

სადოკუმენტო ინტელექტის სისტემების გამოყენება საქართველოში

კანონმდებლობა და პრაქტიკა

თბილისი, 2021



ინფორმაციის თავისუფლების
განვითარების ინსტიტუტი

ICNL

INTERNATIONAL CENTER
FOR NOT-FOR-PROFIT LAW

კვლევა დაფინანსებულია არაკომერციული სამართლის საერთაშორისო ცენტრის (ICNL) მიერ. ინფორმაციის თავისუფლების განვითარების ინსტიტუტი (IDFI) მადლობას უხდის ICNL-ს კვლევის მომზადებაში მხარდაჭერისთვის. ICNL შესაძლოა არ იზიარებდეს მასში გამოთქმულ მოსაზრებებს. მის შინაარსზე მთლიანად პასუხისმგებელია IDFI.

ხელოვნური ინტელექტის
სისტემების გამოყენება
საქართველოში

კანონმდებლობა და პრაქტიკა

ავტორები: დავით ერისთავი; გიორგი დავითაძე

რედაქტორები: ლევან ავალიშვილი; თეონა ბურაძე

შინაარსი

შესავალი	7
მეთოდოლოგია	8
1. საჯარო ინფორმაციის მოთხოვნების შედეგად მიღებული ინფორმაციის განხორციელებული ანალიზი	10
2. საჯარო დანახაბულებების მიერ ხელოვნური ინტელექტის გამოყენების დადასტურებული შემთხვევები და მათი აღწერილობა	13
2.1. შსს - საექსპერტო-კრიმინალისტიკური დეპარტამენტის სახის ამომცნობი სისტემა ...	13
2.2. შსს - სსიპ საზოგადოებრივი უსაფრთხოების მართვის ცენტრი (112) - სანომრე ნიშნების და სახის ამომცნობი სისტემა	14
2.2.1. შსს-ს მიერ ქვიკიანი და ზოგადი ხედვის კამერებიდან მოპოვებული ინფორმაციის დამუშავება	14
2.2.2. „ქვიკიანი“ და ზოგადი ხედვის კამერებით სანომრე ნიშნების ამოცნობის სისტემა და სახის ამომცნობი სისტემა	17
2.2.3. სამინისტროს მიერ ვიდეო-სამეთვალყურეო სისტემის გამოყენების კანონიერება - სახელმწიფო ინსპექტორის სამსახურის მიერ შინაგან საქმეთა სამინისტროს შემომწოდების შედეგები	19
2.3. საქართველოს პროკურატურა - IBM i2 ხელოვნური ინტელექტის შემცველი ანალიტიკური პროგრამული უზრუნველყოფა	22
2.4. სსიპ - საქართველოს ტურიზმის ეროვნული ადმინისტრაცია - სენტიმენტების ავტომატური ანალიზი (“Emotions Are Georgia”)	23
2.5. სსიპ - განათლების მართვის საინფორმაციო სისტემა - მონაცემთა ასოციაციური ანალიზი	24
2.6. სსიპ - განათლების ხარისხის განვითარების ეროვნული ცენტრი - DLP და მთარგმნელობითი მეხსიერების მოდული	24

3. ხელოვნური ინტელექტის ადგილი საქართველოს სამართლებრივ წესრიგში -----	26
4. საქართველოს ეროვნული ბანკის ძალისხმევა საფინანსო სექტორის რეგულირების თვალსაზრისით -----	28
5. ხელოვნური ინტელექტი უნდა კასუსობდეს კანონმდებლობის მოთხოვნებს -----	29
6. ხელოვნური ინტელექტის გამოყენება და გამჭვირვალობა -----	30
7. ხელოვნური ინტელექტის თავსებადობა დემოკრატიული და სამართლებრივი სახელმწიფოს პრინციპებთან -----	32
8. საჯარო დანახაბულებებში დანერგული ხელოვნური ინტელექტის სისტემებიდან მომდინარე საფრთხეები -----	34
დასკვნა -----	37



შესავალი

ტექნოლოგიურმა განვითარებამ არსებითად გაზარდა ხელოვნურ ინტელექტზე დაფუძნებული სერვისების შექმნისთვის საჭირო ტექნიკური თუ პროგრამული საშუალებების ხელმისაწვდომობა. ხელოვნურ ინტელექტს გააჩნია ფაქტობრივად ყველა სამუშაო თუ ბიზნეს პროცესის მართვის ტრადიციული მიდგომების სასიკეთოდ გარდაქმნის პოტენციალი. არა-კომერციული სამართლის საერთაშორისო ცენტრის მიერ დაფინანსებული პროექტის - „[გამჭვირვალობისა და ეთიკური სტანდარტების ხელშეწყობა ხელოვნური ინტელექტის \(AI\) გამოყენებაში](#)“ - ფარგლებში, IDFI-მ მიზნად დაისახა საჯარო სექტორში ხელოვნური ინტელექტის მოქმედი სისტემების შესწავლა. ჩვენ განსაკუთრებულ ყურადღებას გავამახვილებთ საქართველოში საჯარო დაწესებულებების მიერ აღნიშნული ტექნოლოგიური შესაძლებლობის გამოყენების თვალსაზრისით არსებულ გამოწვევებზე.

საჯარო სექტორში ხელოვნური ინტელექტის (AI) სისტემების გამოყენებას მნიშვნელოვანი სარგებლის მოტანა შეუძლია გადაწყვეტილების მიღების პროცესის გამარტივების, მომსახურების მიწოდების გაუმჯობესებისა და სხვა მრავალი ინოვაციური მიდგომების დანერგვის კუთხით. თუმცა, ხელოვნური ინტელექტით სარგებლობა არაერთ რისკს წარმოშობს. მისი გამოყენება დაკავშირებულია გამჭვირვალობის, ანგარიშვალდებულების, გამოსატვის თავისუფლების, პირადი ცხოვრების დაცვის უფლების თვალსაზრისით არსებულ გამოწვევებთან. ამასთან, ისეთ ქვეყნებში, როგორცაა საქართველო, სადაც შედარებით სუსტია ძალოვანი სტრუქტურების მიმართ არსებული საზედამხედველო მექანიზმები და არსებობს კითხვები სასამართლოს დამოუკიდებლობასთან დაკავშირებით, ხელოვნური ინტელექტის თანმხლები რისკების დაბალანსების პრობლემა მომეტებული კრიტიკულობით ვლინდება.

კვლევის ძირითად ნაწილში საჯარო დაწესებულებების მიერ ხელოვნური ინტელექტის გამოყენების თაობაზე მოპოვებული ინფორმაცია, განხილულია ეთიკური ხელოვნური ინტელექტის საბაზისო სტანდარტებისა და საქართველოს კანონმდებლობის ძირითადი პრინციპების პარალელურად.



აეთოოლოოია

სახელმწიფო უწყებების მიერ ხელოვნური ინტელექტის გამოყენების თაობაზე არაერთ პრაქტიკულ თუ სამართლებრივ პრობლემასთან არის დაკავშირებული. მაგალითად, არ არსებობს ხელოვნური ინტელექტზე დაფუძნებული ინფორმაციული სისტემების ერთიანი რეესტრი, ხელოვნური ინტელექტის ნორმატიული დეფინიცია ან/და მასთან სპეციალური კანონმდებლობა.

საჯარო დაწესებულებაში ხელოვნური ინტელექტის გამოყენების შესაძლო შემთხვევების იდენტიფიცირების მიზნით, IDFI გამოიყენა საჯაროდ ხელმისაწვდომი ინფორმაცია, რომელიც მიანიშნებდა, რომ შესაბამისი დაწესებულება იყენებდა ხელოვნური ინტელექტის შემცველ სერვისებს. ამასთან, ჩვენ ინფორმაცია მოვითხოვეთ ორგანოებიდან, რომელთა ფუნქციებიდან გამომდინარე, მაღალი იყო ალბათობა, რომ სარგებლობდნენ სამიზნე ტექნოლოგიური საშუალებით. საჯარო დაწესებულებების იდენტიფიცირების შემდგომ, IDFI-მ მათ შესაბამისი საჯარო ინფორმაციის მოთხოვნით მიმართა. ინფორმაციის მოთხოვნის წერილები გაიგზავნა 54 უწყებაში.

აღსანიშნავია, რომ საქართველოს კანონმდებლობა არ განსაზღვრავს ხელოვნური ინტელექტის ცნებას. იმავდროულად, ყოველთვის არ არის ნათელი ზღვარი ხელოვნურ ინტელექტსა და სხვა ტიპის ფუნქციურ ალგორითმებს შორის.¹ ამ ბუნდოვანების გასაქარწყლებლად და არასწორი ინფორმაციის მიღების ალბათობის შესამცირებლად, საჯარო ინფორმაციის გამოთხოვამდე IDFI-მ შესაბამისი საჯარო დაწესებულების წარმომადგენლებთან გამართა შეხვედრა, რომლის ერთერთი მიზანი იყო საჯარო ინფორმაციის მოთხოვნის წინასწარ გაცნობა, რათა მაქსიმალურად ყოფილიყო უზრუნველყოფილი ზუსტი პასუხების მიღება.

¹ ალგორითმი არის პროგრამული ინსტრუქციების კრებული, რომელიც მონაცემების დამუშავების შედეგად ავტომატურ რეჟიმში იღებს გადაწყვეტილებებს. ხელოვნური ინტელექტი კი უფრო ფართო ცნებაა და მოიაზრებს ალგორითმების ნაკრებს. ამგვარი სისტემები, პროგრამის მიერ დამუშავებული მონაცემების საფუძველზე, ადამიანის ჩარევის გარეშე, თავად ქმნიან საკუთარ ალგორითმებს შეყვანილი მონაცემებისა და მონაცემების დამუშავების შედეგად გამოვლენილი ახალი გარემოებების მიხედვით (მანქანური სწავლება).

საჯარო ინფორმაციის მოთხოვნის პარალელურად ჩვენ შევისწავლეთ ხელოვნური ინტელექტის მარეგულირებელი ნორმატიული ბაზა. სახელდობრ, მართალია საქართველოში არ არსებობს საჯარო დაწესებულებების მიერ ხელოვნური ინტელექტის შემცველი პროგრამული სერვისების მარეგულირებელი სპეციალური კანონმდებლობა, თუმცა საქართველოს კონსტიტუცია ისევე, როგორც სხვა საკანონმდებლო აქტები ადგენს არაერთ ნორმატიულ მოთხოვნას, რომლებიც საჯარო დაწესებულების მიერ ხელოვნური ინტელექტის გამოყენებაზე გავრცელდება.



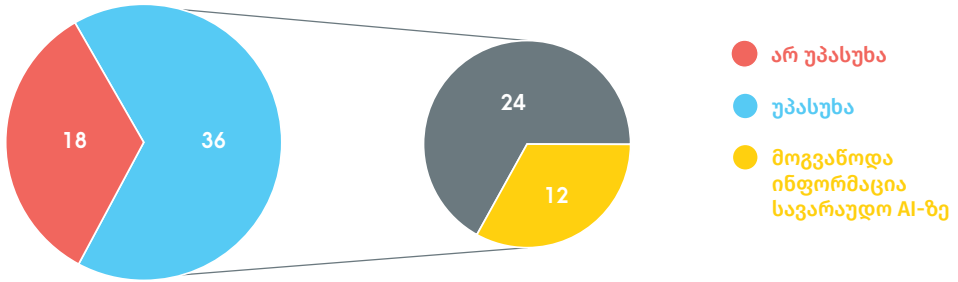
1. საჯარო ინფორმაციის მოთხოვნის შედეგად მიღებული ინფორმაციის განმარტებული ანალიზი

იდენტიფიცირებული 54 საჯარო დაწესებულებიდან, IDFI-მ გამოითხოვა მათ მიერ შექმნილი, აგრეთვე მათ სარგებლობაში არსებული ინფორმაციული სისტემების, პროგრამული საშუალებების და ხელოვნური ინტელექტის სისტემების შესახებ ინფორმაცია. თუმცა, კვლევის პროცესში აქცენტი გაკეთდა ხელოვნური ინტელექტის შემცველ პროგრამებზე. კერძოდ, IDFI-მ საჯარო დაწესებულებებიდან მოითხოვა შემდეგი ინფორმაცია:

1. პროგრამული საშუალების დასახელება, დანიშნულება, შექმნილი და მომხმარებელი;
2. აღწერილობა, პარამეტრები, მის მიერ დაყენებული შედეგები და მისი გამოყენება გადაწყვეტილების მიღების პროცესში;
3. მომხმარებლის სახელმძღვანელო/ინსტრუქცია, აგრეთვე, ტექნიკური სახელმძღვანელო;
4. პროგრამული საშუალების გამოყენების მარეგულირებელი სამართლებრივი აქტები;
5. ეთიკისა და პერსონალური მონაცემების დამუშავების სტანდარტების დაცვის წესები;
6. პროგრამის ფუნქციონირების შესახებ ჩატარებული აუდიტის ანგარიში და დასკვნა.

