DOI: https://doi.org/10.65454/lc/2026/2/51-76

სახის ამომცნობი ტექნოლოგიები საქართველოს სისხლის სამართლის პროცესში – ხელოვნური ინტელექტი, „შავი ყუთი“ და სამართლიანი სასამართლოს უფლება

ეკა ხუციშვილი
სამართლის მაგისტრი
ფულბრაიტის სტიპენდიანტი
ჰუბერტ ჰ. ჰამფრის სტიპენდიის მონაწილე
ევროკომისიის სტიპენდიანტი სისხლის სამართლის
საერთაშორისო სასამართლოში
ekakhutsishvili77@gmail.com

ნინო გვენეტაძე
სამართლის დოქტორი, პროფესორი
თბილისის ივანე ჯავახიშვილის სახელობის
სახელმწიფო უნივერსიტეტის პრორექტორი
nino.gvenetadze@tsu.ge

რეფერატი. სტატია ეძღვნება სახის ამომცნობი ტექნოლოგიების (Facial Recognition Technologies – FRT) გამოყენებით ადამიანის უფლებრივი რისკების სამართლებრივ ანალიზს საქართველოს სისხლის სამართლის პროცესში. ნაშრომში განხილულია საზოგადოებრივი თავშეყრის (ხალხმრავალ) ადგილებში სისტემური და მასშტაბური მონიტორინგის განხორციელების პირობებში FRT გამოყენებით მოპოვებული მტკიცებულების სამართლებრივი შედეგები სისხლის სამართლის პროცესში. გამოვლენილია პერსონალურ მონაცემთა დაცვის შესახებ კანონის ხარვეზები, მონაცემთა დაცვაზე ზეგავლენის შეფასების (DPIA) დოკუმენტის სავალდებულო რეკვიზიტებთან დაკავშირებით. აღნიშნული წარმოქნის პირადი ცხოვრების ხელშეუხებლობისა და სამართლიანი სასამართლოს უფლების დარღვევის რისკებს. კვლევაში გაანალიზებულია ამ გზით მოპოვებული მტკიცებულების დასაშვებობის საკითხი – საქართველოს სისხლის სამართლის პროცესში და ადამიანის უფლებათა ევროპული კონვენციის

(ECHR) მე-6 და მე-8 მუხლების სტანდარტების მიხედვით. კვლევა ეყრდნობა ევროპის საბჭოსა და ევროკავშირის მიერ დადგენილ უახლეს სტანდარტებს; ადამიანის უფლებათა ევროპული სასამართლოს მიერ ჩამოყალიბებულ პრინციპებს; აშშ-ის სასამართლო პრაქტიკით და აკადემიური დებატებით დადგენილ დოქტრინალურ მიდგომებსა და სტანდარტებს – ე.წ. Frye/Daubert, „Glass Box" vs „Black Box" ხელოვნური ინტელექტისა (AI) და, მათ შორის, FRT მიმართებით და, ამასთან, საქართველოს მოქმედ საკანონმდებლო ჩარჩოს. საქართველოში პერსონალურ მონაცემთა დაცვის სტანდარტი განახლებული კანონმდებლობის შედეგად გაუმჯობესდა (2024 წლის მარტში ამოქმედებული საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ" უფრო მეტად მიუახლოვდა ევროკავშირის პერსონალურ მონაცემთა დაცვის აქტის – GDPR სტანდარტებს). მიუხედავად ამისა, არსებობს ხარვეზები, რომლებიც საჭიროებს აღმოფხვრას პირადი ცხოვრების ხელშეუხებლობისა და სამართლიანი სასამართლოს უფლების სრულყოფილი დაცვის მიზნით. DPIA რეკვიზიტების დახვეწა და შემდგომ სისხლის სამართლის პროცესში ამ დოკუმენტის გამოყენება არსებით როლს შეასრულებს ზემოაღნიშნული უფლებების სრულყოფილ დაცვაში.

საკვანძო სიტყვები: *სახის ამოცნობის ტექნოლოგია, ალგორითმული მიკვლევადობა, მონაცემთა დაცვაზე ზეგავლენის შეფასება, მტკიცებულებათა დასაშვებობა, სამართლიანი სასამართლო*

I. შესავალი

AI, როგორც მონაცემებზე დაფუძნებული გადაწყვეტილების მიღების მექანიზმი, დღეისათვის ცხოვრების თითქმის ყველა სფეროში გამოიყენება. მისი ერთერთი ფორმაა სახის ამომცნობი ტექნოლოგიები (FRT). FRT შესაძლებელს ხდის ციფრული გამოსახულებების შედარებას ერთი და იმავე პირის იდენტიფიცირების მიზნით ვიდეოკამერებიდან (CCTV) მიღებული კადრების მონაცემთა ბაზაში არსებულ გამოსახულებებთან შედარებით[1].

[1] European Union Agency for Fundamental Rights, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement* (FRA, November 2019) https://fra.europa.eu accessed 7 December 2025. p. 1.

ბოლო ათწლეულის განმავლობაში აღნიშნული ტექნოლოგიები ფართოდ დანერგეს როგორც აშშ-ის, ისე ევროკავშირის სამართალდამცავმა ორგანოებმა[2]. ამ პრაქტიკის მასშტაბს ნათლად აჩვენებს შექმნილი ბიომეტრიულ მონაცემთა ბაზების მოცულობა. უნგრეთში დაახლოებით 30 მილიონი სახის ფოტო, იტალიაში – 17 მილიონი, საფრანგეთში – 8 მილიონი, გერმანიაში – დაახლოებით 5.5 მილიონი; აშშ-ში 641 მილიონი[3].

FRT გამოყენების მასშტაბურობის პარალელურად, აშკარად გამოიკვეთა გამოყენების უკანონო და უფლებადამრღვევი პრაქტიკაც. მაგალითად, საფრანგეთში 2023 წლის ზაფხულის არეულობების დროს, ჟანდარმერიამ უკანონოდ გამოიყენა ისრაელის კომპანია – Briefcam-ის მიერ შემუშავებული დისტანციური FRT პროგრამა (post-remote FRT) სასამართლო ორგანოების ნებართვის გარეშე. არსებული ბაზიდან ატვირთეს ორი პირის ფოტო, სისტემამ ამოიცნო ისინი, თუმცა, გამოძიებით დადგინდა, რომ აღნიშნული ორი პირი საერთოდ არ მონაწილეობდა დანაშაულში[4].

FRT სისტემების უმრავლესობის სიზუსტე არ არის გარანტირებული. აღნიშნული ოფიციალურად აღიარებულია ევროკავშირის ხელოვნური ინტელექტის 2024 წლის რეგულაციით (EU AI Act), „ტექნიკური უზუსტობები ...შესაძლოა იწვევდეს მიკერძოებულ შედეგებს. ...ასეთი პოტენციური მიკერძოებული შედეგები და დისკრიმინაციული ეფექტები განსაკუთრებით აქტუალურია ასაკთან, ეთნიკურ წარმომავლობასთან, რასასთან, სქესთან ან შეზღუდულ შესაძლებლობებთან მიმართებით“[5]. აღნიშნულ უზუსტობებზე მიუთითებს, ასევე, აშშ-ს ანგარიშვალდებულების ოფისი. 2024 წლის აპრილში მის მიერ გამოქვეყნებულ ანგარიშში, მითითებულია, რომ ბიომეტრიული იდენტიფიკაციის ტექნოლოგიების უზუსტობის შედეგად, პირთა შეცდომით დაპატიმრება არის ამ ტექნოლოგიების გამოყენების უარყოფითი მხარის ერთ-ერთი გამოვლინება[6].

---

[2] Tracol, X. (2025) ‘*The Use of Facial Recognition Technologies by Law Enforcement Authorities in the US and the EU: Towards a Convergence on Regulation?*’ TechReg 289. p. 292.

[3] იქვე, p. 292-293.

[4] იქვე, p. 294

[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised rules on artificial intelligence (AI Act) [2024]. OJ L 2024/1689, recital 32.

[6] US Government Accountability Office, *Biometric Identification Technologies: Considerations to Address Information Gaps and Other Stakeholder Concerns* (GAO-24-106293, April 2024). https://www.gao.gov accessed 5 December 2025.

