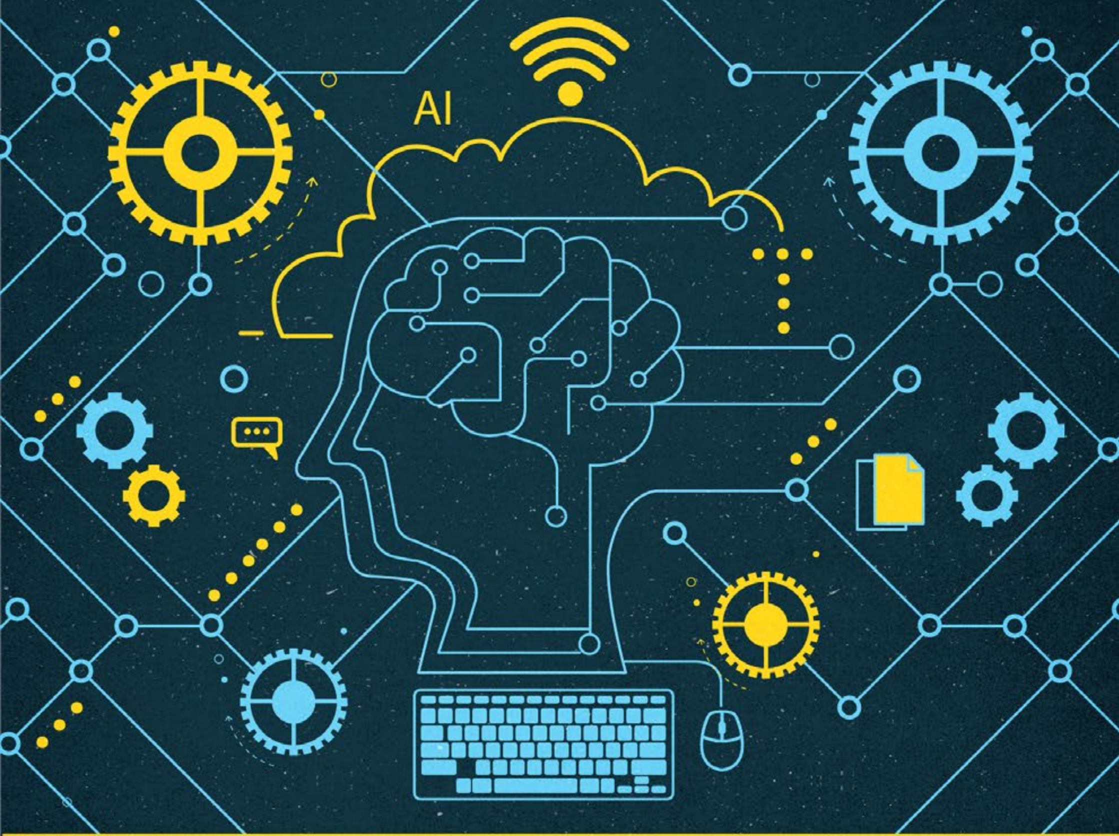


THE USE OF ARTIFICIAL INTELLIGENCE SYSTEMS IN GEORGIA

Legislation and Practice

Tbilisi, 2021

IDFI Institute for Development of Freedom of Information

ICNL INTERNATIONAL CENTER FOR NOT-FOR-PROFIT LAW

The study was financed by the International Center for Not-for-Profit Law (ICNL). The Institute for Development of Freedom of Information would like to thank ICNL for the support in the Study's development. ICNL does not necessarily share the opinions here within expressed. IDFI bears the sole responsibility for the content.

THE USE OF ARTIFICIAL INTELLIGENCE SYSTEMS IN GEORGIA

Legislation and Practice

AUTHORS: DAVID ERISTAVI; GIORGI DAVITURI

EDITORS: LEVAN AVALISHVILI; TEONA TURASHVILI

TABLE OF CONTENTS

INTRODUCTION

Technological advances have substantially increased the availability of technical or software means required for the creation of services rooted in artificial intelligence. Artificial Intelligence (AI) has the potential to transform virtually every traditional approach to work or business process management for the better. Within the framework of the project - *"Promoting Greater Transparency and Ethical Standards of Using Artificial Intelligence (AI) in Georgia"* – financially supported by the International Center for Non-Commercial Law, IDFI aims to study the functioning of artificial intelligence systems in the public sector. We are paying special attention to the challenges in terms of the use of this technological solution by the public institutions in Georgia.

The use of artificial intelligence (AI) systems in the public sector can yield significant benefits in terms of simplifying the decision-making process, improving service delivery, and introducing many other innovative approaches. The use of artificial intelligence, however, carries a few risks. Its use is linked to challenges in terms of transparency, accountability, freedom of expression, and the right to privacy. At the same time, in countries such as Georgia, where oversight mechanisms for law enforcement agencies are relatively weak and there are questions about the independence of the judiciary branch, the problem of balancing the risks associated with artificial intelligence is becoming increasingly critical to address.

In the main part of the study, the information obtained on the use of artificial intelligence by public institutions is discussed in parallel with the basic standards of ethical artificial intelligence and the main principles of current Georgian legislation.