IDFI-მ კვლევის ფარგლებში გაგზავნილ 54 მოთხოვნაზე პასუხი მიიღო 36 უწყებიდან. მათგან მხოლოდ 12-მა უწყებამ გასცა ინფორმაცია მათ მიერ გამოყენებულ პროგრამულ უზრუნველყოფაზე, ხოლო ნაწილმა ინსტიტუტს აცნობა, რომ ხელოვნური ინტელექტის სისტემებს არ იყენებენ. სამიზნე უწყებების მნიშვნელოვანმა ნაწილმა არ უპასუხა საჯარო ინფორმაციის მოთხოვნის წერილს, ხოლო მიღებული პასუხების უმრავლესობა შემოიფარგლა მხოლოდ იმის აღნიშვნით რომ უწყებაში ხელოვნური ინტელექტის გამოყენება არ ხდება. მსგავსმა პასუხებმა, რამდენიმე შემთხვევაში აღძრა ეჭვი, რომ დაწესებულებებმა ისარგებლეს ტერმინის „ხელოვნური ინტელექტი“ შინაარსობრივი ბუნდოვანებით და თავი აარიდეს ინფორმაციის გამჟღავნებას.

მოთხოვნა გაიზარდა სულ 54 საჯარო დაწესებულებაში



ხელოვნური ინტელექტის სისტემების და სხვა ავტომატიზებული პროგრამული უზრუნველყოფების ერთმანეთისგან გამიჯვნის სირთულიდან გამომდინარე, კვლევის ფარგლებში ცალკეული უწყებებიდან მივიღეთ ინფორმაცია მათ მიერ გამოყენებულ ისეთ პროგრამულ საშუალებებზეც, რომლებიც არ შეიცავენ ხელოვნური ინტელექტის ელემენტებს, თუმცა გამოირჩევიან ავტომატიზების მაღალი ხარისხით. ასეთის მაგალითია შემოსავლების სამსახური, რომელსაც დანერგილი აქვს საბაჟო მონაცემთა ავტომატიზებულ სისტემას (ASYCUDA), დღგ-ს უკან დაბრუნების სისტემა და ელექტრონული განცხადებების დამუშავების სისტემა. საჯარო ინფორმაციის მოთხოვნის პირველ და მეორე პუნქტებზე (ე.ი. პროგრამების დასახელება და ზოგადი აღწერა) პასუხი მიღებულია 12 უწყებიდან. მათგან, 8 უწყებამ მოგვანოდა ინფორმაცია, მათ მიერ გამოყენებული ისეთ პროგრამულ საშუალებებზე, რომელთა მახასიათებლებიც არ ემთხვევა ხელოვნურ ინტელექტზე დაფუძნებულ სისტემებს. საჯარო დაწესებულებებიდან მიღებული პასუხების ანალიზის შედეგად, ხელოვნური ინტელექტის გამოყენება დადასტურდა 4 უწყებაში, ხოლო საქართველოს პროკურატურის მიერ ხელოვნური ინტელექტის გამოყენების თაობაზე ინფორმაცია, ხელმისაწვდომი გახდა საჯარო წყაროებიდან.

დაწესებულებები, რომლებიც იყენებენ ხელოვნურ ინტელექტის შემცველ სისტემებს:

- 1 საქართველოს შინაგან საქმეთა სამინისტრო და მის მმართველობაში შემავალი სსიპ - საზოგადოებრივი უსაფრთხოების მართვის ცენტრი 112
- 2 საქართველოს გენერალური პროკურატურა
- 3 საქართველოს ტურიზმის ეროვნული ადმინისტრაცია
- 4 სსიპ - განათლების მართვის საინფორმაციო სისტემა
- 5 სსიპ - განათლების ხარისხის განვითარების ეროვნული ცენტრი

ხელოვნური ინტელექტის გამოყენების 4 დადასტურებული შემთხვევიდან მომხმარებლის სახელმძღვანელო და შესაბამისი ინფორმაციული სისტემების მარეგულირებელი აქტები მოგვანოდა მხოლოდ განათლების ხარისხის განვითარების ეროვნულმა ცენტრმა, ხოლო სისტემის გამოყენების ეთიკისა და პერსონალური მონაცემების დაცვის სტანდარტებზე ინფორმაცია გაგვიზიარა მხოლოდ განათლების ხარისხის განვითარების ეროვნულმა ცენტრმა და ტურიზმის ეროვნულმა ადმინისტრაციამ. აღსანიშნავია, რომ პროგრამის ფუნქციონირების შესახებ ჩატარებული აუდიტის ანგარიში და დასკვნა არც ერთი უწყებისგან არ იქნა მიღებული, მათი ნაწილის ცნობით, აღნიშნული სისტემების და პროგრამების ფუნქციონირების აუდიტი არ ჩატარებულა, ხოლო დანარჩენებმა პუნქტი უპასუხოდ დატოვეს.²

2 აღსანიშნავია, რომ სახელმწიფო ინსპექტორის სამსახურმა 2019 წელს შეისწავლა საქართველოს შინაგან საქმეთა სამინისტროში ე.წ. „ჭკვიანი“ კამერების საშუალებით ადმინისტრაციულ სამართალდარღვევების დაფიქსირების პროცედურა. აღნიშნული შემოწმების დასკვნა IDFI-მ გამოითხოვა ინსპექტორის სამსახურისგან და კვლევის ფარგლებში გთავაზობთ მის მიმოხილვას.



2. სავარო დაწესებულების მიერ ხელმოწერილი ინტელექტის გამოყენების დადასტურებული შედეგები და მათი აღწერილობა

კლევის სამიზნე უწყებებიდან მხოლოდ რამდენიმე იყენებს ხელოვნურ ინტელექტზე დაფუძნებულ ალგორითმებს. მათგან შედარებით მაღალი კომპლექსურობით გამოირჩევა საქართველოს შინაგან საქმეთა სამინისტროს სისტემაში შემავალი დაწესებულებების სისტემები.

2.1

შს - საქსავარო-კრიმინალისტიკური ლაბორატორიის სახის ამოცნობის სისტემა

სამინისტროს საექსპერტო-კრიმინალისტიკურ დეპარტამენტში ფუნქციონირებს სახის ავტომატიზებული ამოცნობის, **Papillon Systems**-ის მიერ ლიცენზირებული აპლიკაცია POLY-FACE, რომლის შესყიდვა განხორციელდა 2013 წელს, „შპს მაი მობაილ + ისგან“, ხოლო შემდგომ 3-ჯერ მოხდა განახლების შესყიდვა 2017, 2018 და 2019 წლებში, რის შედეგადაც პროგრამას დაემატა 3D ფოტორობოტის შექმნის, ვიდეო-ანალიზის და მანქანური სწავლების „Deep Learning“ ფუნქციები. შესყიდვების საერთო ღირებულებამ ჯამში 460,576 ლარი შეადგინა. პროგრამა წარმოადგენს ჰაბიტუსკოპიურ საიდენტიფიკაციო სისტემას, რომელიც **სახის ამოცნობას ახორციელებს ორი ნიმუშის ერთმანეთთან შედარების საფუძველზე, მათ შორის, შესაძლოა გამოყენებულ იქნას სუბიექტური პორტრეტები (ფოტორობოტები).**

უწყების ინფორმაციით, პროგრამა გამოიყენება საინფორმაციო-ანალიტიკური დეპარტამენტის მიერ, სამინისტროს წინაშე მდგარი ამოცანების შესაბამისად, მათ შორის რეგისტრირებული დანაშაულის გამოძიების პროცესის ინფორმაციული უზრუნველყოფისა და სისხლისსამართლებრივი პროცედურების განხორციელების მიზნით. Papillon Systems-ის სათაო ოფისი მდებარეობს რუსეთში და მათი პროგრამული უზრუნველყოფის პროდუქტები **ფაქტობდ გავსცელებულია** რუსულ ძალოვან სტრუქტურებში, თურქეთში, ინდოეთში, ნიგერიაში და რამდენიმე პოსტ-საბჭოთა სახელმწიფოში.

შინაგან საქმეთა სამინისტროს სსიპ საზოგადოებრივი უსაფრთხოების მართვის ცენტრის - „112“-ის ბაზაზე დანერგულია სახელმწიფო სანომრე ნიშნისა და პიროვნების სახის ამომცნობი პროგრამული უზრუნველყოფა: - სახელმწიფო სანომრე ნიშნის ამომცნობი პროგრამის მწარმოებელია საერთაშორისო კომპანია „ISS“ - **ინტელექტუალური უსაფრთხოების სისტემები**, რომელიც აწარმოებს მრავალგვარ ციფრულ პროდუქტებს. ხოლო, სახის ამომცნობი პროგრამის მწარმოებელს წარმოადგენს იაპონური კომპანია - „NEC“. სამინისტროს ინფორმაციის თანახმად, ზემოაღნიშნული ორივე პროგრამა გამოიყენება ადმინისტრაციული სამართალდარღვევების დაფიქსირების, საზოგადოებრივი წესრიგის დაცვის, პირის უსაფრთხოებისა და საკუთრების დაცვის, ასევე საგამოძიებო მოქმედებების ხელშეწყობისთვის. დამატებით აღსანიშნავია, რომ NEC-ის სახის ამომცნობი პროგრამა, POLYFACE-ისგან განსხვავებით, **ინტეგრირებულია ქვეყნის ტერიტორიაზე დამონტაჟებულ ვიდეო-კამერათა ქსელთან და მოქმედებს რეალურ დროში, აფიქსირებს ვიდეო მასალაზე ასახული პირების ბიომეტრიული მონაცემებს და ახდენს მათ შედარებას ძებნილი პირების მონაცემთა ბაზასთან.**³

უშუალოდ საქართველოს შინაგან საქმეთა სამინისტროს მიერ მოწოდებული ინფორმაცია არის ზოგადი და არ იძლევა სრულს სურათს ჭკვიანი კამერების სრული პოტენციალის ან/და ამ პოტენციალის ათვისებული ნაწილის თაობაზე. თუმცა, ამის თაობაზე შედარებით მეტ მონაცემს გვაძლევს პროგრამული უზრუნველყოფის მწარმოებლების საჯაროდ ხელმისაწვდომის რესურსები და სახელმწიფო ინსპექტორის სამსახურის მიერ შინაგან საქმეთა სამინისტროში ჩატარებული ინსპექტირების თაობაზე მიღებული გადაწყვეტილების⁴ ერთობლივი ანალიზი.

საქართველოს შინაგან საქმეთა სამინისტრო იყენებს ორი ტიპის „ჭკვიან“ და ზოგადი ხედვის კამერებს. 112-ის მონაცემებით, საქართველოს მასშტაბით 4,705 ვიდეოკამერაა განთავსებული, რომელთაგან 1,745 არის ნომრის ამომცნობი (ე.წ) ხოლო 2,960 არის ზოგადი

3 სისტემის ფუნქციონირების შესახებ ამ დასკვნას არ ამყარებს შინაგან საქმეთა სამინისტროდან მიღებული ოფიციალური დოკუმენტები. თუმცა, მათ წარმომადგენლებმა ეს ინფორმაცია დაადასტურეს სატელეფონო ზარის საშუალებით. გარდა ამისა, ეს ფაქტი განმარტებულია ერთ-ერთ პრესრელიზში, რომელიც გამოქვეყნდა სამინისტროს ვებ-გვერდზე. [nbi.gov.ge](#)

4 სახელმწიფო ინსპექტორის სამსახურის 2019 წლის 27 ივნისის Nგ-1/222/2019 გადაწყვეტილება „საქართველოს შინაგან საქმეთა სამინისტროს შემოწმების დასრულების შესახებ“.

ხედვის კამერა.⁵ აღსანიშნავია, რომ 2020 წლის 10 დეკემბერს, შინაგან საქმეთა სამინისტრომ 417,800 ლარად შეიძინა კიდევ 500 ზოგადი ხედვის კამერა რომელთა განთავსება, ხელშეკრულების მიხედვით, სავარაუდოდ, 2021 წლის მარტში დასრულდება.⁶

კამერათა ტექნიკური აღწერა მიუთითებს, რომ მათ აქვთ მაღალი გარჩევადობის კამერები, რაც ბუნებრივია გაადვილებს მიღებული გამოსახულების ვიდეო ანალიტიკური პროგრამით გადამუშავებას. აღსანიშნავია, რომ იგივე დგინდება სახელმწიფო ინსპექტორის სამსახურის გადანყვეტილებით. კერძოდ, ინსპექტირებისას მითითებულ იქნა, რომ როგორც ქვიანი, ისე ზოგადი ხედვის ქსელური კამერები დღე-ღამის ნებისმიერ დროს იძლევა მაღალი გარჩევადობის (რეზოლუციის) გამოსახულების მიღების შესაძლებლობას.