საქართველო უერთდება იმ ქვეყნების სიას, სადაც ზედამხედველობის ინფრასტრუქტურა ინტენსიურად ვითარდება. 2024 წლის 28 ნოემბრის შემდეგ ქვეყანაში გამართული დემონსტრაციების ფონზე, შინაგან საქმეთა სამინისტრომ, თბილისში გააძლიერა ვიდეო-სამეთვალყურეო სისტემა და განათავსა PTZ (Pan–Tilt–Zoom) ტიპის მბრუნავი კამერები, რომლებსაც, არსებული საჯარო ინფორმაციით, გააჩნიათ სახის ამოცნობისა და ავტომატური თვალთვალის ფუნქციონალი და ჩინური წარმოებისაა[7]. ამ გარემოებამ დღის წესრიგში კიდევ ერთხელ დააყენა საკითხი: რა ტიპის უფლებრივი და საპროცესო სტანდარტებია საჭირო, რომ FRT მიერ მოპოვებული მტკიცებულება იყოს არა მხოლოდ „კანონიერად მოპოვებული“, არამედ მეცნიერული სანდოობისა და სამართლიან სასამართლოში დასაშვები.

ევროპისა და აშშ-ის მაგალითზე განხორციელებული სამართლებრივი რეგულირების შედარებითმა კვლევამ წარმოაჩინა საჭიროება – საქართველომ ჩამოაყალიბოს არა მხოლოდ ზოგადი მონაცემების დაცვის სტანდარტები, არამედ FRT გამოყენების ფილტრები სისხლის სამართლის მართლმსაჯულების პროცესში.

II. FRT ქართული და ევროპული კანონმდებლობა

სახის ამომცნობი ტექნოლოგიების მასობრივი გამოყენება, რომელიც უშუალოდ უკავშირდება პირადი ცხოვრების ხელშეუხებლობის უფლების დარღვევის მაღალ რისკს, (ECHR, მუხლი 8), ავტომატურად უქმნის საფრთხეს სხვა ფუნდამენტურ უფლებებს[8], მათ შორის, სამართლიანი სასამართლოს უფლებას (ECHR, მუხლი 6). იმ შემთხვევაში, თუ სახელმწიფო იყენებს ტექნოლოგიურად მაღალი ინტენსივობის მეთვალყურეობას ბიომეტრიული იდენტიფიკაციისთვის, მაგრამ მის გამოყენებას არ ახლავს მკაფიო სამართლებრივი ჩარჩო; წინასწარი რისკების შეფასება და ეფექტიანი ზედამხედველობა – ეს მხოლოდ „კონფიდენციალობის“ პრობლემა არ არის. ყოველივე ნიშნავს, რომ სასამართლო პროცესი ეფუძნება ისეთ მტკიცებულებას, რომლის მოპოვებისა და მეცნიერული სანდოობის კანონიერება ეჭვქვეშაა. სწორედ აღნიშნული საკითხის ღრმა ანალიზია წარმოდგენილი წინამდებარე სტატიაში.

[7] https://idfi.ge Institute for Development of Freedom of Information (IDFI), მანიფესტანტების მასიური თვალთვალი და პერსონალურ მონაცემთა დაცვის სამსახურის არასათანადო რეაგირება. https://idfi.ge accessed 7 December 2025. pp 4-5.

[8] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 'Guidelines on facial recognition' (Council of Europe, 2021). https://rm.coe.int accessed 7 December 2025. p. 5.

საერთაშორისო სტანდარტების შესაბამისად (CoE, EU AI Act, OECD, UN), FRT გამოყენება, განსაკუთრებით საჯარო სივრცესა და სისხლის სამართლის საქმის გამოძიებისას, უნდა დაექვემდებაროს მკაცრ წინასწარ ფილტრებს – ტექნოლოგიის ლიცენზირებას, DPIA, ალგორითმული მიკერძოების აუდიტს და ადამიანის ზედამხედველობას[9].

AI გამოყენების პროცესში ევროკავშირის 2024 წლის აქტი ადგენს რეგულაციებს, რომლებიც მოიცავს მისი ფუნქციონირების ყველა ეტაპს, პასუხისმგებლობის გადანაწილებას მთელი სიცოცხლის ციკლზე, დიზაინსა და მონაცემთა მიწოდებაზე, დამზადებასა და განახლებებზე, დანერგვასა და ზედამხედველობაზე[10].

ზედმიწევნით რომ განვმარტოთ EU AI Act რეგულირებული „სიცოცხლის ციკლის“ (Lifecycle) დეფინიცია[11], მაგალითად მოვიყვანოთ სასამართლოსთვის ან პოლიციისთვის შექმნილი ალგორითმული პროგრამა, რომელიც არ არის ერთჯერადი პროდუქტი და გადის რამდენიმე ფაზას:

[9] Council of Europe, Committee of Ministers, *Recommendation CM/Rec (2020)1 on the human rights impacts of algorithmic systems* (adopted 8 April 2020). Principle 3, 4, 5 https://search.coe.int accessed 7 December 2025; EU AI Act (n 5) art 13-15, 27; OECD, *Recommendation of the Council on Artificial Intelligence* (C(2019)34/FINAL, adopted 22 May 2019). Principle 1.2, 1.3, 1.4, 1.5. https://legalinstruments.oecd.org accessed 7 December 2025; United Nations Human Rights Council, *The right to privacy in the digital age* (A/HRC/54/21, 11 September 2023). paras 7-10. https://undocs.org accessed 7 December 2025.

[10] EU AI Act (n 5) art 8-15. https://eur-lex.europa.eu accessed 7 December 2025.

[11] ხელოვნური ინტელექტის სიცოცხლის ციკლს აღწერს ხელოვნური ინტელექტის სისტემების კლასიფიკაციის OECD-ის ჩარჩო, რომელიც მოიცავს დაგეგმვას, მონაცემთა შეგროვებას, მოდელის შექმნას, განთავსებას და გამოყენებას, სადაც რეგულირებისა და რისკების მართვის მოთხოვნები დგება მთელი ამ ციკლის განმავლობაში: OECD, '*OECD Framework for the Classification of AI systems*' (OECD Digital Economy Papers №323, 2022). https://www.oecd.org accessed 7 December 2025.

ფაზა	აღწერა	მაგალითი
დიზაინი conception	მიზნის განსაზღვრა, მონაცემთა წყაროს შერჩევა, ეთიკური საზღვრების დადგენა	რისკის შეფასების მოდელი გაქცევის პროგნოზირების ალბათობაზე
შექმნა development	ალგორითმის გაწვრთნა მონაცემებზე, არქიტექტურის და ჰიპერპარამეტრების განსაზღვრა	მეცნიერთა ჯგუფის მიერ მანქანური სწავლების მოდელის შექმნა
ტესტირება validation	შედეგების სიზუსტე, მიკერძოების შემოწმება, შეცდომების ანალიზი	სატესტო შემოწმება სქესისა და ეთნიკურობის მიკერძოებაზე
დანერგვა deployment	მოდელის გადასვლა რეალურ ინსტიტუციურ გარემოში (მაგ: სასამართლოსა ან პოლიციის პროგრამაში)	სასამართლო პროგრამის მიერ რისკის ქულის მიღება გადაწყვეტილების მხარდასაჭერად
ზედამხედველობა და განახლება monitoring & updates	მონიტორინგი, შეცდომების გამოსწორება, ახალი მონაცემებით მოდელის ხელახალი გაწვრთნა	ექვს თვეში ერთხელ ალგორითმის ხელახალი შეფასება

FRT, როგორც AI ერთ-ერთი ფორმა, სანდო უნდა იყოს მთელი მისი „სიცოცხლის ციკლის“ (lifecycle) განმავლობაში, რათა მისი შედეგები სისხლის სამართლის პროცესში უტყუარ მტკიცებულებად ჩაითვალოს.

FRT სიცოცხლის ციკლის თითოეული ეტაპი ითვალისწინებს მკაფიო სამართლებრივ პასუხისმგებლობას: პროვაიდერი ვალდებულია შექმნას ტექნიკური დოკუმენტაცია, ჩაატაროს რისკ-შეფასება და სანდოობის ტესტები; დამნერგავი ორგანო (მაგ., პროდუქტის გამომყენებელი სამინისტრო) ვალდებულია გამოი-

ყენოს სისტემა მხოლოდ განსაზღვრული მიზნებით, უზრუნველყოს ადამიანის ზედამხედველობა და შეინახოს ლოგები; დისტრიბუტორი/იმპორტიორი ვალდებულია არ გაავრცელოს არასერტიფიცირებული/არასანდო პროდუქტი[12].

