დამუშავების შემთხვევაში სათანადო ყურადღება უნდა მიექცეს ყველა პოტენციურ რისკს, რომლებიც უკავშირდება ძირითადი უფლებებისა და თავისუფლებების დაცვას და დაინტერესებულ პირთა ინტერესებს. აღნიშნულ პროცესში მხედველობაში უნდა იქნეს მიღებული, მათ შორის, დისკრიმინაციის არარსებობა, პროფაილინგთან დაკავშირებული რისკები და მანიპულაციის რისკები.[77]

ზემოაღნიშნული გამოწვევები მოითხოვს როგორც ტექნიკური, ასევე სამართლებრივი ზომების მიღებას იმისათვის, რომ სათანადოდ შეფასდეს და შემცირდეს კონფიდენციალობასთან დაკავშირებული რისკები. თუკი ორგანიზაციები ამ ზომებს არ მიიღებენ, ისინი არა მხოლოდ დაარღვევენ მონაცემთა დაცვის შესახებ მოქმედ კანონმდებლობასა და პრინციპებს, არამედ საზოგადოებაში მათ მიმართ გაჩნდება უნდობლობის განცდა. უნდობლობამ შეიძლება მნიშვნელოვანი გავლენა იქონიოს ეკონომიკის ეფექტიანობაზე და, საბოლოოდ, ხელი შეუშალოს მონაცემთა მიმოცვლას.

გაზიარებული და დამუშავებული მონაცემების მოცულობის გათვალისწინებით, ორგანიზაციებმა ახალი პროდუქტის შექმნის ეტაპზევე პროაქტიულად უნდა დანერგონ მონაცემთა დაცვის სტანდარტები ("privacy by design"). თუკი ამგვარი სტანდარტები საწყის ეტაპზე არ დაინერგა, შემდგომი ზომების მიღება დამატებით ხარჯებთან შეიძლება იყოს დაკავშირებული. ასევე, წარმოიშობა უფრო მაღალი, არაპირდაპირი ხარჯები და ბუნდოვანებები მოქალაქეებისა და კომპანიებისთვის მონაცემთა გაზიარების კონტექსტში.

მონაცემთა დამუშავების ყველა პრინციპის დაცვით მონაცემთა გაზიარებამ შეიძლება დადებითი გავლენა იქონიოს არა მხოლოდ ბიზნეს სექტორზე, არამედ მთლიანად საზოგადოებაზე. აღნიშნული პრინციპები უნდა დაინერგოს ეფექტიანი, ტექნოლოგიებზე ორიენტირებული მიდგომებით, რათა მონაცემთა გაზიარებისას დაცულ იქნეს მონაცემთა დაცვის პრინციპები

[77] *Citron D.K. and Solove D.J.,* Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, 102 Boston University Law Review 793, 2022, <https://ssrn.com/abstract=3782222> [18.09.2025].

და მოთხოვნები. მონაცემთა გაზიარების ტრადიციული მეთოდები, კერძოდ, მონაცემთა ნაკრებების გაერთიანება შეუზღუდავი ფორმით, რომელზე წვდომაც ექნება ყველა ორგანიზაციას, ვერ უზრუნველყოფს აღნიშნული მოთხოვნების დაცულობას.

თანამედროვე რეალობაში კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები მნიშვნელოვნად აუმჯობესებს მონაცემთა გაზიარების პროცესს რისკების აღმოფხვრისა თუ შემცირების გზით. ტექნოლოგიური მიღწევებით, თანამშრომლობის პროცესში, ადრე არსებული გამოწვევები აღმოფხვრილია და უკვე შესაძლებელია მონაცემთა გაზიარების ყველა ეტაპზე პერსონალური მონაცემების დაცვა.