როგორც ქვიანი, ისე ზოგადი ხედვის კამერები გამოიყენება ადმინისტრაციულ სამართალდარღვევათა დასაფიქსირებლად. პირველ შემთხვევაში, ადმინისტრაციული სამართალდარღვევის დაფიქსირება ხდება ავტომატურად. მეორე შემთხვევაში, სამართალდარღვევა ფიქსირდება 112 ცენტრის ოპერატორების მიერ „არავტომატური გზით.“⁷

აღსანიშნავია, რომ არც შინაგან საქმეთა სამინისტროს და არც 112-ის ვებგვერდზე არ იძებნება დეტალური ინფორმაცია, კამერების საშუალებით მიღებული მონაცემების დამუშავების თაობაზე. თუმცა, აღნიშნულის შესახებ მნიშვნელოვან ინფორმაციას გვაწვდის სახელმწიფო ინსპექტორის ზემოთმოყვანილი გადანყვეტილება.

სახელმწიფოს ინსპექტორის გადანყვეტილებიდან ირკვევა, რომ სამართალდარღვევის ავტომატური დაფიქსირებისას, ქვიანი კამერა ვიდეო ანალიტიკური პროგრამის მონაცემთა ბაზაში ასახავს დამრღვევი ავტოსატრანსპორტო საშუალების სახელმწიფო სანომრე ნიშანს და უნიკალური ID-ს, აგრეთვე სამართალდარღვევის დაფიქსირების მაიდენტიფიცირებელ სხვა მონაცემებს.⁸ იდენტიფიცირებული შემთხვევა გადამისამართდება სამართალდარღვევების ერთიან ბაზაში, სადაც ავტომატურად ივსება დაფიქსირებულ ადმინისტრაციულ სამართალდარღვევასთან დაკავშირებული სხვადასხვა მონაცემები.⁹ აღსანიშნავია, რომ სამართალდარღვევათა ეს სისტემა დაკავშირებულია შსს მომსახურების სააგენტოს მონაცემთა ბაზებთან და მისგან ავტოსატრანსპორტო საშუალების შესახებ გარკვეული მონაცემები ავტომატურად ივსება.¹⁰

5 იხ. შინაგან საქმეთა სამინისტროს სსიპ საზოგადოებრივი უსაფრთხოების მართვის ცენტრი 112-ის *მონაცემები*.

6 იხ. *ხელშეკრულება*. მაღალია ალბათობა, რომ ეს კამერები ჯერ კიდევ არ არის დაინსტალირებული და უახლოეს პერიოდში კამერების რაოდენობა 5,000 გადააჭარბებს.

7 შინაგან საქმეთა სამინისტროს სსიპ საზოგადოებრივი უსაფრთხოების მართვის ცენტრის „112“ ვებგვერდიდან ირკვევა, რომ ქვიანი კამერებს შეუძლიათ ავტომატურად დააფიქსირონ შემდეგი სამართალდარღვევები „წითელ შექინთანზე გავლა; ორმაგი ღერძულა საზის გადაკვეთა; მუნიციპალური ტრანსპორტის ზოლში მოძრაობა; მოძრაობის სანინალმდეგო მიმართულებით გადაადგილება; დაშვებული ჩიქქარის გადაჭარბება.“

8 სამართალდარღვევის ჩადენის თარიღს და დროს; სამართალდარღვევის ტიპს; კამერის კოორდინატებს; იმ სერვერის დასახელებას რომელზეც მოხდა მონაცემების დამუშავება და დამრღვევი ავტოსატრანსპორტო საშუალების ფოტოს ბმულს.

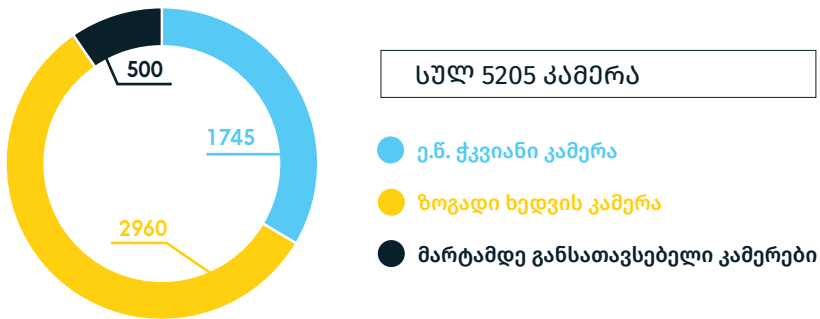
9 ადმინისტრაციული სამართალდარღვევის ადგილი, თარიღი და საქართველოს ადმინისტრაციულ სამართალდარღვევათა კოდექსის შესაბამისი მუხლი.

10 შსს მომსახურების სააგენტოს მონაცემთა ბაზიდან ავტომატურად ივსება ავტოსატრანსპორტო საშუალების მოდელის, ფერისა და მფლობელის შესახებ ველები.

ანალოგიური პროცედურა ხორციელდება ზოგადი ხედვის კამერით სამართალდარღვევის ფაქტის დაფიქსირების შემთხვევაშიც. თუმცა, ნაცვლად ავტომატური მეთოდისა, სამართალდარღვევის ფაქტის გამოვლენა ხორციელდება ადამიანური რესურსის გამოყენებით (ოპერატორის მიერ). სხვაგვარად, მონაცემთა დამუშავების ავტომატიზაციის ხარისხი არის იგივე, გამონაკლისია უშუალოდ სამართალდარღვევის დაფიქსირების მომენტი. აღსანიშნავია, ზოგადი ხედვის კამერის საშუალებით დაფიქსირებისას გამოიყენება „იგივე ვიდეო ანალიტიკური პროგრამა, რომელიც უზრუნველყოფს ქვიანი კამერების ფუნქციონირებას“¹¹ სხვაგვარად, როგორც ქვიანი, ისე ზოგადი ხედვის კამერებით სამინისტროს მიერ მიღებული ვიდეო-მონაცემები მუშავდება, ერთიანი ანალიტიკური პროგრამით.

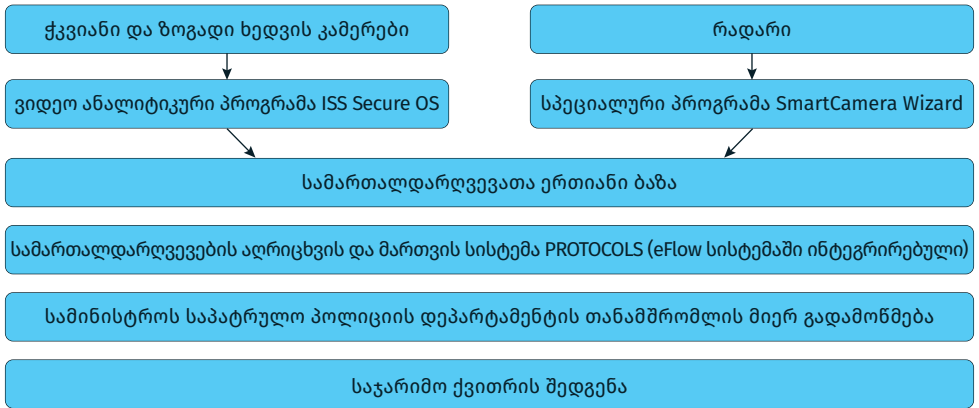
რადარის შემთხვევაში, ხორციელდება მხოლოდ მოძრაობის დადგენილი სიჩქარის გადაჭარბების ფაქტის დაფიქსირება, რის შემდეგაც **ფოტო მასალა და შესაბამისი მონაცემები ავტომატურად ინახება ფოტო-ვიდეო მასალის შემნახველ სერვერზე. აღნიშნული** ჩანაწერების ავტომატური დამუშავების შემდეგ (სპეციალური პროგრამა - SmartCamera Wizard-ის მეშვეობით), შესაბამისი მონაცემები თანდართულ ფოტო ფაილთან ერთად იტვირთება სამართალდარღვევების ერთიან ბაზაში.

საჯარიმო ქვითრის გამონერამდე, მონაცემებს ამოწმებენ საპატრულო პოლიციის დეპარტამენტის თანამშრომლები, კერძოდ ავტოსატრანსპორტო საშუალების სახელმწიფო სანომრე ნიშანი და ადმინისტრაციული სამართალდარღვევის ფაქტი ემთხვევა თუ არა დოკუმენტზე თანდართულ ფოტო/ვიდეო მასალაზე ასახულ სამართალდარღვევის ფაქტს. ცდომილების არარსებობის შემთხვევაში, საპატრულო დეპარტამენტის თანამშრომლები, სამართალდარღვევას საბოლოოდ აფიქსირებენ და ადგენენ შესაბამის საჯარიმო ქვითარს.



მითითებული მონაცემებიდან გამოსაყოფია, რომ ქვიანი კამერების მიერ მიღებული გადაწყვეტილებები (დაფიქსირებული შემთხვევები) ექვემდებარება წინასწარ გადამოწმებას. სხვაგვარად, ხელოვნური ინტელექტის სისტემის მიერ მიღებული გადაწყვეტა არის საბოლოო და ექვემდებარება წინასწარ ადამიანურ კონტროლს.

¹¹ ინსპექტორის გადაწყვეტილება გვ. 6.



2.2.2 „ჭკვიანი“ და ზოგადი ხედვის კამერებით სასაზღვრო ნიშნების ამოცნობის სისტემა და სახის ამოცნობის სისტემა

ჭკვიანი კამერების პოტენციალის ასათვისებლად მხოლოდ ამგვარი კამერების ქონა საკმარისი არაა. მართალია, ამგვარ ვიდეო-სამეთვალყურეო საშუალებას შესწევს ფიზიკურ გარემოზე დაკვირვებით მეტი ელექტრონული მონაცემის მიღების უნარი, თუმცა თუ მისი მენეჯმენტი სათანადო პროგრამული საშუალებით არ ხდება, თითქმის სრულად იკარგება ის პოტენციალი, რომელიც ჭკვიან კამერებს გააჩნიათ. სხვაგვარად, პრაქტიკული თვალსაზრისით, „ჭკვიან კამერას ჭკვიანად აქცევს სათანადო პროგრამული უზრუნველყოფა“, რომელიც ხელოვნურ ინტელექტზე დაფუძნებულ ალგორითმებს იყენებს. ამასთან, საკმარისად განვითარებული პროგრამული უზრუნველყოფას, ვიდეო ანალიტიკურ სისტემას სათანადო რეზოლუციის მქონე ნებისმიერი კამერის ჭკვიან კამერად ქცევის პოტენციალი გააჩნია. მაგალითად, განვითარებული სახის ამოცნობის სისტემები¹² საერთოდ არ მოითხოვს, რომელიმე სპეციფიკური კამერის გამოყენებას.

შინაგან საქმეთა სამინისტროს ჭკვიანი კამერების სამართავი სისტემის თაობაზე საერთოდ არ მოუწოდებია ინფორმაცია. თუმცა მან სანომრე ნიშნების ამოცნობის კონტექსტში მითითება გააკეთა ISS მიერ შექმნილ ვიდეო ანალიტიკურ პროგრამაზე,¹³ ხოლო სახის ამოცნობის სისტემის კონტექსტში იაპონური ტექნოლოგიური კომპანიისგან შექმნილ სპეციალურ პროგრამულ უზრუნველყოფაზე.¹⁴

როგორც საჯაროდ ხელმისაწვდომი, ისე შსს-ის მიერ მოწოდებული ინფორმაციიდან ირკვევა,

12 მათ შორის ის სისტემა, რომელსაც შსს იყენებს.