მითითებული მოდელი პირდაპირ ეხება კითხვას: თუ არც ერთ ეტაპზე არ არის დანერგილი სანდოობისა და მიკერძოების სათანადო კონტროლი, ჩაითვლება თუ არა ამ სისტემის მიერ წარმოქმნილი შედეგი „სანდო“ მტკიცებულებად სისხლის სამართლის საქმეში.

III. მონაცემთა დაცვაზე ზეგავლენის შეფასების (I) დოკუმენტი და მტკიცებულების დასაშვებობა საქართველოს სისხლის სამართლის საპროცესო კანონმდებლობაში

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ითვალისწინებს DPIA ჩატარების ვალდებულებას, როდესაც ხდება მაღალი რისკის მონაცემთა დამუშავება, მათ შორის ბიომეტრიული მონაცემების დამუშავება, რომელშიც ასევე იგულისხმება FRT[13]. DPIA ჩატარება სავალდებულოა მის დანერგვამდე, ცვლილების ან განახლებისას[14]. პრაქტიკულად, DPIA დოკუმენტია, რომელიც ამართლებს ჩარევის „კანონიერებას, საჭიროებას და პროპორციულობას“ ECHR მე-8 მუხლის სტანდარტით.

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის მიერ გამოცემული ნორმატიული აქტი, რომელიც DPIA რეკვიზიტებს განსაზღვრავს, არ ითვალისწინებს, რომ FRT შემთხვევაში დოკუმენტაცია ასევე უნდა შეიცავდეს გამოყენებული AI სისტემის შესახებ ინფორმაციას, მისი ზემოთაღნიშნული ალგორითმული მიკვლევადობის უზრუნველყოფის მიზნით. აღნიშნულის საპირისპიროდ, AI შესახებ ევროკავშირის აქტი აწესებს AI სისტემების პროვაიდერების ვალდებულებას, უზრუნველყონ მაღალი რისკის სისტემების რეგისტრაცია ევროკავშირის საჯარო მონაცემთა ბაზაში[15]. ხოლო რეგისტრაციის პროცესში პროვაიდე-

[12] EU AI Act (n 5) art 16-26.

[13] „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი, 12/11/2025, მუხლი მე-3; 31-ე.

[14] პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება №21, 2024 წლის 28 თებერვალი, მუხლი მე-6.

[15] EU AI Act (n 5) art 13, 27, 49.

რის მიერ მიწოდებული დეტალური ინფორმაცია, დარეგისტრირებული AI სისტემის შესახებ, უნდა იქნას გათვალისწინებული ადამიანის ძირითად უფლებებზე ზეგავლენის შეფასების დოკუმენტში (FRIA), როგორც მისი ერთ-ერთი ძირითადი კომპონენტი AI სისტემის შესაძლებლობების, ლიმიტებისა და ადამიანის ზედამხედველობის ზომების შესახებ[16]. იმის გათვალისწინებით, რომ FRIA საქართველოს კანონმდებლობით ინტეგრირებული DPIA, აღნიშნული რეკვიზიტები ინტეგრირებულ უნდა იქნეს DPIA ფარგლებში.

აღნიშნული ტექნიკური გამჭვირვალობის გარეშე, DPIA იძენს ფორმალურ ხასიათს და ვერ ასრულებს იმ ფუნქციას, რომელიც საერთაშორისო სტანდარტებითაა გათვალისწინებული. ამასთან, ვერ ხდება სასამართლოსთვის იმ ინფორმაციის მიწოდება, რომლის საფუძველზეც ის შეაფასებდა, იყო თუ არა ჩარევა ობიექტურად აუცილებელი, „დემოკრატიულ საზოგადოებაში საჭირო“ და მტკიცებულების წყარო – მეცნიერულად სანდო.

საქართველოს კონსტიტუციით გამამტყუნებელი განაჩენი უნდა ეფუძნებოდეს უტყუარ მტკიცებულებებს[17], ხოლო საქართველოს სისხლის სამართლის საპროცესო კოდექსი (სსსკ) პროცედურულად არეგულირებს მტკიცებულების უტყუარობას და განსაზღვრავს, რომ თუ ის მოპოვებულია ფორმალური და არსებითი დარღვევით, ან თუ კანონიერად მოპოვებული მტკიცებულება უკანონოდ მოპოვებულ მტკიცებულებაზე დაყრდნობით, იგი არის დაუშვებელი[18].

როდესაც DPIA შინაარსი არ მოიცავს ტექნიკური სანდოობის ანალიზს, დაცვის მხარესა და ასევე სასამართლოს, არ აქვს შესაძლებლობა, შეისწავლოს:

1. FRT გამოყენებისას დაცული პროპორციულობა და აუცილებლობა;
2. გამოყენებული სისტემის მეცნიერული სანდოობა;
3. FRT მოპოვების კანონიერება და მისი შინაარსის სიზუსტე.

ამდენად, FRT შემთხვევაში, უკანონოდ მისი მოპოვება შეიძლება გამოვლინდეს პირადი ცხოვრების ხელშეუხებლობისა (ECHR, მუხლი 8) და შემდგომ, სამართლიანი სასამართლოს უფლების დარღვევაში (ECHR, მუხლი 6).

[16] იქვე.

[17] საქართველოს კონსტიტუცია, 31-ე მუხლი. 29/06/2020.

[18] საქართველოს სისხლის სამართლის საპროცესო კოდექსი, 72-ე და 82-ე მუხლები, 16/10/2025.

IV. ალგორითმული მიკვლევადობა, „შავი ყუთი“ და დაცვის უფლება

FRT-ის სტანდარტების გამოყენებისას სისხლის სამართლის სასამართლო პროცესში, აუცილებელია, გავიაზროთ ალგორითმის საფუძველზე მოპოვებული მტკიცებულების ირგვლივ არსებული სამართლებრივი დისკუსიებისა და მიგნებების რეალური არსი. აღნიშნული დისკუსიები და მიგნებები ბოლო წლების განმავლობაში აქტუალური ხდება AI განვითარებასთან ერთად. აღნიშნული ტიპის მტკიცებულების სპეციფიკა ორ დონეზე ქმნის პრობლემას. ერთი მხრივ, ის არის ოპერაციულად გაუმჭვირვალე (opacity)[19]. შესაბამისად, დაცვის მხარე და მოსამართლე ხშირად ვერ ხედავენ, როგორ მიიღო ალგორითმმა კონკრეტული შედეგი. მეორე მხრივ, ასეთ სისტემებს ხშირად თან სდევს სტრუქტურული მიკერძოება (bias) – ისტორიული მონაცემების, დისკრიმინაციული პრაქტიკის და არასაკმარისი გადამოწმების გამო[20].

ამ პირობებში, ცენტრალური ხდება არა მხოლოდ კითხვა – *„საიდან მოვიდა ეს მონაცემი?“*, არამედ – *„რამდენად სამართლიანია თავად მეცნიერულ-ტექნიკური მეთოდი, რომელსაც სახელმწიფო იყენებს მოქალაქის წინააღმდეგ?“* სწორედ ამ შემთხვევაში განსაკუთრებულ მნიშვნელობას იძენს ტექნიკური/სამეცნიერო მტკიცებულების დასაშვებობის სტანდარტები.

აშშ-ში ეს დებატი ისტორიულად განვითარდა Frye-სა და Daubert-ის დოქტრინების ფარგლებში, რომლებმაც ჩამოაყალიბეს მოსამართლის როლი როგორც „კარიბჭის მცველი“ (gatekeeper) არასამეცნიერო მტკიცებულების მიმართ[21]. Frye/Daubert-ის მოდელი დღესაც წარმოადგენს ვიწრო მნიშვნელობით ამერიკულ, მაგრამ ფართო მნიშვნელობით – უნივერსალურ ჩარჩოს კითხვაზე პასუ-

[19] Burrell, J. (2016). ‘*How the machine ‘thinks’: Understanding opacity in machine learning algorithms*’. 3 Big Data & Society 1, p. 2-3. https://www.researchgate.net accessed 7 December 2025.

[20] Limantė, A. (2024). ‘*Bias in Facial Recognition Technologies Used by Law Enforcement: Understanding the Causes and Searching for a Way Out*’. 42 (2) *Nordic Journal of Human Rights 115,* pp. 1-3. https://www.tandfonline.com accessed 7 December 2025.