კონფიდენციალობის გამაძლიერებელი ტექნოლოგიები შეიძლება მიჩნეულ იქნეს პარტნიორობისა და თანამშრომლობის ხელშემწყობ ფაქტორად, რადგან აწესრიგებს მონაცემთა გაზიარებასთან დაკავშირებულ საკითხებს, რაც ადრე გამოწვევას წარმოადგენდა. უპირველესად, ორგანიზაციებმა უნდა უპასუხონ შემდეგ კითხვებს: რატომ აზიარებენ მონაცემებს; ვინ არის მონაცემთა მიმღები; მონაცემთა გაზიარების შესახებ არიან თუ არა ინფორმირებულები მონაცემთა სუბიექტები; მონაცემთა სუბიექტებს შეუძლიათ თუ არა თავიანთი უფლებებით სარგებლობა. შემდგომ ეტაპზე, კონფიდენციალობის გამაძლიერებელი ტექნოლოგიების გამოყენებით, ორგანიზაციებს შეუძლიათ კიდევ უფრო გააძლიერონ მონაცემთა დაცვის სტანდარტები, რომელთა საშუალებითაც მინიმუმამდე იქნება შემცირებული მონაცემთა გაზიარებასთან დაკავშირებული რისკები. საერთო ჯამში, კონფიდენციალობის გამაძლიერებელ ტექნოლოგიებს შეუძლია გადამწყვეტი როლი შეასრულოს ერთობლივი გადაწყვეტილების მიღების საფუძვლის შექმნაში, რაც საზოგადოებას სარგებელს მოუტანს და მიჩნეული იქნება „პარტნიორობის ხელშემწყობ ტექნოლოგიად“.[78]

მონაცემთა გაზიარების პროცესში, ჰარმონიზებულ და საერთაშორისო დონეზე კოორდინირებულ მარეგულირებელ ჩარჩოში ზემოაღნიშნული ტექნოლოგიების ინტეგრაციით, შესაძლებელი იქნება ეკონომიკური და სოციალური სარგებლის მიღება და ადამიანის უფლებების დაცვა გლობალურ დონეზე.

[78] *The Royal Society, From privacy to partnership: the role of Privacy Enhancing Technologies in data governance and collaborative analysis, 2023* <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf> [24.09.2025].

ბიბლიოგრაფია:

1. African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention, 2014).
2. *Asrow K. and Samonas S.,* Privacy Enhancing Technologies: Categories, Use Cases and Considerations, Federal Reserve Bank of San Francisco, CA, 2021.
3. Australian Data Availability and Transparency Act 2022.
4. *CDEI (n.d.), PETs Adoption Guide*, <https://cdeiuk.github.io/pets-adoption-guide/adoption-guide> [02.10.2025].
5. China, Measures for the Standard Contract for the Outbound Transfer of Personal Information, Cyberspace Administration of China, Decree No. 13.
6. China, Provisions on Facilitating and Regulating Cross-Border Data Flow (effective 22 March 2024).
7. China Regulation on Network Data Security Management (effective 1 January 2025), State Council Decree No. 790.
8. *Citron D.K., Solove D.J.,* Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, 102 Boston University Law Review 793, 2022.
9. Council of Europe, Convention 108 + Convention for the protection of individuals with regard to the processing of personal data, June 2018.
10. Councile of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), Strasbourg, 28.I.1981.
11. *d'Alessandro B., O'Neil C., La Gatta T.,* Conscientious Classification: a Data Scientist's Guide to Discrimination-Aware Classification, Big Data, 2017, 5(2), 120–34.
12. *Danezis G. et al.,* Privacy and Data Protection by Design – From Policy to Engineering, Computer Law & Security Review, Vol. 34, Issue 2, 2018.
13. *El Emam K., Mosquera L., Hoptroff R.,* Practical Synthetic Data Generation: Balancing Privacy and the Broad Availability of Data, O'Reilly Media, 2020.
14. *ENISA, Readiness Analysis for the Adoption and Evolution of Privacy-Enhancing Technologies (PETs), 2022.*
15. *ENISA Data Pseudonymisation: Advanced Techniques & Use Cases Technical analysis of cybersecurity measures in data protection and privacy - January 2021.*
16. *ENISA's PETs Maturity Assessment Repository, November 2018.*
17. *ENISA, Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, December 2015.*
18. *European Data Protection Board (EDPB), Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, Version 2.0, 7 July 2021*.
19. European Commission, Proposal for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM(2022) 68 final.
20. European Commission, A European Strategy for Data, COM(2020) 66 final, 19 February 2020.
21. European Convention on Human Rights, Rome, 4.XI.1950.