13 Intelligence Security Systems (ISS), website: <https://issivs.com>.

14 <https://www.nec.com/en/>

რომ განსახილველი ვიდეო ანალიტიკური პროგრამული საშუალება გამოიყენება მხოლოდ სამართალდარღვევაში მონაწილე ავტომობილის სანომრე ნიშნების აღმოსაჩენად. აღნიშნული მოდული ISS Secure OS პროგრამის მხოლოდ ერთი კომპონენტია, რომელსაც მეტი შესაძლებლობები გააჩნია ვიდრე სამართალდარღვევის მომენტში ავტომობილის სანომრე ნიშნის ამოცნობა.¹⁵ კერძოდ, ISS-ის მიერ შემუშავებული License Plate Recognition (LPR/ANPR) იყენებს ჩაღმავებულ სწავლებაზე (deep learning) დაფუძნებულ ალგორითმს, რომელსაც შეუძლია ავტომობილი გაარჩიოს კამერაზე დაფიქსირებული სხვა ობიექტებისგან და ამოიცნოს ავტომობილის ნომერი. იმავდროულად, აღსანიშნავია მისი შემდეგი ფუნქციები:

- ა) ამ ალგორითმს ავტომობილის ნომრის ამოსაცნობად არ სჭირდება სპეციალიზებული კამერა. ნებისმიერი კამერა, რომლის გაფართოება აღემატება 1280x720 რეზოლუციას, გამოიყენება.¹⁶ სანიშნოდ, 2020 წლის 31 დეკემბრის ხელშეკრულების საფუძველზე, შინაგან საქმეთა სამინისტროს მიერ შესყიდული კამერების რეზოლუციაა 2048 x 1536;
- ბ) მანქანის ნომერს აფიქსირებს არამხოლოდ სამართალდარღვევის ჩადენისას, არამედ აქვს ავტომობილის ნომრით და სხვა მახასიათებლებით ძებნის ფუნქცია;
- გ) მას აქვს, საძიებო ავტომობილთა სხვადასხვა სიების დამატების (მაგალითად ძებნილი ავტომობილები) შესაძლებლობა. აგრეთვე, იძლევა ოპერატორებთან ავტომატური შეტყობინების გაგზავნის შესაძლებლობას სიაში აღმოჩენილი ავტომობილის თაობაზე;
- დ) პროგრამას აქვს ავტომობილის გადაადგილების მიმართულების წინასწარ განსაზღვრის ფუნქცია;
- ე) ანალიტიკური პროგრამა ინტეგრირებადია (მისი დაკავშირება შესაძლებელია) გარე მონაცემთა ბაზებთან, აგრეთვე მისი გამოყენება შესაძლებელია სხვა აპლიკაციებთან ერთად (API Support).

ეს არის მხოლოდ ნომრის ამომცნობი მოდულის ფუნქციების არასრული ჩამონათვალი. აღსანიშნავია, რომ საზოგადოებრივი უსაფრთხოების მართვის ცენტრი (112) ასევე იყენებს, მსოფლიოში წამყვანი კომპანიის (NEC) მიერ შემუშავებულ სახის ამომცნობ სისტემას. მწარმოებლის ვებგვერდიდან ირკვევა,¹⁷ რომ სახის ამომცნობი სისტემის ერთ-ერთ მთავარ ღირსებას მისი დახვეწილი ალგორითმი წარმოადგენს, რომელიც ხელოვნურ ინტელექტსა და მონაცემთა ანალიტიკაზეა დაფუძნებული. სახის ამომცნობი აღნიშნული სისტემის მთავარი ღირსშესანიშნაობებია:

- ა) სახის ამომცნობა შეუძლია, არამხოლოდ მაღალი გარჩევადობის გრაფიკული გამოსახულებებიდან, არამედ დაბალი ხარისხის ვიდეო/ფოტო მასალიდან (24 pixel). თუნდაც, ამოსაცნობ სუბიექტს ეხუროს ქედი, შარფი ან მოძრაობდეს.

¹⁵ ISS-ის მიერ შემუშავებული (License Plate Recognition (LPR/ANPR)). ვიდეო ანალიტიკის ამ კონკრეტული მოდულის შესაძლებლობები.

¹⁶ იხ. კამერის დეტალური ტექნიკური მონაცემები.

¹⁷ იხ. NEC ოფიციალურ ვებსაიტზე, განთავსებული ინფორმაცია, კომპანიის მიერ დამუშავებული სახის ამომცნობი სისტემის შესახებ.

ბ) წარმატებით მუშაობს, როგორც საზოგადოებრივი თავშეყრის ადგილებში და სხვადასხვა კამერებიდან მიღებული მონაცემების საფუძველზე ყოველწუთიერად ათასობით სახის სკანირება შეუძლია.

გ) გააჩნია პლანიმეტრიული ფოტოების (2D) სამგანზომილებიან (3D) სივრცეში გარდაქმნის შესაძლებლობა. გადაყვანის შემდგომ, ადამიანის თავის 3D გამოსახულებას აბრუნებს [360 გრადუსით] და ამ პროცესში ხელოვნურად ადებს სხვადასხვა განათებას, გამომეტყველებას და შედეგად თითქმის ყველა პირობებში 99% სიზუსტით იძლევა სახის ამოცნობის შესაძლებლობას.

სამწუხაროდ, შინაგან საქმეთა სამინისტროს არ მოუწოდებია დამატებითი ინფორმაცია აღნიშნული სახის ამოცნობი სისტემის გამოყენების თაობაზე. ეს ინფორმაცია არც საჯარო ხელმისაწვდომი წყაროებიდან ირკვევა.

2.2.3

სამინისტროს მიერ ვიდეო-საპოლიციური სისტემის გამოყენების კანონიერება – სახელმწიფო ინსპექციის სასახურის მიერ შინაგან საქმეთა სამინისტროს უპოვნების შედეგად

2019 წელს სახელმწიფო ინსპექტორის სამსახურმა განახორციელა შინაგან საქმეთა სამინისტროს შემოწმება. ინსპექტირების საგანი არ ყოფილა სახის ამომცნობი ანალიტიკური სისტემის გამოყენება, თუმცა იგი მოიცავს სამინისტროს მიერ ISS Secure OS ვიდეო ანალიტიკური პროგრამის საშუალებაში დაცულ ვიდეო ჩანაწერთა დამუშავების კანონიერებას. ინსპექტირების შედეგები შემაშფოთებელია, იმდენად რამდენადაც, სახელმწიფო ინსპექტორის სამსახურმა ჩანაწერთა დამუშავების ფაქტობრივად ყველა ეტაპზე დაადგინა დარღვევა.

შემოწმების შედეგად, სახელმწიფო ინსპექტორმა აღმოაჩინა დარღვევები მონაცემების შენახვის ვადებთან დაკავშირებით. მონაცემები და ფოტო-ვიდეო მასალა, რომელიც უნდა წაშლილიყო დღეების ან თვეების განმავლობაში, ცალკეულ შემთხვევებში, წლობით ინახებოდა სერვერზე. პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონის თანახმად, მონაცემები შეიძლება შენახულ იქნეს მხოლოდ იმ ვადით, რომელიც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად. იმ მიზნის მიღწევის შემდეგ, რომლისთვისაც მუშავდება მონაცემები, ისინი უნდა დაიბლოკოს, წაიშალოს, განადგურდეს ან შენახულ უნდა იქნეს პირის იდენტიფიცირების გამომრიცხავი ფორმით, თუ კანონით სხვა რამ არ არის დადგენილი.

აღსანიშნავია, რომ შსს არ აღრიცხავდა ISS Secure OS ანალიტიკური პროგრამით/ხელოვნური ინტელექტის გამოყენებით მონაცემთა ბაზებში განხორციელებულ აქტივობებს. სხვაგვარად, შეუძლებელი იყო ხელოვნური ინტელექტის გამოყენების ინდივიდუალურ შემთხვევათა მართლზომიერების გადამოწმება (თრეინინგი). ეს განსაკუთრებით პრობლე-

მერი იმ გარემოების გათვალისწინებით, რომ ანალიტიკურ პროგრამით მუშავდება არამხოლოდ სამართალდარღვევის დაფიქსირების მომენტის არამედ სახელმწიფოს მასშტაბით დამონტაჟებული ყველა ჭკვიანი თუ ზოგადი კამერის უწყვეტი ჩანაწერები.

შემომწების მიგნებების საფუძველზე, სახელმწიფო ინსპექტორის გადანყვეტილებით, შინაგან საქმეთა სამინისტროს დაევალა:

- ვიდეო ანალიტიკურ პროგრამაში, ისევე როგორც აღნიშნული პროგრამის მონაცემთა ბაზაში არსებული მონაცემების მიმართ ყველა მოქმედების აღრიცხვა.
- ზოგადი ხედვის კამერით ადმინისტრაციული სამართალდარღვევის მანუალური მეთოდით დაფიქსირების დროს ცენტრის ოპერატორის ლოკალურ პერსონალურ კომპიუტერში შენახული ფოტო/ვიდეო ფაილების მიმართ არსებული ყველა მოქმედების აღრიცხვა.
- ცენტრალურ ვიდეო სერვერებზე განთავსებული ვიდეო ჩანაწერების მიმართ განხორციელებული ყველა მოქმედების აღრიცხვა.
- ფოტო/ვიდეო მასალების შემნახველ სერვერზე განთავსებული ფოტო/ვიდეო ფაილების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა.
- სამართალდარღვევების ერთიანი ბაზის ვებ-აპლიკაციაში, ისევე როგორც აღნიშნული ვებ-აპლიკაციის მონაცემთა ბაზაში არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა.
- დოკუმენტრუნვის ელექტრონულ სისტემაში დაფიქსირებული ადმინისტრაციული სამართალდარღვევის ამსახველი ჩანაწერების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა.
- ფოტო/ვიდეო ტექნიკით მოპოვებული მონაცემების შენახვის ვადების განსაზღვრა და განსაზღვრული ვადის შემდგომ მონაცემების ნაშლა/დეპერსონალიზაცია.

IDFI-ის მიერ შინაგან საქმეთა სამინისტროსთან ხელოვნური ინტელექტის თაობაზე გაგზავნილი წერილით, მოთხოვნილ იქნა, მათ შორის, სამართლებრივი აქტები/სახელმძღვანელოები ან ინსტრუქციები, რომელიც უწყებაში ხელოვნური ინტელექტის გამოყენებას შეეხებოდა. ერთადერთი სამართლებრივი აქტი, რომელიც მეტნაკლებად დეტალურად არეგულირებს ვიდეოსამეთვალყურეო სისტემის გამოყენების საკითხს არის საქართველოს შინაგან საქმეთა მინისტრის **2017 წლის 28 ივნისის N328 ბიძანება**, რომელიც არეგულირებს „საქართველოს პოლიციის სარგებლობაში არსებულ შესაბამისი ამოსაცნობი ნიშნების არმქონე ავტოსატრანსპორტო საშუალებაზე ავტომატური ფოტო- და ვიდეოტექნიკის, არასტაციონარული (მოძრავი) სიჩქარის მზომი ხელსაწყოს განთავსებისა და გამოყენების, აგრეთვე მონაცემთა დამუშავების პირობებსა და პროცედურებს“. შსს მოწოდებული ინფორმაციიდან ირკვევა, რომ ეს ბრძანება სამინისტროს მიერ სამხრე კამერებით, ავტოსატრანსპორტო საშუალებებზე, გზებზე და გარე პერიმეტრზე განთავსებული კამერებით მოპოვებული ინფორმაციის დამუშავებას არეგულირებს. თუმცა, გასათვალისწინებელია ორი გარემოება, პირველი ეს ბრძანება შეეხება მხოლოდ სამეთვალყურეო სისტემის გამოყენებას უკონტაქტო პატრულირების (საგზაო მოძრაობის უსაფრთხოების უზრუნველყოფის) განხორციელების მიზნით. იგი საერთოდ არ არეგულირებს იგივე სისტემის გამოყენებას მაგ. დანაშაულის ან მისი მცდელობის დაფიქსირების, ძებნილი პირებისა

და ავტომობილების აღმოჩენის მიზნით, რაც თავის მხრივ „საზოგადოებრივი უსაფრთხოების მართვის ცენტრის 112-ის ფუნქციას წარმოადგენს. იმავდროულად, N328 ბრძანების მე-7 მუხლის მე-2 პუნქტის თანახმად, „სამინისტრო ვალდებულია უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების/ინფორმაციის მიმართ შესრულებული ყველა მოქმედების აღრიცხვა“. სამინისტროს ეს ვალდებულება 2017 წლიდან გააჩნია, თუმცა როგორც სახელმწიფო ინსპექტორის სამსახურის მიერ 2019 წლის შემოწმების შედეგად გამოვლინდა, შსს საერთოდ არ აღრიცხავდა დამუშავებული ჩანაწერების მიმართ შესრულებულ მოქმედებებს. ეს შესაძლებელია გამოწვეული იყოს იმით, რომ საჯარო ინფორმაციაზე გამცემმა პირმა გააკეთა სამართლებრივი აქტის არასწორად იდენტიფიცირება და ბრძანების მოქმედება საერთოდ არ ვრცელდება ქვიანი და ზოგადი ხედვის კამერებით მოპოვებული ინფორმაციის დამუშავებაზე, მათ შორის ISS Secure OS-ის ანალიტიკური პროგრამის გამოყენებით დამუშავებაზე. ანდა, როგორც მინიმუმ, 2019 წლამდე სამინისტრო არღვევდა მისსავე დადგენილ ინფორმაციის დამუშავების წესს. შსს მიერ იდენტიფიცირებული ყველა სხვა სამართლებრივი აქტი არის ზოგადი, საუკეთესო შემთხვევებში, მხოლოდ ინფორმაციის ვიდეო ანალიტიკური პროგრამული საშუალებით დამუშავების ზოგად სამართლებრივ საფუძველს და მიზნებს განსაზღვრავს. იგი საერთოდ არ შეეხება ამგვარი ანალიტიკური პროგრამების გამოყენების წესს და მათი გამოყენებით შექმნილი რისკების პრევენციას.