[21] Scirica, A. J. ‘*Preface: The Judges' Book*’ in *The Judges' Book: Creating a Fairer, More Effective and More Responsive Judiciary* (2020) 1. p. 45. https://repository.uclawsf.edu accessed 7 December 2025; Faigman, D. L., Slobogin, Ch., Monahan, J. (2016). ‘*Gatekeeping Science: Using the Structure of Scientific Inference to Draw the Line Between Admissibility and Weight in Expert Testimony*’. 110 Nw UL Rev 859, p. 7 https://scholarlycommons.law.northwestern.edu accessed 7 December 2025.

ხის გასაცემად – *როდის არის სამეცნიერო მტკიცებულება დასაშვები სასამართლოში?*

ევროპის საბჭოს სისტემაში Frye/Daubert პირდაპირ არ არსებობს, თუმცა ECHR-ის მე-6 მუხლი – სამართლიანი სასამართლოს უფლება – პრაქტიკაში ასრულებს ფუნქციურად მსგავს როლს: ის მოითხოვს, რომ ნებისმიერი მტკიცებულება (მათ შორის AI-ზე აგებული) გამოიყენებოდეს ისე, რომ არ დაირღვეს პროცესის სამართლიანობა მთლიანობაში (Al-Khawaja and Tahery v. UK, 2011)[22].

ამ თავში, ერთი მხრივ, მიმოვიხილავთ Frye-ისა და Daubert-ის სტანდარტებს, როგორც სამეცნიერო მტკიცებულების კლასიკურ ფილტრს, ხოლო მეორე მხრივ, ვაჩვენებთ, როგორ გადაიქცევა მათი მიდგომა ევროპული სამართლიანი სასამართლოს სტანდარტად – განსაკუთრებით AI პირობებში.

FRYE სტანდარტი

ამერიკაში სამეცნიერო მტკიცებულების კლასიკური ფილტრი იყო Frye v. United States (1923), სადაც სასამართლომ განაცხადა, რომ ახალი სამეცნიერო ტესტი მხოლოდ მაშინ არის დასაშვები, თუ ის „ზოგადად მიღებულია“ (general acceptance) შესაბამის სამეცნიერო საზოგადოებაში[23]. Frye იდეა მარტივია: თუ მეთოდი ნამდვილად სანდოა, მასზე შეიქმნება კონსესუსი ექსპერტულ საზოგადოებაში; თუ ასეთი კონსესუსი არ არსებობს, სასამართლო თავს იკავებს მისი გამოყენებისგან. ამ სტანდარტს ჰქონდა ორი აშკარა სარგებელი: ის იცავდა სასამართლოს ექსპერიმენტული მეცნიერებისგან; პასუხისმგებლობა სამეცნიერო სანდოობაზე მეტწილად გადაჰქონდა „სამეცნიერო საზოგადოებაზე“[24].

თანამედროვე ავტორები მიუთითებენ Frye-ის შემდეგ ძირითად ნაკლოვანებაზე: გადაჭარბებული კონსერვატიზმი – ინოვაციური, მაგრამ სანდო მეთოდები შეიძლება წლების განმავლობაში არ გახდეს „ზოგადად მიღებული“ და, შესაბამისად, სასამართლო პროცესიდან გამორიცხული დარჩეს; „ზოგადი მიღებულობის“ ბუნდოვანება – არ არის გამოკვეთილი, ვინ ქმნის „რელევანტურ სამეცნიე-

[22] *Al-Khawaja and Tahery v United Kingdom* (26766/05 and 22228/06) [2011]. ECHR 2127.

[23] *Frye v United States*, 293 F 1013 (DC Cir 1923); 'Admitting Doubt: A New Standard for Scientific Evidence' (2010). 123 Harv L Rev 2021 p. 2021. https://harvardlawreview.org accessed 7 December 2025.

[24] იქვე, p. 2023.

რო საზოგადოებას“ და როგორ განისაზღვრება „მიღებადობა“; სანდოობაზე არაპირდაპირი ფოკუსი – Frye არ სვამს კითხვას მეთოდოლოგიურ სიზუსტესა და შეცდომის მაჩვენებელზე; ის მხოლოდ ინტერესდება, „რას ფიქრობს“ პროფესიული საზოგადოება[25].

AI კონტექსტში Frye განსაკუთრებით პრობლემურია: ალგორითმული ინსტრუმენტები შეიძლება სწრაფად გახდეს ფართოდ გამოყენებადი, მაგრამ არა სავალდებულოდ ღრმა გადამოწმებით გამყარებული.

DAUBERT დოქტრინა: მოსამართლე როგორც „კარიბჭის მცველი“

Frye შემდგომი, გარდამტეხი მომენტი იყო Daubert v. Merrell Dow Pharmaceuticals (1993), სადაც აშშ-ის უზენაესმა სასამართლომ განაცხადა, რომ მტკიცებულებათა ფედერალური წესები – 702 (Rule 702) ცვლის Frye-ის დოქტრინას და მოსამართლეს ანიჭებს აქტიური კარიბჭის მცველის როლს: მოსამართლემ უნდა განიხილოს არა მხოლოდ მტკიცებულების რელევანტურობა, არამედ მისი სანდოობაც[26].

Daubert ერთად განვითარებულმა და ტრილოგიის სახელწოდებით დამკვიდრებულმა – „Daubert trilogy“ საქმეებმა: General Electric Co. v. Joiner (1997) და Kumho Tire Co. v. Carmichael (1999) – უფრო დეტალურად გამოავლინა მოსამართლის ვალდებულება, შეაფასოს როგორც სამეცნიერო, ისე ტექნიკური ექსპერტიზის სანდოობა[27].

Daubert-მა ჩამოაყალიბა რამდენიმე სახელმძღვანელო ფაქტორი:

1. ტესტირებადობა და ფალსიფიცირებადობა – შესაძლებელია თუ არა თეორიის ან ტექნიკის შემოწმება/გაბათილება ემპირიულად?
2. შეცდომის მაჩვენებელი (error rate) – რა არის ცნობილი პოტენციური შეცდომის სიხშირეზე, როგორ ვლინდება მცდარი დადებითი/მცდარი უარყოფითი (false positives/false negatives)?

[25] იქვე, p. 2021-2023.
[26] იქვე, p. 2021.
[27] Bernstein, D. E., Jackson, J. D. (2004). ‘*The Daubert Trilogy in the States*’. 44 Jurimetrics J 351, p. 2. https://www.researchgate.net accessed 7 December 2025.

3. რეცენზირება და პუბლიკაცია (peer review & publication) – არის თუ არა მეთოდი სამეცნიერო ჟურნალებში განხილული და აკადემიურად გაანალიზებული?
4. რეგულირების სტანდარტები – არსებობს თუ არა პროფესიული სტანდარტები, პროტოკოლები და ხარისხის კონტროლი, რომლებიც არეგულირებენ მეთოდის გამოყენებას?
5. ზოგადი მიღებადობა – რჩება მნიშვნელოვანი, მაგრამ როგორც ერთ-ერთი ფაქტორი სხვებთან ერთად, და არა ერთადერთი ფილტრი[28].

აშშ-ის მტკიცებულებათა ფედერალური წესების (Federal Rules of Evidence 2023) ბოლო ცვლილებები (2023), კიდევ უფრო ცხადად აფიქსირებს, რომ მტკიცებულების შემომტანმა მხარემ (proponent) უნდა დაამტკიცოს უფრო მეტად, ვიდრე ნაკლებად – *more likely than not* – სტანდარტით, რომ ექსპერტის დასკვნა დაყრდნობილია სანდო პრინციპებსა და მეთოდებზე და რომ ეს მეთოდები სწორად იქნა გამოყენებული მოცემულ საქმეზე[29].

AI სისტემისთვის ეს ჩარჩო უკიდურესად მნიშვნელოვანია: მსგავს სისტემებს ახასიათებთ „შიდა შავი ყუთი“, დინამიკური სწავლა, გამუდმებული განახლებები და რთული შეცდომის პროფილი. თუ სასამართლო არ სვამს Daubert-ის კითხვებს – როგორ არის ტესტირებული მოდელი, რა არის მისი შეცდომის მაჩვენებელი (error rate), რა მონაცემებზე აიგო, რა ხარისხის კონტროლი არსებობს – მაშინ AI-მტკიცებულება ფაქტობრივად მიიღება „რწმენით და არა ცოდნით“.