22. European Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 22.12.2023, p. 1-71.
23. European Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), OJ L 152, 3.6.2022, p. 1–44.
24. European Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
25. *Favaretto M., De Clercq E. & Elger B.S.,* Big Data and discrimination: perils, promises and solutions. A systematic review, J Big Data 2019, 6-12.
26. *Financial Services User Group (FSUG), Assessment of current and future impact of Big Data on Financial Services, 2016.*
27. *Granville K.,* Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens, the New York Times, 2018.
28. *Gregory Voss W.,* "Cross-Border Data Flows, the GDPR, and Data Governance," Washington International Law Journal, Vol. 29, No. 3, 2020.
29. Harvard University (n.d.), Differential Privacy, Harvard University Privacy Tools Project, <https://privacytools.seas.harvard.edu/differential-privacy> [02.10.2025].
30. International Covenant on Civil and Political Rights (Adopted by General Assembly resolution 2200 (XXI) of 16 December 1966).
31. *Isaak J. and Hanna M.*, User data privacy: Facebook, Cambridge Analytica, and Privacy Protection, Computer, Vol. 51/8, pp. 56-59, 2018.
32. *Jurcys P., Corrales Compagnucci M., Fenwick M.,* The Future of International Data Transfers: Managing Legal Risk with a User-Held Data Model, Computer Law & Security Review, Volume 46, September 2022, 105691.
33. *Konečnỳ J., McMahan B., Ramage D.*. Federated optimization: Distributed optimization beyond the datacentre, arXiv preprint arXiv:1511.03575, 2015.
34. *Kroll J.A., Huey J., Barocas S., Felten EW., Reidenberg JR., Robinson DG., Yu HL*., Accountable algorithms, Univ Pa Law Rev. 2017, 165(3), 633–705.
35. *McCarthy N., Fourniol F.,* The role of technology in governance: The example of Privacy Enhancing Technologies, Data & Policy, 2020.
36. *OECD, "Emerging privacy-enhancing technologies: Current regulatory and policy approaches", OECD Digital Economy Papers, No. 351, OECD Publishing, Paris, 2023.*
37. *OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013 Revision. OECD, Explanatory memoranda of the OECD Privacy Guidelines, 2022, PP 11-12.*

38. *OECD*, *Recommendation of the Council on, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, OECD/LEGAL/0463, 2021.*
39. *OECD, Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, OECD Publishing, Paris, 2019*.
40. *OECD, Declaration on the Digital Economy: Innovation, Growth and Social Prosperity (Cancún Declaration), OECD, Paris, 2016*
41. *OECD, Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 2013.*
42. *OECD, Recommendation of the Council for Enhanced Access and More Effective Use of Public Sector Information, OECD, Paris, 2008.*
43. *Nissenbaum H*., Privacy as Contextual Integrity, Washington Law Review, Vol. June, 2004.
44. *Royal Society, From privacy to partnership: the role of Privacy Enhancing Technologies in data governance and collaborative analysis, 2023.*
45. *Schermer BW.*, The Limits of Privacy in Automated Profiling and Data Mining, Comput Law Secur Rev. 2011, 27(1), 45–52.
46. SDAIA, Data Sharing Policy, 2024
47. *Tene O.and Polonetsky J.,* Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239, 2013.
48. *Truby J. et al.*, "A Sandbox Approach to Regulating High-Risk Artificial Intelligence Applications", European Journal of Risk Regulation, 2021.
49. UK, Data Sharing Governance Framework, 2022.
50. UK Information Commissioner's Office, Privacy-enhancing technologies (PETs), June 2023.
51. UN General Assembly Resolutions on the right to privacy in the digital age, e.g., A/RES/68/167 (2013).
52. *United Nations guide on Privacy-Enhancing Technologies for official statistics. United nations Big Data 2023.*
53. *United Nations, Roadmap for Digital Cooperation, 2020.*
54. US National Strategy lists technologies suitable for Privacy Preserving Data Sharing and Analytics.
55. *van Blarkom J.J., van Eck B.M.A. & Verhaar P.,* Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents, College bescherming persoonsgegevens, 2003.
56. *Wang Y. & Kobsa A.,* Privacy-Enhancing Technologies: Classification and Applications, in The Handbook of Privacy and Privacy-Enhancing Technologies, 2018.
57. *World Economic Forum*, *Good Data: Sharing Data and Fostering Public Trust and Willingness*, p. 6, 2021.