ჩვენთვის უცნობია რამდენად განხორციელდა სამინისტროში სახელმწიფო ინსპექტორის სამსახურის აღნიშნული რეკომენდაციების აღსრულება, თუმცა, იმის გათვალისწინებით რომ სამინისტროს არცერთი სათანადო სამართლებრივი აქტი არ მოუწოდებია, შეგვიძლია, ვივარაუდოთ, ISS Secure OS-ის გამოყენების პრაქტიკის მნიშვნელოვნად არ შეცვლილა.

საქართველოს გენერალურმა პროკურატურამ 2020 წლის 22 ოქტომბერს საჯარო ინფორმაციის მოთხოვნის წერილზე პასუხად IDFI-ს აცნობა, რომ მის სარგებლობაში არსებულ რესურსებში არ გამოიყენება ხელოვნურ ინტელექტზე დაფუძნებული ალგორითმები და სისტემები. თუმცა, გენერალური პროკურორის პირველმა მოადგილემ საპროკურორო საბჭოსთვის საქართველოს პროკურატურის საქმიანობის 2020 წლის ანგარიშის წარდგენისას განაცხადა, რომ *საქართველოს პროკურატურაში დაიწყო ხელოვნური ინტელექტის გამოყენება გამოძიების პროცესში*. განმეორებით გაგზავნილი მოთხოვნის შემდგომ, 2021 წლის 5 თებერვალს საქართველოს პროკურატურამ მოგვანოდა ინფორმაცია, რომ უწყებაში დანერგეს IBM2 ანალიტიკური პროგრამა.

საქართველოს გენერალური პროკურატურის 2020 წლის ანგარიშის თანახმად, საქართველოში ამერიკის შეერთებული შტატების საელჩოს მხარდაჭერით და ხელშეწყობით, საქართველოს პროკურატურაში დაინერგა IBM I2 ანალიზის პროგრამა. IBM I2 პროგრამა მომხმარებელს აძლევს განსხვავებული ფორმატის, სხვადასხვა წყაროდან მოპოვებული საბანკო და სატელეფონო კომუნიკაციის ამონაწერების და სხვა ინფორმაციის პროგრამაში ინტეგრაციის შესაძლებლობას. პროგრამა ახდენს მონაცემების ანალიზს, დახარისხებას, სტრუქტურის ანალიზს და ავტომატიზაციის საშუალებით, დროის მცირე მონაკვეთში, დამუშავებული, მშრალი მონაცემების ვიზუალიზაციით ორ ან რამდენიმე ქსელს შორის კავშირის გამოვლენას, შაბლონური ქცევების და ლატენტური საფრთხის აღმოჩენას და დანაშაულებრივი ქმედებების მიდევნებას. სისტემაში მონაცემების მიღება-დამუშავება შესაძლებელია რეალურ დროშიც. ანგარიშის თანახმად პროგრამული უზრუნველყოფა გამოიყენება როგორც დანაშაული პრევენციის, ისე დანაშაულის დროულად გამოძიებისთვის.

საქართველოს პროკურატურის მიერ გავრცელებულ ინფორმაცია არ შეიცავს დეტალურ მონაცემებს პროგრამის ანალიტიკური შესაძლებლობების თაობაზე. IDFI-მ შეისწავლა მწარმოებლის მიერ აღნიშნულ პროგრამის შესახებ საჯაროდ ხელმისაწვდომი ინფორმაცია¹⁸ და გაეცნო სისტემის სადემონსტრაციო პრეზენტაციას. შესწავლის შედეგად გამოვლინდა, რომ პროგრამული უზრუნველყოფას სხვადასხვა ტიპის განვითარებული ანალიტიკური შესაძლებლობები გააჩნია. მათგან გამოსაყოფია:

- მონაცემთა მარტივი ინტეგრაცია: სწრაფად და მარტივად უკავშირდება შიდა და გარე მონაცემთა ბაზებს;
- პროგრამას შესწევს დიდ მონაცემთა შორის დაფარული მახასიათებლების და კავშირების (find hidden patterns and connections) გამოვლენის შესაძლებლობა;
- გეო-ლოკაციური გამოძიება: ინტეგრირდება რუკებთან და შესაძლებელს ხდის გამოძიების გეოგრაფიულ ვიზუალიზაციას.

18 IBM Security Solution Brief Investigative analysis in Law Enforcement საგამოძიებო ორგანოებისთვის <https://www.ibm.com/downloads/cas/OW3KJN1Y>. დოკუმენტის სანახავად, შეიძლება მოგთხოვოთ ავტორიზაცია.

- სოციალური ქსელის ანალიზი: ანალიტიკოსებს საშუალებას აძლევს შეისწავლონ და გააანალიზონ მონაცემთა სტრუქტურები, ქსელში კომუნიკაციური ნაკადები, განსაზღვრონ გამოძიების კონტურები და ინტერესის მთავარი ობიექტები (to identify key players and lines of investigation).

გენერალური პროკურორის მოადგილის თქმით, აღნიშნული პროგრამული უზრუნველყოფა პროკურორებსა და გამომძიებლებს საგამომძიებო თუ ოპერატიული გადაწყვეტილებების დროულ მიღებაში ეხმარება და დროის მცირე მონაკვეთში ეფექტიანი შედეგის მიღების შესაძლებლობას აძლევს. ამ ეტაპზე, ინსტიტუტისთვის, სამწუხაროდ, უცნობია, თუ რა ხარისხით და კონკრეტულად რა მიმართულებით ხდება აღნიშნულ პროცესში ხელოვნური ინტელექტის გამოყენება. მაგალითად, რომელ მონაცემთა ბაზებთანაა დაკავშირებული ეს პროგრამული უზრუნველყოფა? რას გულისხმობს მისი გამოყენება დანაშაულის პრევენციის მიზნით? დაშვება ამ პროგრამული უზრუნველყოფის გამოყენებაზე და სხვა მსგავსი საკითხები.¹⁹

2.4

სსიპ - საქართველოს ტერიტორიული ერთეულის ადმინისტრაცია - საინფორმაციო ავტომატური ანალიზი ("Emotions Are Georgia")

ტურიზმის ეროვნულმა ადმინისტრაციამ 2017 წელს, სარეკლამო კომპანია „ვინდფორსს“ ერთჯერადად დაუკვეთა მარკეტინგული კამპანია „Emotions are Georgia“, რომელიც შპს „პულსარი“-ს მიერ შეიქმნა ხელოვნური ინტელექტის გამოყენებით. პროექტის ფარგლებში მოხდა საქართველოში ტურისტულად მყოფი ადამიანების მიერ სოციალურ ქსელებში გამოქვეყნებული საჯარო პოსტების ანალიზი და კატეგორიზაცია. ხელოვნური ინტელექტის გამოყენება განხორციელდა ორი მიმართულებით: საჯარო ფოტოებზე გამოსახული საგნების, ლოკაციების, პეიზაჟებისა და სხვა ობიექტების ამოცნობით და კატეგორიზაციით, და საჯარო პოსტებში მოცემული ტექსტების ანალიზით მათში მოცემული სენტიმენტების დასადგენად (პოზიტიური, ნეგატიური, ნეიტრალური). საბოლოო პროდუქტი წარმოადგენს 2017 წლის განმავლობაში საქართველოში მყოფი ტურისტების მიერ გამოქვეყნებული საჯარო პოსტების კრებულს, რომელშიც **დავებითი ემოციის მქონე ვიზუალები და ტექსტური მასაღაა წაჩმოდ-გენილი**. ტურიზმის ადმინისტრაციის ცნობით, პირადი მონაცემების უსაფრთხოების მიზნით, შემუშავებული იქნა ორი დოკუმენტი, რის საფუძველზეც მოხდა მონაცემების გამოყენება. დოკუმენტებში აღნიშნულია, რომ ადმინისტრაციამ მოიპოვა კამპანიაში ჩართული ყველა პოსტის ავტორის წერილობითი თანხმობა.

¹⁹ IDFI საქართველოს პროკურატურას განმეორებით მიმართა საჯარო ინფორმაციის მოთხოვნით და აგრძელებს აღნიშნული საკითხის შესწავლას.

2.5

სსიპ - განათლების მართვის საინფორმაციო სისტემა - ომასვათა ასოციაციური ანალიზი

განათლების მართვის საინფორმაციო სისტემა იყენებს მონაცემთა ვიზუალიზაციისა და ანგარიშების ანალიტიკურ სისტემა **Qlik sense-ს**. მასში ინტეგრირებულია ზოგადი განათლების მართვის საინფორმაციო სისტემა და ანგარიშგება (მოსწავლეებისა და მასწავლებლების რაოდენობა სხვადასხვა ქრილში სასწავლო წლების მიხედვით, სკოლის მიტოვების მაჩვენებლები, და ა.შ). პროგრამის ოფიციალური ვებგვერდიდან ცნობილია, რომ მას აქვს ხელოვნურ ინტელექტზე დაფუძნებული, მონაცემთა ასოციაციური ანალიზის ფუნქცია, თუმცა უწყებას არ მოუწოდებია დეტალური ინფორმაცია იმის შესახებ, თუ როგორ ხდება აღნიშნული ფუნქციის გამოყენება. უწყების ცნობით, შპს ენ ჯი თი გრუპთან გაფორმებულ იქნა ხელშეკრულება მონაცემთა ვიზუალიზაციის, ანალიზისა და ანგარიშების პროგრამული უზრუნველყოფის თანმდევი მომსახურებით. სახელშეკრულებო ღირებულება შეადგენდა 80,268.00 ლარს. ამასთან, შპს ენ ჯი თი გრუპთან გაფორმებულია ხელშეკრულება მართვის სისტემის მოხმარებაში არსებული ვიზუალიზაციის, ანალიზისა და ანგარიშების ანალიტიკური სისტემა Qlik Sense-ის Pro User-ის ერთწლიანი ტექნიკური მხარდაჭერის მომსახურებისა და საპროექტო დავალებების დანერგვის სამუშაოების შესყიდვაზე, სახელშეკრულებო ღირებულება შეადგენს 22,390 ლარს.

2.6

სსიპ - განათლების ხარისხის განვითარების ეროვნული ცენტრი - DLP და მთარგმნელობითი მანქანის მოქმედება

განათლების ხარისხის განვითარების ეროვნული ცენტრი სარგებლობს პროგრამა Office 365-ით. აღნიშნული გახლავთ კომპანია Microsoft-ის პროგრამების ნაკრები, რომელიც უზრუნველყოფს კოლაბორაციას, საოფისე პროგრამულ უზრუნველყოფას და სხვადასხვა ავტომატიზაციის ონლაინ სერვისებს. სისტემაში ჩაშენებულია ხელოვნურ ინტელექტზე დაფუძნებული DLP მოდული. ეს გახლავთ მონაცემთა გაჟონვის სანინააღმდეგო მოდული, რომელიც ავტომატური სწავლების რეჟიმის მეშვეობით (Machine Learning) აიდენტიფიცირებს სენსიტიურ და პირად მონაცემებს, ახდენს მათ კლასიფიკაციას და გაჟონვის საფრთხის დაფიქსირების შემთხვევაში, ახორციელებს ავტომატურ დაშიფვრას (encryption). მისი საშუალებით ასევე ხორციელდება არასანქცირებული შეღწევებისგან ავტომატური ბლოკირება და სხვადასხვა უსაფრთხოების პროცესების ავტომატიზაცია.

ცენტრის ინფორმაციის თანახმად, აღნიშნული პლატფორმა ორგანიზაციას ეხმარება ყოველდღიურად გამოყენებადი სერვისების (როგორცაა Email, Teams, SharePoint და სხვ.) უსაფრთხოების უზრუნველყოფაში. უკანონო ქმედებების ფაქტის დადგენის შემთხვევაში, პროგრამა აგზავნის შეტყობინებას ტექნიკურად პასუხისმგებელ პირთან, რაც ეხმარება უწყებას სხვადასხვა გადაწყვეტილების მიღებაში, როგორცაა მაგალითად - მომხმარებლის დაბლოკვის საკითხი.