გარდა ზემოაღნიშნული სასამართლო სტანდარტისა, თანამედროვე ამერიკული ლიტერატურა უკვე ცალკე განიხილავს ალგორითმულ მტკიცებულებას.

Feigenson ახალმა ნაშრომმა AI-ს მტკიცებულებაზე აჩვენა, რომ სასამართლოს მოუწევს არამარტო ალგორითმის, არამედ შეიძლება „გაყალბებული“ ციფრული შინაარსის შეფასებაც კი: გაყალბებული ვიდეო ე.წ. deepfake, სინთეზური აუდიო, გენერირებული ტექსტები[30]. აქ Daubert-ის ტესტირებადობა, გადამოწმება-

[28] Daubert v Merrell Dow Pharmaceuticals Inc [1993], 509 US 579.
[29] Advisory Committee on Evidence Rules, *Agenda Book for Committee Meeting, April 19, 2024* (2024). pp. 16-17. https://www.uscourts.gov accessed 7 December 2025.
[30] Feigenson, N., Carney, B. (2025). '*Generative AI as Courtroom Evidence: A Practical Guide*'. 52 Mitchell Hamline L Rev 1, pp. 2-6. https://open.mitchellhamline.edu accessed 7 December 2025.

დობა – peer review და შეცდომის პროცენტული მაჩვენებელი – error rate კიდევ უფრო კრიტიკულია[31] .

V. ევროპული კონტექსტი: ECHR-ის მე-6 მუხლი როგორც FRY/DAUBERT სტანდარტის ფუნქციური ეკვივალენტი

ევროპის საბჭოს სისტემაში არ არსებობს Daubert ან Frye ფორმალური ეკვივალენტი. თუმცა, სამართლიანი სასამართლოს უფლება (ECHR, მუხლი მე-6) და სტრასბურგის სასამართლოს პრაქტიკა, ქმნიან ფუნქციურად მსგავს ფილტრს ნებისმიერი მტკიცებულების, მათ შორის სამეცნიერო და ალგორითმულ გამოყენებაზე.

ECtHR სახელმძღვანელოები და საქმეები ხაზს უსვამს, რომ:

- კონვენცია არ აწესებს „კოდიფიცირებულ“ მტკიცებულებით სამართალს – წევრ სახელმწიფოებს რჩებათ დისკრეცია განსაზღვრონ, რა არის დასაშვები მტკიცებულება;
- მაგრამ სასამართლო მუდმივად ამოწმებს, არღვევს თუ არა კონკრეტული მტკიცებულების გამოყენება „პროცესის საერთო სამართლიანობას“[32].

Al-Khawaja and Tahery v. UK-ში გამოკვეთილი „Al-Khawaja test“ – hearsay მტკიცებულების დასაშვებად – კარგი მაგალითია იმისა, როგორ აშენებს სტრასბურგი პროცედურული უსაფრთხოების მექანიზმებს მაშინ, როდესაც მტკიცებულება ვერ გადის პირდაპირ დაკითხვას და ჯვარედინ დაკითხვას (cross-examination): გაგონილი – hearsay არ უნდა იყოს ერთადერთი ან გადამწყვეტი, და აუცილებელია საკმარისი დამაბალანსებელი ფაქტორები[33].

ალგორითმული მტკიცებულება ამ კონტექსტში, გარკვეულწილად, „ციფრული hearsay“ ხდება: დაცვას არ შეუძლია დაკითხოს ალგორითმი, გადაამოწმოს მისი ინტუიცია, არ იცის, რა მონაცემებზეა აგებული სისტემა. სწორედ, ამიტომ კონვენციის მე-6 მუხლის ძირითადი პრინციპები პრაქტიკულად ახორციელებს Daubert-ის გზავნილს ევროპაში.

ECtHR პრაქტიკაში განმტკიცებულია, რომ მხარეებს უნდა ჰქონდეთ ადეკვატუ-

[31] იქვე, pp. 36-39.
[32] European Court of Human Rights, *Guide on Article 6 of the European Convention on Human Rights (Criminal limb)* (2024), p. 7. https://ks.echr.coe.int accessed 7 December 2025.
[33] *Al-Khawaja* (n 22).

რი დრო და შესაძლებლობა თავიანთი დაცვის მოსამზადებლად, რაც მოიცავს ხელმისაწვდომობას საქმის მასალებზე და არსებით მტკიცებულებაზე[34].

AI-მტკიცებულების შემთხვევაში ეს ითარგმნება რამდენიმე კონკრეტულ მოთხოვნად:

- დაცვას უნდა ჰქონდეს შესაძლებლობა მიიღოს ინფორმაცია გამოყენებული მოდელის შესახებ, მინიმუმ, გადამოწმების შედეგები, შეცდომის მაჩვენებლები, მონაცემების ზოგადი აღწერა;
- მხარეს უნდა შეეძლოს წარმოადგინოს საკუთარი ექსპერტი, რომელიც შეაფასებს ალგორითმის სანდოობას;
- სასამართლომ არ უნდა დაუშვას, რომ გადამწყვეტი მტკიცებულება იყოს ისეთი, რომლის ტექნიკური შემოწმებაც ფაქტობრივად შეუძლებელია.

„შედავების შესაძლებლობის უფლება“ (right to contest) არის არა მარტო მონაცემთა დაცვის, არამედ სამართლიანი სასამართლოს ცენტრალური კომპონენტი; გამოყენებული AI შესაძლოა იყოს არაზუსტი და ამ ფონზე, სწორედ სამართლიანი პროცესის აღნიშნული მექანიზმები გამოასწორებს მას[35].

ამ მხრივ, Daubert-ის ტესტირების, რეცენზირების – peer review-ის და შეცდომის მაჩვენებლის – error rate-ის მოთხოვნები ევროპულ კონტექსტში გადაიქცევა მოთხოვნად იმისა, რომ მხარემ გააკონტროლოს და გაასაჩივროს სახელმწიფოს მიერ მოწოდებული ტექნიკური მეთოდი.

აშშ-სა და ევროპის სტანდარტებთან ერთად, გაერო-ს სპეციალური მომხსენებლის (Satterthwaite) 2025 წლის ანგარიში აცხადებს, რომ „ადამიან მოსამართლეზე უფლება“ მოითხოვს, საბოლოო გადაწყვეტილება მიიღოს არა ალგორითმმა, არამედ დამოუკიდებელმა და მიუკერძოებელმა მოსამართლემ, რომელიც რეალურად აკონტროლებს ტექნიკურ ინსტრუმენტებს და არ არის მათზე მექანიკურად დამოკიდებული[36].

[34] ECtHR, *Guide on Article 6 (Criminal limb)* (n 32), p. 39. https://ks.echr.coe.int. accessed 7 December 2025.

[35] Kaminski, M. E., Urban, J. M. (2021). '*The Right to Contest AI*'. 121 Colum L Rev 1957, pp. 1999-2000. https://www.columbialawreview.org accessed 7 December 2025.

[36] UN General Assembly, *AI in judicial systems: promises and pitfalls*, Report of the Special Rapporteur on the independence of judges and lawyers, Margaret Satterthwaite, A/80/169 (16 July 2025). https://docs.un.org accessed 7 December 2025.

ეს ხედვა პრაქტიკულად ნიშნავს: თუ სასამართლო თვითონ არ ფლობს მინიმალურ ცოდნას AI-ს ბუნებისა და შეზღუდვების შესახებ, ის ვერ უზრუნველყოფს კონვენციის მე-6 მუხლის მიერ მოთხოვნილ დონეს – არც Daubert-ის არსი იქნება დაცული, არც სამართლიანი სასამართლოს სტანდარტი.

თუ FRT-ის შედეგი გამოიყენება ადამიანის ძირითადი უფლების შეზღუდვისთვის, დაცვის მხარეს უნდა ჰქონდეს რეალური შესაძლებლობა:

- გაიგოს, „როგორ“ მივიდა სისტემა კონკრეტულ შედეგამდე (interpretability);
- მიიღოს ინფორმაცია შეცდომის მაჩვენებლებსა და მიკერძოების შესახებ;
- მოითხოვოს დამოუკიდებელი კონტრ-ექსპერტიზა (counter-expertise).

ავტორები, Garrett და Rudin თანამედროვე დებატებში ხატოვნად საუბრობენ „მინის ყუთის გამოყენების უფლებაზე“ – „Right to a Glass Box“. აღნიშნულში იგულისხმება ახსნადი, ინტერპრეტირებადი და გასაგები მოდელი[37]. ავტორები აცხადებენ, რომ „მინის ყუთის“ (*glass box*) ტიპის ხელოვნური ინტელექტის შემთხვევაში, არამარტო ხდება შედეგების უფრო მარტივად გასაგები ფორმით წარმოდგენა, არამედ შესაძლებელია კონკრეტული მოდელების „დაშლა“ ისე, რომ შესაბამისი ფაქტორები გაგებულ იქნას ინდივიდუალურ გადაწყვეტილებასთან მიმართებით (ე.წ. ინტერპრეტირებადობის კონცეფცია)[38]. სამ ფუნდამენტურ გამოწვევაზე მიუთითებენ ავტორები, რომელიც ხელოვნური ინტელექტის ყველა სისტემას ემუქრება და განსაკუთრებულ პრობლემებს ქმნის სისხლის სამართლის საქმეებში:

1. მონაცემების პრობლემა: უწინარეს ყოვლისა, სისხლის სამართლის მართლმსაჯულების მონაცემები ხშირად არის ბუნდოვანი, მაღალი შერჩევითობით მიღებული და არასრული, ისევე როგორც შეცდომებით სავსე;
2. გადამოწმება და შეცდომის კორექცია: მეორე მხრივ, „მინის ყუთის“ ტიპის AI გამოყენებისას, ჩვენ შეგვიძლია მოვახდინოთ სისტემის გადამოწმება, შეცდომების აღმოჩენა და კორექტირება;
3. გაგებადობის (ინტერპრეტირებადობის) აუცილებლობა: მესამე, ინტერპრეტირებადობა განსაკუთრებით მნიშვნელოვანია სამართლებრივ გარემოში, სა-

[37] Garrett, B. L., Rudin, C. ‘*Right to a Glass Box: Explainability and Transparency in Criminal Justice Algorithms*’ (SSRN Working Paper №4361462, 2023), p. 5. https://ssrn.com accessed 7 December 2025.
[38] იქვე, p. 5.

დაც AI მომხმარებლებს, როგორებიც არიან პოლიციის თანამშრომლები, იურისტები, მოსამართლეები და ნაფიცი მსაჯულები, არ შეუძლიათ სამართლიანად და ზუსტად გამოიყენონ ის, რისი გაგებაც არ ძალუძთ[39].

„შავ ყუთში“ იგულისხმება ბუნდოვანი მოდელი, რომლის ფუნქციონირების ლოგიკა გაუგებარია არაპროფესიონალების და მათ შორის ექსპერტებისთვისაც[40]. FRT სისტემებში კი, უმეტესწილად, სწორედ შავი ყუთის სისტემები გამოიყენება[41].

საქართველოს სისხლის სამართლის საპროცესო კოდექსი არ ითვალისწინებს ალგორითმთან დაკავშირებული მტკიცებულების დასაშვებობის სტანდარტს, მას მტკიცებულებათა დასაშვებობის ზოგად კონტექსტში მოიაზრებს, ხოლო პერსონალურ მონაცემთა დაცვის კანონმდებლობა არ ითვალისწინებს:

- ვალდებულებას, FRT სისტემის სანდოობისა და მიკერძოების შესახებ დოკუმენტაციის DPIA განსაზღვრის აუცილებლობაზე;
- ვალდებულებას, რომ ეს დოკუმენტაცია ხელმისაწვდომი იყოს სასამართლოსა და დაცვის მხარისთვის;

შედეგად, ბრალდების მხარე პრაქტიკულად იღებს უფლებას, გამოიყენოს „შავი ყუთი“ მტკიცებულებად, ხოლო დაცვის მხარე რჩება ტექნოლოგიური ლაბირინთის გარეთ. ეს არღვევს მხარეთა თანასწორობის (equality of arms) და შეჯიბრებითობის (adversarial trial) პრინციპებს, რომლებიც ECHR-ის მე-6 მუხლის ბირთვია.

ციფრული ინსტრუმენტები წარმოშობს სამ ფუნდამენტურ საპროცესო მოთხოვნას:

1. ახსნადობა – მხარემ უნდა იცოდეს, „რა“ და „როგორ“ გამოითვალა;
2. თანასწორი დაშვება – დაცვას უნდა ჰქონდეს წვდომა მეთოდოლოგიაზე, მონაცემებზე და შეცდომის საზომებზე/ცდომილების მაჩვენებელზე;
3. კონტრ-ექსპერტიზა – რეალური შესაძლებლობა დამოუკიდებელი ტესტირებისა და ექსპერტიზის ჩატარებისთვის.

[39] იქვე, p. 5.
[40] იქვე, p. 4.
[41] იქვე, p. 14.

ECtHR ევოლუციური ინტერპრეტაცია ცხადყოფს, რომ ტექნიკური ბარიერები, რაც ხელოვნურ ინტელექტს უკავშირდება, სინამდვილეში იურიდიული ბარიერებია დაცვის უფლებისთვის.

დაცვის უფლება (ECHR 6(3)(c)) მოიცავს ადვოკატის „რეალურ და არა ფორმალურ“ შესაძლებლობას, რასაც შეჯიბრებითობა გულისხმობს, რომ არც ერთი მხარე არ იყოს ინფორმაციულად პრივილეგირებული ისეთი კრიტიკული მტკიცებულების მიმართ, როგორიც არის FRT.

ამ კონტექსტში, Frye–Daubert-ის ამერიკული სტანდარტები ჩვენთვის არა როგორც უცხო მოდელი, არამედ გასაზიარებელი დოქტრინული მიდგომაა: მტკიცებულების მეცნიერული სანდოობა უნდა იყოს სასამართლოს მიერ აქტიურად კონტროლირებადი, წინააღმდეგ შემთხვევაში, სამართლიანი სასამართლოს სტანდარტი შინაარსობრივად იცვლება.

ECHR უახლესი პრაქტიკა (Glukhin v Russia[42], Podchasov v Russia[43] და სხვ.) ქმნის ერთიან სტანდარტს, რომელიც პირდაპირ ვრცელდება FRT:

1. ბიომეტრიული მეთვალყურეობა არის უკიდურესად მაღალი ინტენსივობის ჩარევა ადამიანის უფლებათა დაცვის კონვენციის მე-8 მუხლის ფარგლებში;
2. ამგვარი ჩარევა კანონიერია მხოლოდ მაშინ, თუ არსებობს მკაფიო სამართლებრივი ჩარჩო – DPIA/FRIA, ტექნიკური დოკუმენტაცია, დამოუკიდებელი ზედამხედველობა;
3. თუ ეს მექანიზმები არ არსებობს, ჩარევა უკანონოა და მის შედეგად მოპოვებული ინფორმაცია არ შეიძლება ჩაითვალოს სამართლიან პროცესთან თავსებად მტკიცებულებად.

ამ ფონზე, საქართველოში FRT გამოყენების შემთხვევაში, თუ

- DPIA არ ჩატარდა, მიუხედავად სავალდებულოობისა; ან
- DPIA ჩატარდა, მაგრამ არ შეიცავს ტექნიკური სანდოობის მონაცემებს; ტექნოლოგია არ არის სერტიფიცირებული საერთაშორისო სტანდარტების შესაბამისად;

[42] *Glukhin v Russia* (2023) App no 11519/20 (ECtHR).
[43] *Podchasov v Russia* (2024) App no 33696/19 (ECtHR).

მაშინ:

- ECHR-ის სტანდარტით მე-8 მუხლი დარღვეულია– ჩარევა „კანონის ხარისხისა“ და „პროპორციულობის“ ტესტს არ აკმაყოფილებს;
- Art 6 დარღვევად შეიძლება შეფასდეს, თუ ეს მონაცემი გამოიყენება, როგორც მტკიცებულება ისე, რომ დაცვას არ აქვს წვდომა ტექნიკურ დეტალებზე და კონტრ-ექსპერტიზაზე.

დასკვნა

კვლევა ცხადყოფს, რომ სახის ამომცნობი ტექნოლოგიების (FRT) უკონტროლო ინტეგრაცია საქართველოს სისხლის სამართლის საპროცესო მართლმსაჯულებაში, წარმოშობს ღრმა უფლებრივ და საპროცესო ხარვეზებს, რომელიც უპირისპირდება ადამიანის უფლებათა ევროპული კონვენციის (ECHR) მე-8 (პირადი ცხოვრების) და მე-6 (სამართლიანი სასამართლოს) მუხლების მოთხოვნებს.