ხელოვნური ინტელექტის კომპონენტი ასევე გააჩნია განათლების ხარისხის განვითარების ეროვნული ცენტრში დანერგილ მთარგმნელობით კომპიუტერულ პროგრამას *SDL Trados Studio*, ვინაიდან მას გააჩნია ეგრეთ წოდებული „თარგმნის მეხსიერება“ (Translation Memory), რომელიც ავტომატურად ივსება მთარგმნელ-რედაქტორების მიერ ახალი ტერმინების დამატებით და შემდგომ ახორციელებს სათარგმნი წინადადებების სხვადასხვა შეთავაზებების ავტომატურ მიწოდებას (auto-suggest) მთარგმნელებისათვის, რაც მანქანური სწავლების მარტივი მაგალითია.

მთარგმნელობითი კომპიუტერული პროგრამა SDL Trados Studio ბრიტანული კომპანია SDL-ის ბრენდს ეკუთვნის. ცენტრის თქმით, მათ მიერ საერთაშორისო ექსპერტებისათვის ითარგმნება უმაღლესი სასწავლო დაწესებულებების მიერ წარმოდგენილი სააკრედიტაციო და საავტორიზაციო დოკუმენტები, ასევე ხდება საერთაშორისო ექსპერტების ჩართულობით მომზადებული ავტორიზაციისა და აკრედიტაციის დასკვნების თარგმნა ინგლისურიდან ქართულ ენაზე უმაღლესი საგანმანათლებლო დაწესებულებებისათვის. ცენტრის თანახმად, თარგმნის პროცესი მნიშვნელოვნად გამარტივდა სერვერული პროგრამის შექმნის შემდეგ, იმავე რაოდენობის დოკუმენტების თარგმნა 15-ის მაგივრად მხოლოდ 7 თარჯიმნის მიერ ხორციელდება. ცენტრმა ასევე მოგვანოდა დაკავშირებული ნორმატიული მასალები, სადაც აღწერილია თუ რა შემთხვევებში ახორციელებს ცენტრი მთარგმნელობით მომსახურებას. თუმცა, პროგრამული უზრუნველყოფის შესახებ დეტალური ინფორმაცია არ გვხვდება. დამატებით აღსანიშნავია, რომ ცენტრის ცნობით, შიდა აუდიტის სამსახურს არ ჩაუტარებია ინფორმაციული სისტემების/პროგრამული საშუალებების/ხელოვნური ინტელექტის სისტემის ფუნქციონირების აუდიტორული შემოწმებები.



3. ხელოვნური ინტელექტის ადგილი საქართველოს სამართლებრივ წესრიგში

საჯარო დაწესებულებების მიერ ხელოვნური ინტელექტის გამოყენების პრაქტიკის შესწავლის შემდგომ, გვსურს მოკლედ მიმოვიხილოთ ეთიკური ხელოვნური ინტელექტის მას-სიათებელი რამდენიმე საბაზისო პრინციპი სამართლებრივი სახელმწიფოს ძირითადი დებულებების პარალელურად.

ტერმინი „ხელოვნური ინტელექტი“ საქართველოს საკანონმდებლო მაცნეზე განთავსებულ ნორმატიულ აქტებში მხოლოდ **სამგან ახის ნახსენები**. არცერთი მათგანი არ არის საკანონმდებლო აქტი. ამ ნორმატიული აქტებიდან ორი მიმართულია კერძო საფინანსო სექტორში²⁰ ხელოვნური ინტელექტზე დაფუძნებული სერვისების შემუშავება/შეთავაზების საკითხების რეგულირებისკენ, ხოლო ერთი მათგანი „ხელოვნური ინტელექტის“ როგორც მაღალი ტექნოლოგიის სტატუს აღიარებს სამეწარმეო (Startup) საქმიანობის სფეროში. საქართველოს კანონმდებლობა არაფერს ამბობს საჯარო დაწესებულებების მიერ ხელოვნური ინტელექტის სისტემების გამოყენების თაობაზე. თუმცა, ეს არ ნიშნავს, რომ საჯარო დაწესებულებებს ხელოვნური ინტელექტის გამოყენება ეკრძალებათ. საქართველოს სამართლებრივ სივრცეში ხელოვნური ინტელექტის ადგილის განსაზღვრად, მნიშვნელოვანია ზოგადად გავიაზროთ რა არის ხელოვნური ინტელექტი.

ხელოვნური ინტელექტის განსაზღვრების თაობაზე საერთაშორისოდ აღიარებული და შეჯერებული კონცეფცია არ არსებობს.²¹ თუმცა, არსებულ განსაზღვრებათა აბსოლუტური უმრავლესობა ხელოვნური ინტელექტის ფუნქციონალურ გაგებას ეფუძნება. სახელდობრ, ეს განმარტებები ხელოვნურ ინტელექტს სხვა ციფრული ალგორითმებისგან მისი შესაძლებლობებით (ავტონომიურობის ხარისხით და ადაპტირების უნარით) გამოარჩევს. ხელოვნური ინტელექტის სხვადასხვა დონეებიც ამავე კრიტერიუმით ხარისხდება. აქედან

20 ვგულისხმობთ საბანკო და სადაზღვეო სექტორს.

21 მითითება, რომ ხელოვნური ინტელექტის ეს განსაზღვრება არ მიემართება AI singularity-ის და საუბარია პრაქტიკულ ხელ

გამომდინარე, ხელოვნური ინტელექტი არის კომპიუტერული ალგორითმების ნაირსახეობა, ტექნოლოგიური განვითარების ერთერთი მთავარი მიღწევა, რომლის შესაძლებლობები მუდმივად იზრდება.

საქართველოს კანონმდებლობა არ უკრძალავს საჯარო დაწესებულებას სამსახურეობრივი უფლებამოსილების ეფექტურად განსახორციელებლად გამოიყენოს ტექნოლოგიური პროგრესი. პირიქით, ტექნოლოგიური მიღწევების საჯარო ადმინისტრირებაში კანონის შესაბამისად გამოყენება მისასალმებელია, რამდენადაც იგი მნიშვნელოვნად ამარტივებს იმ ლეგიტიმური მიზნების მიღწევას რისთვისაც შესაბამისი დაწესებულებაა შექმნილი. იმავდროულად, სამართლებრივი სახელმწიფოს მოთხოვნაა, რომ საჯარო დაწესებულების ნებისმიერი მოქმედება უნდა შეესაბამებოდეს კანონის მოთხოვნებს. აქედან გამომდინარე, იმ პირობებში, როდესაც საქართველოს კანონმდებლობა ხელოვნური ინტელექტის შემცველი სისტემების მიმართ სპეციფიკურ მოთხოვნებს არ განსაზღვრავს, მათი შექმნისა თუ გამოყენების კონკრეტული შემთხვევები მოწესრიგდება შესაბამისი სამართლებრივი ურთიერთობის მარეგულირებელი კანონმდებლობით. სახელდობრ, ხელოვნური ინტელექტის გამოყენება შესაძლებელია სხვადასხვა სამართლებრივ ურთიერთობებში არაერთი ერთმანეთისგან განსხვავებული მიზნების მისაღწევად. აქედან გამომდინარე, იმის მიხედვით, რომელი უფლება იზღუდება და როგორია შესაბამისი ურთიერთობის მომწესრიგებელი კანონმდებლობა ხელოვნური ინტელექტის გამოყენების თითოეული შემთხვევის მიმართ სხვადასხვა სამართლებრივი ნორმების მისადაგება იქნება საჭირო.

კვლევის ამ ნაწილში, საქართველოს სამართლებრივ წესრიგში დამკვიდრებულ ძირითად სამართლებრივ პრინციპებს, რომლებიც დაცული უნდა იქნეს საჯარო დაწესებულებების მიერ ხელოვნური ინტელექტის შემუშავებისას/გამოყენებისას და, რომლებიც, იმავდროულად ეთიკური ხელოვნური ინტელექტის განუყოფელი ელემენტებია. აგრეთვე, იმ საფრთხეებზე რომლებიც, საჯარო სექტორში ხელოვნური ინტელექტის დადასტურებული შემთხვევებიდან მომდინარეობს.



4. საქართველოს ეროვნული ბანკის ქალისხევა საფინანსო სექტორის რეგულირების თვალსაზრისით

ეროვნულმა ბანკმა ინსტიტუტს აცნობა, რომ უწყებაში არ იყენებენ ხელოვნური ინტელექტის სისტემებს. თუმცა, მნიშვნელოვანია ყურადღება გავამახვილოთ, ეროვნული ბანკის პრეზიდენტის მიერ 2020 წლის 17 აგვისტოს მიღებული N151/04 ბრძანებაზე. აღნიშნული ბრძანების მიზანია, მონაცემებზე დაფუძნებული სტატისტიკური, ხელოვნური ინტელექტის და მანქანური სწავლების მოდელების (შემდგომში – მოდელი) რისკების მართვის ჩარჩოს ჩამოყალიბებისა და მასთან დაკავშირებული რისკების ეფექტურად მართვის ხელშეწყობა. მისი მოქმედება ვრცელდება საფინანსო სექტორის წარმომადგენლებზე (მაგ.: კომერციული ბანკები, მიკროსაფინანსო ორგანიზაციები), აქამდე გატარებული ღონისძიებებით. აღნიშნული ბრძანება ხსენებულ სუბიექტებს სტატისტიკური, ხელოვნური ინტელექტის და მანქანური სწავლების სისტემების დანერგვისას განუსაზღვრავს ამ მოდელების შექმნის, აუტოსონიგის და გაშვება-განვითარების ეტაპებზე რისკების მართვის პრინციპებს და ადმინისტრაციულ-ორგანიზაციულ კონტროლის მექანიზმებს.

ეროვნულმა ბანკმა IDFI-ის აცნობა, რომ რამდენიმე კომერციულმა ბანკმა შეიმუშავა შემოსავლების შეფასების სტატისტიკური მოდელი, რომელიც გამოიყენება სესხის გაცემის პროცესში. აღნიშნული მოდელი ბანკს საშუალებას აძლევს შემოსავლის დამადასტურებელი საბუთების გარეშე, კლიენტის სხვა ინფორმაციაზე დაყრდნობით, შეაფასოს მისი შემოსავალი და მიიღოს გადაწყვეტილება სესხის გაცემის თაობაზე. ეროვნული ბანკის თანახმად, ექსპლუატაციის დაწყებამდე სუბიექტებმა წარადგინეს მოდელის სრული აღწერილობა და მონაცემების ნუსხა, რომლის მეშვეობითაც მოქმედებს ალგორითმი. ეროვნულმა ბანკმა გადახედა, შეაფასა და გარკვეული შეზღუდვები განუსაზღვრა სუბიექტებს. თუმცა პასუხში დაზუსტებული არ არის კონკრეტულად რა ტიპის შეზღუდვებზეა საუბარი.

კერძო, განსაკუთრებით საბანკო და სადაზღვეო სექტორში, აქტიურად მიმდინარეობს ხელოვნური ინტელექტის შემცველი სისტემების გამოყენება. ამ კვლევის მიზანი საჯარო სექტორის მიერ ხელოვნური ინტელექტის გამოყენების ანალიზია. თუმცა, ეროვნული ბანკის პრეზიდენტის მიერ 2020 წლის 17 აგვისტოს მიღებული N151/04 სახელმწიფოში ხელოვნური ინტელექტისა და მანქანური სწავლების გამოყენების რეგულირების პირველ მცდელობად უნდა ჩაითვალოს.



5. ხელშეწყობის ინტეგრირებული უნდა კანონმდებლის კანონმდებლობის მოთხოვნებს

საქართველოს კონსტიტუციის მე-4 მუხლის პირველი და მე-4 პუნქტების თანახმად, საქართველო არის სამართლებრივი სახელმწიფო, ხოლო სახელმწიფო ხელისუფლება ხორციელდება კონსტიტუციითა და კანონით დადგენილ ფარგლებში. სახელმწიფოს ძირითადი კანონის ეს დებულება სამართლებრივი სახელმწიფოს პრინციპის განამტკიცებს, რომელიც თავის მხრივ მოითხოვს, რომ სახელმწიფოს ნებისმიერი მოქმედება თავსებადი უნდა იყოს კანონმდებლობის მოთხოვნებთან. ბუნებრივია, ჩვენ ვერ დავფარავთ კანონიერების თვალსაზრისით არსებულ ყველა მოთხოვნას, რომელიც ხელოვნურ ინტელექტთან მიმართების გამოყენების პოტენციური გააჩნია, თუმცა ყურადღებას გავამახვილებთ ხელოვნური ინტელექტის კანონმდებლობის დარღვევით გამოყენების შემთხვევებზე.

ხელოვნური ინტელექტის გამოყენების კანონიერების კვლევისას, დარღვევები გამოვლინდა პირადი ცხოვრების/პერსონალური მონაცემების დაცვის თვალსაზრისით. სახელმწიფო, პერსონალურ მონაცემთა დაცვის ინსპექტორს საერთოდ არ შეუსწავლია, სახის ამომცნობი სისტემის გამოყენების საკითხი, თუმცა მან შსს ვიდეო სამეთვალყურეო სისტემების ფუნქციონირების ფაქტობრივად ყველა ეტაპზე გამოავლინა დარღვევა. იმავდროულად, მნიშვნელოვან კითხვები არსებობს შინაგან საქმეთა სამინისტროში ხელოვნური ინტელექტის დანერგვისა და გამოყენების კონსტიტუციურობის თაობაზე.