სამართლებრივი გარანტიების დეფიციტი: საქართველოში არსებული მარეგულირებელი ჩარჩო, კერძოდ, მონაცემთა დაცვაზე ზეგავლენის შეფასება (DPIA), ფორმალიზებულია და არ შეიცავს ალგორითმული მიკვლევადობის (algorithmic traceability) სავალდებულო სტანდარტებს. ამის გარეშე, სახელმწიფო ვერ ამტკიცებს FRT-ის გამოყენების „კანონის ხარისხს“ და პროპორციულობას, რაც პირდაპირ ქმნის ECHR-ის მე-8 მუხლის დარღვევის წინაპირობას.

„შავი ყუთის“ პრობლემა და ECHR მე-6 მუხლი: როდესაც ბრალდების მხარე იყენებს FRT მიერ გენერირებულ მტკიცებულებას, რომლის შიდა ლოგიკა გაუმჭვირვალეა („შავი ყუთი“), ხოლო დაცვის მხარეს არ აქვს წვდომა შეცდომის მაჩვენებელზე (error rate), მიკერძოების აუდიტსა და კონტრ-ექსპერტიზაზე, ირღვევა მხარეთა თანასწორობისა (equality of arms) და შეჯიბრებითობის ფუნდამენტური პრინციპები. ევროპული პრაქტიკა და ამერიკული Daubert-ის დოქტრინის ლოგიკა ერთიანდება მოთხოვნაში: სამეცნიერო მტკიცებულება აქტიურად უნდა კონტროლდებოდეს სასამართლოს მიერ.

ტექნოლოგიური პროგრესის პირობებში, საქართველოსთვის ორმაგი სტანდარტის დანერგვა აუცილებელია:

- DPIA (მონაცემთა დაცვაზე ზეგავლენის შეფასების) შინაარსობრივი გაძლიერება: FRT (სახის ამომცნობი ტექნოლოგიების) სისტემების სანდოობისა და მი-

კერძოების ანალიზის ალგორითმული მოთხოვნების ინტეგრაცია DPIA, ევროკავშირის AI აქტის საუკეთესო პრაქტიკის მიხედვით;

- საპროცესო ფილტრის შემოღება: სისხლის სამართლის საპროცესო კანონმდებლობაში Daubert ფუნქციური ეკვივალენტის განსაზღვრა, რომელიც მოსამართლეს აძლევს უფლებას და ავალდებულებს, შეაფასოს ტექნიკური მეთოდოლოგიის მეცნიერული სანდოობა და უზრუნველყოს „მინის ყუთის“ (Glass Box) პრინციპი.

FRT-ის გამოყენების ლეგიტიმაცია საქართველოს სისხლის სამართლის პროცესში შესაძლებელია მხოლოდ იმ პირობით, თუ ტექნოლოგიური გამჭვირვალობა იქცევა სამართლებრივ ვალდებულებად, ხოლო მოსამართლე დარჩება გადაწყვეტილების მიღების პროცესის რეალურ მაკონტროლებლად და არა ალგორითმის მექანიკურ შემსრულებლად.

გამოყენებული ლიტერატურა

საქართველოს კანონმდებლობა

საქართველოს კონსტიტუცია, 29/06/2020.

საქართველოს კანონი „პერსონალურ მონაცემთა დაცის შესახებ“ (12/11/2025).

საქართველოს სისხლის სამართლის საპროცესო კოდექსი (ბოლოს განახლებული რედაქცია). 16/10/2025.

პერსონალურ მონაცემთა დაცვის სამსახურის უფროსის ბრძანება №21, 2024 წლის 28 თებერვალი.

ევროკავშირის კანონმდებლობა

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 168/1. https://eur-lex.europa.eu/eli/reg/2024/1689/oj accessed 7 December 2025.

საერთაშორისო სამართლებრივი ინსტრუმენტები

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), ‘*Guidelines*

on facial recognition' (Council of Europe, 2021). https://rm.coe.int accessed 7 December 2025.

Council of Europe, Committee of Ministers, Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems (adopted 8 April 2020). https://search.coe.int accessed 7 December 2025.

European Court of Human Rights, *Guide on Article 6 of the European Convention on Human Rights (Criminal limb)* (2024). https://ks.echr.coe.int accessed 7 December 2025.

OECD, '*OECD Framework for the Classification of AI systems*' (OECD Digital Economy Papers №323, 2022). https://www.oecd.org accessed 7 December 2025.

OECD, *Recommendation of the Council on Artificial Intelligence*, C(2019)34/FINAL (adopted 22 May 2019). https://legalinstruments.oecd.org accessed 7 December 2025.

UN General Assembly, *AI in judicial systems: promises and pitfalls*, Report of the Special Rapporteur on the independence of judges and lawyers, Margaret Satterthwaite, A/80/169 (16 July 2025). https://docs.un.org accessed 7 December 2025.

United Nations Human Rights Council, *The right to privacy in the digital age*, A/HRC/54/21 (11 September 2023). https://undocs.org accessed 7 December 2025.

სამეცნიერო სტატიები

'*Admitting Doubt: A New Standard for Scientific Evidence*' (2010) 123 Harv L Rev 2021. https://harvardlawreview.org accessed 7 December 2025.

Bernstein, D. E., Jackson, J. D. (2004). '*The Daubert Trilogy in the States*'. 44 Jurimetrics J 351. https://www.researchgate.net accessed 7 December 2025.

Burrell, J. (2016). '*How the machine 'thinks': Understanding opacity in machine learning algorithms*'. 3 Big Data & Society 1. https://www.researchgate.net accessed 7 December 2025.

Faigman, D. L., Slobogin, Ch., Monahan, J. (2016). '*Gatekeeping Science: Using the Structure of Scientific Inference to Draw the Line Between Admissibility and Weight in Expert Testimony*'. 110 Nw UL Rev 859. https://scholarlycommons.law.northwestern.edu accessed 7 December 2025.

Feigenson, N., Carney, B. (2025). '*Generative AI as Courtroom Evidence: A Practical Guide*'. 52 Mitchell Hamline L Rev 1. https://open.mitchellhamline.edu accessed 7 December 2025.

Kaminski, M. E., Urban, J. M. (2021). '*The Right to Contest AI*'. 121 Colum L Rev 1957. https://www.columbialawreview.org accessed 7 December 2025.

Limantė, A. (2024). '*Bias in Facial Recognition Technologies Used by Law Enforcement: Understanding the Causes and Searching for a Way Out*'. 42 (2) Nordic Journal of Human Rights 115. https://www.tandfonline.com accessed 7 December 2025.

Tracol, X. (2025). '*The Use of Facial Recognition Technologies by Law Enforcement Authorities in the US and the EU: Towards a Convergence on Regulation?*' TechReg 289.

წიგნები, ანგარიშები და სხვა პუბლიკაციები

Advisory Committee on Evidence Rules, *Agenda Book for Committee Meeting, April 19, 2024* (2024). https://www.uscourts.gov accessed 7 December 2025.

European Union Agency for Fundamental Rights, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement* (FRA, November 2019). https://fra.europa.eu accessed 7 December 2025.

Garrett, B. L., Rudin, C. (2023). '*Right to a Glass Box: Explainability and Transparency in Criminal Justice Algorithms*' (SSRN Working Paper №4361462). https://ssrn.com accessed 7 December 2025.

Institute for Development of Freedom of Information (IDFI), მანიფესტანტების მასიური თვალთვალი და პერსონალურ მონაცემთა დაცვის სამსახურის არასათანადო რეაგირება. https://idfi.ge accessed 7 December 2025.

Scirica, A. J. (2020). '*Preface: The Judges' Book*' in *The Judges' Book: Creating a Fairer, More Effective and More Responsive Judiciary*, 1. https://repository.uclawsf.edu accessed 7 December 2025.

US Government Accountability Office, *Biometric Identification Technologies: Considerations to Address Information Gaps and Other Stakeholder Concerns*, GAO-24-106293 (April 2024). https://www.gao.gov accessed 5 December 2025.

სამოსამართლო პრაქტიკა

ადამიანის უფლებათა ევროპული სასამართლოს გადაწყვეტილებები

Al-Khawaja and Tahery v United Kingdom (2011), 54 EHRR 23.
Glukhin v Russia, App no 11519/20 (ECtHR, 4 July 2023).
Podchasov v Russia, App no 33696/19 (ECtHR, 7 February 2023).