მოყვანილი შემთხვევა მიუთითებს, კანონმდებლობის მოთხოვნათა დაცვის საქმიანობაზე. კანონიერების მოთხოვნას არსებითი მნიშვნელობა აქვს თავად ხელოვნური ინტელექტის სისტემის გამოყენების სტაბილურობისთვისაც. კერძოდ, თუ ხელოვნური ინტელექტის შემუშავებისას საფუძვლად არ იქნება გათვალისწინებული კანონმდებლობის ყველა მოთხოვნა და ცვლად სამართლებრივ გარემოსთან მარტივად ადაპტაციის შესაძლებლობა, მნიშვნელოვნად შეფერხდება შესაბამისი ელექტრონული სისტემის გამოყენება და შეიძლება არაერთი ძვირადღირებული რეფორმა ჩავარდეს.



6. ხელოვნური ინტელექტის გამოყენება და გაუმჯობესება

ეთიკური ხელოვნური ინტელექტის მიმართ წაყენებულ მოთხოვნათაგან ერთ-ერთია მისი გამჭვირვალობა. კერძოდ, იგი უნდა იყოს ღია, ხოლო მისი მუშაობის პრინციპების უნდა იყოს ახსნადი და სამომხმარებლო ენაზე ინტერპრეტირებადი. გამჭვირვალობის გარეშე შეუძლებელი იქნება ხელოვნური ინტელექტის სისტემის სათანადო სამართლებრივი თუ ეთიკური აუდიტი.

საქართველოში არ არსებობს ხელოვნური ინტელექტის შემცველი სისტემების ერთიანი რეესტრი. საჯარო დაწესებულებების მიერ გამოყენებული ხელოვნური ინტელექტის შემცველი ალგორითმების თაობაზე ინფორმაციის მიღების ერთადერთი გზა მათი საჯარო ინფორმაციის სახით გამოთხოვაა.

აღსანიშნავია, რომ კვლევის მიმდინარეობისას დაფიქსირდა შემთხვევა, როდესაც საჯარო დაწესებულების არამეტუ ხელოვნური ინტელექტის ფუნქციონირების პრინციპები, შესაძლებლობები და მის მიერ დაყენებული სამართლებრივი შედეგები, არამედ თავად ამგვარი სისტემის არსებობა მიაჩნდა კონფიდენციალურ ინფორმაციად. კერძოდ, სსიპ ფინანსური მონიტორინგის სამსახურმა თავდაპირველად უარი განაცხადა ხელოვნური ინტელექტის შემცველი სისტემების თაობაზე ნებისმიერი ინფორმაციის მოწოდებაზე. სამართლებრივ საფუძვლად მან აღნიშნული ინფორმაციის კონფიდენციალურობა დაასახელა. წერილში მითითებული იყო, რომ სამსახური იყენებს მხოლოდ სპეციალიზებულ პროგრამულ საშუალებებს, რომელთა მუშაობის სპეციფიკა, ტექნიკური მახასიათებლები, არქიტექტურა ან/და მათში რეალიზებული ალგორითმები მკაცრად კონფიდენციალურია. IDFI-ის მიერ აღნიშნული პასუხის ადმინისტრაციული წესით გასაჩივრების შემდგომ, ჩატარდა ზეპირი განხილვა, სადაც საჯარო დაწესებულების მიერ გამოითქვა პოზიცია, რომ ინფორმაცია იყენებს თუ არა იგი ხელოვნური ინტელექტის შემცველ პროგრამულ საშუალებებს უნდა იყოს საიდუმლო. საბოლოოდ, ადმინისტრაციული საჩივრის განხილვის შემდგომ სსიპ ფინანსური მონიტორინგის სამსახურმა მოგვანოდა ინფორმაცია და აღნიშნა, რომ დაწესებულება ხელოვნური ინტელექტის სისტემებზე დაფუძნებულ სისტემებს არ იყენებს.

ხელოვნური ინტელექტის შემცველი სისტემების თაობაზე ინფორმაციის არარსებობა, შეუძლებელს ხდის მათზე, როგორც სამართლებრივი ისე საზოგადოებრივი კონტროლის განხორციელების შესაძლებლობას. მაგალითად, შსს გააჩნია სახის ამომცნობი სისტემა, რომელიც მსოფლიოში წამყვანი კომპანიის მიერ არის შემუშავებული და ყოველწუთიერად ათასობით მოქალაქის ბიომეტრიული მონაცემების გადამუშავება შეუძლია 99%-იანი სიზუსტით. საზოგადოებისთვის უცნობია, როგორ გამოიყენება ხელოვნური ინტელექტის შემცველი ეს პროგრამული უზრუნველყოფა. დაკავშირებულია თუ არა იგი საქართველოს მასშტაბით განთავსებულ ყველა კამერასთან? ინახავს თუ არა მუდმივ რეჟიმში ადამიანთა ბიომეტრიულ მონაცემებს? აგრეთვე სხვა რელევანტური საკითხები. ამგვარი ინფორმაციული ვაკუუმი ართულებს, როგორც საერთო სასამართლოსთვის მიმართვის და სამართლიანი სასამართლოს უფლებით ეფექტურად სარგებლობის შესაძლებლობას, ისე ეფექტურ კონტროლს შესაბამისი ინფორმაციული სისტემების კონსტიტუციურად და კანონიერად გამოყენების კონტროლს.



7. ხელოვნური ინტელექტის თავსებადობა დემოკრატიული და საპარტიდობრივი სახელმწიფოს პრინციპებთან

ამ მოთხოვნის უმთავრესი მიზანია ადამიანის ღირსების, თავისუფლების და ინფორმაციული თვითგამორკვევის უფლების პატივისცემა. კერძოდ, ხელოვნური ინტელექტის შემცველი სისტემების გამოყენების მოკლე ისტორიის მიუხედავად, მსოფლიოს პრაქტიკაში დადასტურდა მისი ბოროტად და დემოკრატიული სახელმწიფოს პრინციპებთან შეუთავსებელი გამოყენების არაერთი შემთხვევა.

განსაკუთრებულ ყურადღებას იმსახურებს სამართალდამცავი და უსაფრთხოების სექტორის ხელთ არსებული მონაცემთა ბაზების ხელოვნური ინტელექტის სისტემით დამუშავების რისკები. აღნიშნულის თვალსაჩინო მაგალითს წარმოადგენს შინაგან საქმეთა სამინისტროს ხელოვნურ ინტელექტზე დაფუძნებული ანალიტიკური შესაძლებლობის მუდმივი ზრდა, ამ პროცესებიდან მომდინარე რისკების დამბალანსებელი აუცილებელი მექანიზმების არარსებობის ფონზე.

რისკების ნათლად წარმოსადგენად, შეგვიძლია განვიხილოთ მონაცემთა ცენტრალური ბანკის მაგალითი. კერძოდ, სახელმწიფო უსაფრთხოების სამსახურის სსიპ - ოპერატიულ ტექნიკური სააგენტოს მიენიჭა მაიდენტიფიცირებელ მონაცემთა ცენტრალური ბანკის შექმნის უფლებამოსილება. „საჯარო სამართლის იურიდიული პირის – საქართველოს ოპერატიულ-ტექნიკური სააგენტოს შესახებ“ საქართველოს კანონის მე-11 მუხლის თანახმად, სააგენტო ქმნის მაიდენტიფიცირებელ მონაცემთა ცენტრალურ ბანკს. ამ მიზნით, იგი უფლებამოსილია „ქჭონდეს დისტანციური წვდომა ელექტრონული კომუნიკაციის კომპანიის ელექტრონული კომუნიკაციის მაიდენტიფიცირებელ მონაცემთა ბაზებზე და განახორციელოს მათი კოპირება და შენახვა“. აღსანიშნავია, რომ აღნიშნულ მონაცემთა ბანკში ინახება საქართველოში მოქმედი ელექტრონული კომუნიკაციის ყველა კომპანიის²² ინფრასტრუქტურის განხორციელებული საშუალებით ინტერნეტ თუ სატელეფონო კომუნიკა-

22. ³⁶⁰ პუნქტის თანახმად, ელექტრონული კომუნიკაციის კომპანია არის „ავტორიზებული პირი, რომლის საქმიანობის ან/და მომსახურების სახეა სატელეფონო ქსელებით ან/და ინტერნეტქსელებით უზრუნველყოფა ან/და მომსახურება“.

ციის მაიდენტიფიცირებელი მონაცემები. „ელექტრონული კომუნიკაციების შესახებ“ საქართველოს კანონის მე-2 მუხლის 3⁶² პუნქტის თანახმად, ელექტრონული კომუნიკაციების მაიდენტიფიცირებელი მონაცემები არის „მომხმარებლის მაიდენტიფიცირებელი მონაცემები; კომუნიკაციის წყაროს კვალის დადგენისა და იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის ადრესატის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის თარიღის, დროისა და ხანგრძლივობის იდენტიფიცირებისათვის საჭირო მონაცემები; კომუნიკაციის სახის იდენტიფიცირებისათვის საჭირო მონაცემები; მომხმარებლის კომუნიკაციის აღჭურვილობის ან შესაძლო აღჭურვილობის იდენტიფიცირებისათვის საჭირო მონაცემები; მობილური კომუნიკაციის აღჭურვილობის ადგილმდებარეობის იდენტიფიცირებისათვის საჭირო მონაცემები“.

სხვაგვარად, საქართველოში ერთიან მონაცემთა ბანკში ინახება საქართველოს მასშტაბით განხორციელებული ნებისმიერი სატელეფონო თუ ინტერნეტ კომუნიკაციის მაიდენტიფიცირებელი მონაცემები. აღსანიშნავია, რომ მონაცემთა ცენტრალური ბანკის არსებობის კონსტიტუციურობა საქართველოს საკონსტიტუციო სასამართლოში უკვე მეორედ არის გასაჩივრებული. სასამართლოს საბოლოო გადაწყვეტილება ამ საქმეზე ჯერ არ მიუღია, თუმცა ნიშანდობლივია, რომ საქართველოს ოპერატიულ ტექნიკურ სააგენტოს წარმომადგენელმა, საქმის არსებითი განხილვის სხდომაზე, მონაცემთა ცენტრალური ბანკის არსებობის ერთერთ საჭიროებად გამოყო მასში მართვის ავტომატური საშუალებების (ალგორითმების) გამოყენების ტექნიკური შესაძლებლობა.

აღნიშნული დანებსებულების მიერ მოწოდებული ინფორმაციიდან ირკვევა, რომ იგი არ იყენებს ხელოვნურ ინტელექტზე დაფუძნებულ სისტემას. თუმცა, მონაცემთა ცენტრალურ ბანკში არსებული ინფორმაციის ხელოვნური ინტელექტის სისტემის გამოყენებით გადამუშავება მნიშვნელოვნ საფრთხეს ქმნის დემოკრატიული სახელმწიფოსთვის.



8. საჯარო დაწესებულებაში დაწერვილი ხელოვნური ინტელექტის სისტემების სისტემების მოქმედებასა და მართვასთან დაკავშირებული რისკების მართვა

საჯარო დაწესებულებებში დაწერვილი ხელოვნური ინტელექტის საშუალებებიდან მომდინარე რისკების თაობაზე ნათელ წარმოდგენას გვიქმნის საქართველოს შინაგან საქმეთა სამინისტროს ხელთ არსებული ანალიტიკური სისტემები.