ამერიკის შეერთებული შტატების სასამართლოს გადაწყვეტილებები

Frye v United States 293 F 1013 (DC Cir 1923).
Daubert v Merrell Dow Pharmaceuticals 509 US 579 (1993).
General Electric Co v Joiner 522 US 136 (1997).
Kumho Tire Co v Carmichael 526 US 137 (1999).

FACIAL RECOGNITION TECHNOLOGIES IN GEORGIAN CRIMINAL PROCEDURE – ARTIFICIAL INTELLIGENCE, THE 'BLACK BOX' AND THE RIGHT TO A FAIR TRIAL

EKA KHUTSISHVILI
Master of Law
Fulbright Scholar
Hubert H. Humphrey Fellow
Fellow of the European Commission at the International Criminal Court
ekakhutsishvili77@gmail.com

NINO GVENETADZE
Doctor of Law, Professor
Vice-Rector, Tbilisi State University
nino.gvenetadze@tsu.ge

Abstract. This article is dedicated to the legal analysis of human rights risks associated with the use of Facial Recognition Technologies (FRT) within the framework of Georgian criminal procedure. The paper examines the legal consequences of evidence obtained through the use of FRT, specifically in the context of systemic and large-scale monitoring conducted in public (crowded) places during criminal proceedings. The study identifies gaps in the Law of Georgia on Personal Data Protection, particularly concerning mandatory requirements for the Data Protection Impact Assessment (DPIA) document. These gaps create risks of violating the rights to private life and a fair trial. The research analyses the admissibility of evidence obtained with this method under both Georgian criminal procedure and the standards of Articles 6 (Right to a Fair Trial) and Article 8 (Right to Respect for Private and Family Life) of the European Convention on Human Rights (ECHR). The research relies on: the latest standards established by the Council of Europe and the European Union; Principles developed by the European Court of Human Rights (ECtHR); Doctrinal approaches and standards established by US court practice and academic debates-, such as the Frye/Daubert standards and the "Glass Box" vs "Black Box" doctrines in relation to Artificial Intelligence, including FRT; Georgia's current legislative framework. While Georgia's

personal data protection standards have improved following the updated legislation (the Georgian Law "On Personal Data Protection" enacted in March 2024 brought them closer to the EU's General Data Protection Regulation (GDPR) standards), gaps remain. These flaws need to be addressed to ensure full protection of the rights to private life and a fair trial. Specifically, refining the requirements of the Data Protection Impact Assessment (DPIA) document and subsequently utilizing this document in criminal proceedings will play a crucial role in the comprehensive protection of the aforementioned rights.

Keywords: *Facial Recognition Technology (FRT), Algorithmic Traceability, Data Protection Impact Assessment (DPIA), Admissibility of Evidence, Fair Trial*

REFERENCES

LEGISLATION OF GEORGIA

Constitution of Georgia, 29/06/2020.

Law of Georgia "On Personal Data Protection" (12/11/2025).

Criminal Procedure Code of Georgia (Latest updated edition), 16/10/2025.

Order №21 of the Head of the Personal Data Protection Service**,** February 28, 2024; *Mass Surveillance of Protesters and the Inadequate Response of the Personal Data Protection Service*.

LEGISLATION OF THE EUROPEAN UNION

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 168/1. https://eur-lex.europa.eu/eli/reg/2024/1689/oj accessed 7 December 2025.

INTERNATIONAL LEGAL INSTRUMENTS

Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), '*Guidelines on facial recognition*' (Council of Europe, 2021). https://rm.coe.int accessed 7 December 2025.

Council of Europe, Committee of Ministers, Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems (adopted 8 April 2020). https://search.coe.int accessed 7 December 2025.

European Court of Human Rights, *Guide on Article 6 of the European Convention on Human Rights (Criminal limb)* (2024). https://ks.echr.coe.int accessed 7 December 2025.

OECD, '*OECD Framework for the Classification of AI systems*' (OECD Digital Economy Papers № 323, 2022). https://www.oecd.org accessed 7 December 2025.

OECD, *Recommendation of the Council on Artificial Intelligence*, C(2019)34/FINAL (adopted 22 May 2019). https://legalinstruments.oecd.org accessed 7 December 2025.

UN General Assembly, *AI in judicial systems: promises and pitfalls*, Report of the Special Rapporteur on the independence of judges and lawyers, Margaret Satterthwaite, A/80/169 (16 July 2025). https://docs.un.org accessed 7 December 2025.

United Nations Human Rights Council, *The right to privacy in the digital age*, A/HRC/54/21 (11 September 2023). https://undocs.org accessed 7 December 2025.

SCHOLARLY ARTICLES

'*Admitting Doubt: A New Standard for Scientific Evidence*' (2010) 123 Harv L Rev 2021. https://harvardlawreview.org accessed 7 December 2025.

Bernstein, D. E., Jackson, J. D. (2004). '*The Daubert Trilogy in the States*'. 44 Jurimetrics J 351. https://www.researchgate.net accessed 7 December 2025.

Burrell, J. '*How the machine 'thinks': Understanding opacity in machine learning algorithms*' (2016) 3 Big Data & Society 1. https://www.researchgate.net accessed 7 December 2025.

Faigman, D. L., Slobogin, C., Monahan, J. (2016). '*Gatekeeping Science: Using the Structure of Scientific Inference to Draw the Line Between Admissibility and Weight in Expert Testimony*'. 110 Nw UL Rev 859. https://scholarlycommons.law.northwestern.edu accessed 7 December 2025.

Feigenson, N., Carney, B. (2025). '*Generative AI as Courtroom Evidence: A Practical Guide*'. 52 Mitchell Hamline L Rev 1. https://open.mitchellhamline.edu accessed 7 December 2025.

Kaminski, M. E., Urban, J. M. (2021). '*The Right to Contest AI*'. 121 Colum L Rev 1957. https://www.columbialawreview.org accessed 7 December 2025.

Limantė, A. (2024). '*Bias in Facial Recognition Technologies Used by Law Enforcement: Understanding the Causes and Searching for a Way Out*'. 42 (2) *Nordic Journal of Human Rights 115*. https://www.tandfonline.com accessed 7 December 2025.

Tracol, X. (2025). '*The Use of Facial Recognition Technologies by Law Enforcement Authorities in the US and the EU: Towards a Convergence on Regulation?*' TechReg 289.

BOOKS, REPORTS, OTHER PUBLICATIONS

Advisory Committee on Evidence Rules, *Agenda Book for Committee Meeting, April 19 2024* (2024). https://www.uscourts.gov accessed 7 December 2025.

European Union Agency for Fundamental Rights, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement* (FRA, November 2019). https://fra.europa.eu accessed 7 December 2025.

Garrett, B. L., Rudin, C. (2023). '*Right to a Glass Box: Explainability and Transparency in Criminal Justice Algorithms*' (SSRN Working Paper №4361462). https://ssrn.com accessed 7 December 2025.

Institute for Development of Freedom of Information (IDFI), Institute for Development of Freedom of Information (IDFI), Massive surveillance of protesters and the inadequate response of the Personal Data Protection Service, https://idfi.ge accessed 7 December 2025.

Scirica, A. J. '*Preface: The Judges' Book*' in *The Judges' Book: Creating a Fairer, More Effective and More Responsive Judiciary* (2020) 1. https://repository.uclawsf.edu accessed 7 December 2025.

US Government Accountability Office, *Biometric Identification Technologies: Considerations to Address Information Gaps and Other Stakeholder Concerns*, GAO-24-106293 (April 2024). https://www.gao.gov accessed 5 December 2025.

JUDICIAL PRACTICE

JUDGMENTS OF THE EUROPEAN COURT OF HUMAN RIGHTS (ECTHR)

Al-Khawaja and Tahery v United Kingdom (2011), 54 EHRR 23.

Glukhin v Russia, App no 11519/20 (ECtHR, 4 July 2023).

Podchasov v Russia, App no 33696/19 (ECtHR, 7 February 2023).

DECISIONS OF THE COURTS OF THE UNITED STATES

Frye v United States 293 F 1013 (DC Cir 1923).

Daubert v Merrell Dow Pharmaceuticals 509 US 579 (1993).

General Electric Co v Joiner 522 US 136 (1997).

Kumho Tire Co v Carmichael 526 US 137 (1999).