დღეის მდგომარეობით, ქვეყნის მასშტაბით დამონტაჟებული სამეთვალყურეო კამერების რაოდენობა **5,000-მდე აღწევს** და წლიდან წლამდე იზრდება, თუმცა კვლავ მწირი და ძალზედ ზოგადია სახის ამომცნობი ტექნოლოგიების მარეგულირებელი ნორმატიული მასალა. ქვეყნის კამერების მიერ მოპოვებული მონაცემების დამუშავების თაობაზე სამინისტროს მიერ მოწოდებულ მარეგულირებელ აქტებს შორის ფიგურირებს მხოლოდ ზოგადი აქტები, როგორცაა პოლიციის შესახებ კანონი, პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი და საქართველოს პოლიციის ეთიკის კოდექსი. როგორც ზემოთ აღვნიშნეთ, შემონების შედეგად, მხოლოდ პერსონალურ მონაცემთა დაცვის თვალსაზრისით, სისტემით მოპოვებული ვიდეოჩანაწერების დამუშავების ფაქტობრივად ყველა ეტაპზე გამოვლინდა დარღვევა. მათგან ზოგიერთი, ჩვენი მოსაზრებით, განზრახვის ელემენტებს შეიცავს. მაგალითად, შსს თანამშრომელთა მიერ მონაცემთა ბაზებში განხორციელებულ აქტივობების აღრიცხვის არარსებობა, სამართლებრივი და ტექნიკური თვალსაზრისით იმდენად წარმოდგენილი შეცდომაა, რომ აღძრავს განცდას ამ შეცდომის განზრახ დაშვების თაობაზე. განსაკუთრებით იმ ფონზე, რომ აღნიშნული სამინისტროს თანამშრომელთა რაოდენობისა და მისი საქმიანობის ფარულობის ხარისხის გათვალისწინებით, დასაქმებულთა მიერ ხელოვნური ინტელექტის სისტემების ბოროტად გამოყენების რისკი მაღალია. სანიმუშოდ იხ. სახელმწიფო ინსპექტორის სამსახურის გადაწყვეტილება, რომლითაც **დავითაშვილი შსს ეთიკის თანამშრომლის მიერ შეხვედრა თანამშრომლის (საკუთარი დის) დახმავებით, შსს მონაცემთა ბაზებიდან პერსონალურ მონაცემთა ახასამსახურებრივი მიზნებისთვის მოპოვების ფაქტი**. მონაცემთა ბაზებში განხორციელებული აქტივობების აღრიცხვის სისტემის არარსებობა განუზომლად ზრდის თანამშრომელთა მიერ შესაბამისი სისტემების როგორც არამართლზომიერი, ისე არასამსახურებრივი მიზნების გამოყენების რისკებს.

შსს ელექტრონულ რესურსებზე, ავტომობილის ნომრების ამომცნობი სისტემების ფუნქციონირების თაობაზე განთავსებული ინფორმაცია მხოლოდ ზოგადი ხასიათისაა. იგივე პრობლემაა შინაგან საქმეთა სამინისტროს მიერ მოწოდებულ წერილობით პასუხში. ხოლო ოფიციალური ინფორმაცია NEC-ის სახის ამომცნობი სისტემის გამოყენების თაობაზე არის შავი ყუთი, რომლის დახურულად არსებობა ადამიანის უფლებათა დარღვევის მნიშვნელოვან რისკებს შეიცავს.

შსს ყოველწლიურად ზრდის ვიდეო სათვალთვალო სისტემათა რაოდენობას და ვიდეო-ანალიტიკური შესაძლებლობას. რაც, ცალკე აღებული, პრობლემას არ წარმოადგენს. თუმცა, შსს-ში მიერ ხელოვნური ინტელექტის შემცველი სისტემების დანერგვა მიუთითებს, რომ სამინისტრო მათ ორდინალურ პროგრამულ უზრუნველყოფად განიხილავს და დაუბალანსებელი რჩება, გაზრდილი ანალიტიკური შესაძლებლობის ბოროტად გამოყენების საფრთხეები.

შედარებისთვის, ხელოვნურ ინტელექტზე დაფუძნებული ვიდეო-სამეთვალყურეო სისტემების პოტენციურ რისკებს ყველაზე ნათლად წარმოაჩენს ჩინეთის მაგალითი, სადაც სახელმწიფო სახის ამომცნობ ტექნოლოგიებს და ვრცელ ვიდეო-სამეთვალყურეო ქსელებს და განვითარებულ ანალიტიკურ პროგრამებს იყენებს მოქალაქეებზე მასიური დაკვირვების და სხვადასხვა დანაშაულის გამოვლენის მიზნით. აშშ-ის რამდენიმე [გიდი ქაქაქის](#) (მაგ.: სან ფრანცისკო, ბოსტონი, პორტლენდი) ადგილობრივმა კანონმდებლებმა სრულიად აკრძალეს ძალოვანი სტრუქტურების მიერ სახის ამომცნობი ტექნოლოგიების გამოყენება, გამოვლენილი საფრთხეების და რისკების შედეგად. დროებით, [5 წლიან აკრძალვას ევზოკავშირის განიხილავს](#), რათა კანონმდებლებს მიეცეთ ადეკვატური რეგულაციების შემუშავების დრო და საშუალება.

შსს პარალელურად, გასათვალისწინებელი ტურიზმის ეროვნული ადმინისტრაციის მიერ დაკვეთილი, სენტიმენტების ანალიზზე დაფუძნებული სისტემა. კერძოდ, ანალიტიკური ტექნოლოგიის გამოყენებით საჯარო პოსტებში სენტიმენტების ავტომატურად შეფასების შესაძლებლობა. ხელოვნური ინტელექტის ამგვარი სისტემის შექმნამ და პოლიტიკური პოსტების ანალიზმა შესაძლოა მნიშვნელოვანი გავლენა მოახდინოს ქვეყანაში მიმდინარე დემოკრატიულ პროცესებზე.

მიუხედავად იმისა რომ, ხელოვნური ინტელექტის გამოყენება მცირერიცხოვან დაწესებულებებში დადასტურდა, გამოიკვეთა საფრთხის შემცველი ტენდენცია. კერძოდ, სადაზვერვო (intelligence) ბუნების მქონე ორგანოებს (სახელმწიფო უსაფრთხოების სამსახური, ფინანსური მონიტორინგის სამსახური), რომელთაც თავიანთი ფუნქციებიდან გამომდინარე, წესით, მეტად უნდა ესაჭიროებოდეთ გაზრდილი ანალიტიკური შესაძლებლობები გარე საფრთხეების ეფექტური დადგენისა და რეაგირებისთვის, ხელოვნურ ინტელექტზე დაფუძნებული ანალიტიკური სისტემები საერთოდ არ გააჩნიათ. საპირისპიროდ, ხელოვნური ინტელექტის სისტემების დანერგვა აქტიურად მიმდინარეობს შსს-სა და პროკურატურაში.

ტექნოლოგიების გავრცელებასთან და განვითარებასთან ერთად, მნიშვნელოვანია აქტიური საჯარო დისკუსიის წამოწყება და პრევენციული რეგულაციების დანერგვა. საჯარო სექტორში

ხელოვნური ინტელექტის დანერგვით, გაზრდილი ანალიტიკური შესაძლებლობის ბოროტად გამოყენების რისკები უნდა დაბალანსდეს. როგორც ადამიანის ძირითადი უფლებების დაცვა ისე დემოკრატიული სახელმწიფოს პრინციპების რეალიზება მოითხოვს, რომ მეტი ინფორმაცია გახადოს ხელმისაწვდომი საჯარო სექტორში გამოყენებული ხელოვნური ინტელექტის სისტემებისა და მათი ფუნქციონირების პრინციპების თაობაზე. ამგვარი ინფორმაციის არარსებობის პირობებში, საზოგადოებას არ გააჩნია საკუთარი უფლებების ეფექტურად დაცვის შესაძლებლობა. მაგალითად, შეუძლებელი იმის გარკვევა, სახელმწიფოს მიერ შესყიდული სახის ამომცნობი სისტემის გამოყენების თაობაზე, შესაბამისად, არსებითად რთულდება სამართლიანი სასამართლოს უფლებით ეფექტურად სარგებლობა, ვინაიდან ინდივიდებს არ გააჩნია ინფორმაცია მათი ბიომეტრიული მონაცემების შესაძლო დამუშავებასთან დაკავშირებით.



დასკვა

ხელოვნური ინტელექტის სისტემების დანერგვა საქართველოს საჯარო სექტორში განვითარების სანყის ეტაპზე, თუმცა, კერძო სექტორში უკვე მრავლად გვხვდება აღნიშნული ტექნოლოგიის გამოყენების წარმატებული მაგალითები, დისტანციური ვერიფიკაციის სისტემები, დოკუმენტების ავტომატური იდენტიფიკაციის სისტემები, კომუნიკაციის ავტომატიზაციის პროგრამები და მრავალი სხვა საშუალებები. ეს სექტორი განსაკუთრებით მომგებიანი გახდა პანდემიის პირობებში, დისტანციურ სერვისებზე გაზრდილი მოთხოვნის შედეგად. შესაბამისად, უკვე თვალსაჩინოა თუ რა პოტენციალი აქვს ხელოვნური ინტელექტის ფართომასშტაბიან გამოყენებას სხვადასხვა პროცესებში ეფექტიანობის და ხარჯთეფექტურობის გაზრდის თვალსაზრისით. თუმცა, ასევე ანგარიშგასანევია ის რისკები, რაც შეიძლება წარმოიშვას სისტემის ბოროტად გამოყენების, ტექნიკური ხარვეზების და პერსონალური მონაცემების არასწორი მართვის შედეგად.



ხელოვნური ინტელექტი არ არის მორიგი დამხმარე ელექტრონული სისტემა. იგი არსებითად ზრდის სახელმწიფოს მმართველობით შესაძლებლობებს, შესაბამისად, იმატებს მისი არამართლობიერებად გამოყენების ცდუნება. ეს რისკი განსაკუთრებით მაღალია განვითარებადი დემოკრატიის ქვეყნებში. კვლევის შედეგად, გამოვლინდა, რომ სამართალდამცავი უწყებები არის საჯარო სექტორის ერთადერთი მიმართულება სადაც სტაბილურად მიმდინარეობს ხელოვნური ინტელექტის დანერგვის პროცესი, რაც ირიბად ამ რისკების რეალურობაზე მიუთითებს.



წინამდებარე კვლევის შედეგად, თვალსაჩინო ხდება, სამიზნე უწყებებში ხელოვნური ინტელექტის სისტემების მარეგულირებელი ნორმატიული აქტების და ეთიკური ნორმების განმსაზღვრელი დოკუმენტების არარსებობა. იმისათვის, რომ საჯარო სექტორში აღნიშნული ტექნოლოგიებისგან მაქსიმალური სარგებლის მიღება შეძლოს, ტექნოლოგიურ მზაობასთან ერთად, კრიტიკულად მნიშვნელოვანია გამოყენებული სისტემების შესახებ ინფორმაციის ხელმისაწვდომობა და საჯაროობა, რათა საზოგადოებას ჰქონდეს ინფორმაცია სისტემების ფუნქციონირების თავისებურებების შესახებ, გამოირიცხოს მიკერძოების რისკები, შესა-

ძლებელი იყოს გარე დამკვირვებლის მიერ სისტემის შესაძლო ხარვეზებზე მსჯელობა და ნდობის მაღალი ხარისხის მოპოვება. კვლევის შედეგად გამოვლინდა, რომ ხელოვნური ინტელექტის გამოყენების თაობაზე ინფორმაცია იმდენად მწირია, რომ რთულდება არამხოლოდ მათ გამოყენებაზე კონტროლის განხორციელება არამედ სამართლიანი სასამართლოს უფლებით სარგებლობაც.

საჯარო სექტორს ხელოვნური ინტელექტის განვითარების მიმართულებით ორმაგი როლი აკისრია და შესაბამისად, ორმაგი გამოწვევა ხვდება. პირველ რიგში, საჯარო სექტორმა ხელი უნდა შეუწყოს ქვეყანაში ეროვნული სტარტაპების, ინდუსტრიის ჩამოსაყალიბებლად AI-ისთვის სათანადო ეკოსისტემის შექმნას, ინვესტორებისა და დონორების მოზიდვას, AI-ის აპლიკაციების სხვადასხვა სექტორების მიერ გამოყენებას და ხელოვნური ინტელექტით სოციალურ-ეკონომიკური ზრდისა და კეთილდღეობის მიღწევას. ამავდროულად, ხელოვნური ინტელექტის განვითარებისთვის, ხელისუფლებამ უნდა შექმნას ისეთი მარეგულირებელი ჩარჩო, რომელიც დააბალანსებს და შეამცირებს ხელოვნური ინტელექტის სისტემებთან დაკავშირებულ საფრთხეებს, რისკებს, გამოწვევებს, და უზრუნველყოფს მიღებული სამართლებრივი და ეთიკური სტანდარტების აღსრულების ქმედით მექანიზმებს. მნიშვნელოვანია, ასევე განერილი იყოს ხელოვნური სისტემების ფუნქციონირების შემოწმების პროცედურები, პასუხისმგებლობები და საზოგადოებისთვის ხელმისაწვდომი იყოს ამგვარი შემოწმების შედეგები. მნიშვნელოვანია, ამ მიმართულებით შესაბამისი ნაბიჯების გადადგმა ხელოვნური ინტელექტის დანერგვის საწყის ეტაპზე დაიწყოს.

ინფორმაციის თავისუფლების გაწვდილობის ინსტიტუტი (IDFI)

 ძ. შავჩაიშვილის ქ. 20, თბილისი 0108;  + 995 32 2 92 15 14

 info@idfi.ge  www.idfi.ge