METHODOLOGY

The use of artificial intelligence by government agencies is linked with a number of practical as well as legislative problems. For example, there is no unified register of information systems based on artificial intelligence, a normative definition of artificial intelligence and/or specific legislation on AI.

In order to identify possible cases of the use of artificial intelligence in a given public institution, IDFI used publicly available information indicating that said institution was using services containing elements of artificial intelligence in its operations. In addition, we requested information from the agencies that, given their specific functions, were highly likely to be using the aforementioned technology. After identifying these public institutions, IDFI addressed them with a request for relevant public information. 54 agencies received information request letters to this end.

It should be noted that the Georgian legislation does not define the concept of artificial intelligence as such. At the same time, there is not always a clear line between artificial intelligence and other types of functional algorithms.[1] To dispel this ambiguity and reduce the likelihood of receiving misinformation, before requesting public information, IDFI held a meeting with representatives of the relevant public bodies, one of the purposes of which was to familiarize them with the public information request in advance in order to ensure accurate answers to our inquiries.

In parallel with requests for public information, we studied the existing regulatory framework governing artificial intelligence. Namely, while it is true that there is no special legislation in Georgia regulating artificial intelligence software services by public institutions, the Constitution of Georgia, as well as other legislative acts, nevertheless set out a number of normative requirements that would apply to the use of artificial intelligence by a public institution.

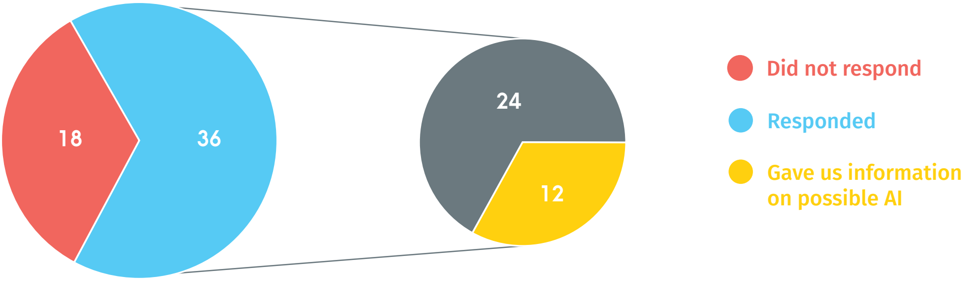
1. GENERAL ANALYSIS OF THE INFORMATION ACQUIRED AS A RESULT OF REQUESTS FOR PUBLIC INFORMATION

IDFI requested information about IT systems, software, and artificial intelligence systems created and used by the 54 public institutions identified at the initial stage. The research process primarily focused on programs containing artificial intelligence. More specifically, IDFI requested the following information from public institutions:

1. Name, purpose, creator, and users of the software;
2. Description, parameters, and its use in the decision-making process;
3. User manual/instruction and the technical manual;
4. Legal acts regulating the use of the software;
5. Rules for the protection of the standards of ethics and personal data processing;
6. Audit report and conclusion on the operation of the software.

IDFI received responses from 36 agencies out of the 54 agencies that received a request for

A TOTAL OF 54 PUBLIC INSTITUTIONS RECEIVED A REQUEST FOR INFORMATION



information. Only 12 of these 36 agencies provided information on the software they used, while some informed IDFI that they did not use artificial intelligence systems. A significant number of the target agencies did not respond to the letter requesting public information at all, while most of the responses received were limited to a statement that the agency did not use artificial intelligence. Such responses have, on several occasions, raised the suspicion that these agencies have taken advantage of the ambiguity of the term "artificial intelligence" and thereby avoided disclosing information.

Taking into account the complexity of distinguishing artificial intelligence systems from other automated software, we also received information from individual agencies on software they use that do not contain elements of artificial intelligence, but are still distinguished by a high degree of automation. As an example, the Revenue Service has introduced the Automated Customs Data System (ASYCUDA), the VAT refund system, and the electronic application processing system. 12 agencies provided a response to the first and second points of the request for public information (i.e., the name of the programs and the general description). Among these, 8 agencies provided information on the software tools they use that do not contain the features of systems that are based on artificial intelligence. According to the results of the analysis of the responses received from public institutions, the use of artificial intelligence was confirmed in 4 agencies, while the information on the use of artificial intelligence by the Prosecutor's Office of Georgia became available from public sources.

Institutions that use systems containing artificial intelligence:

1. Ministry of Internal Affairs of Georgia and LEPL Under Its Management - Public Safety Command Center 112
2. General Prosecutor's Office of Georgia
3. Georgian National Tourism Administration
4. LEPL - Education Management Information System
5. LEPL - National Center for Educational Quality Enhancement

Out of 4 confirmed cases of the use of artificial intelligence, user manual and regulatory acts for the corresponding information systems were provided only by the National Center for Education Quality Development, while information on system ethics and personal data protection standards was shared only by the National Center for Education Quality Development and the National Tourism Administration. It should be noted that the audit report and conclusion on the functioning of the program was not received from any of the agencies; according to some of them, the audit of the functioning of the mentioned systems and programs was not conducted, while others left the point unaddressed.[2]

[2] It should be noted that in 2019, the State Inspector's Office examined the so-called procedure for recording administrative offenses with the help of "smart" cameras. IDFI requested the conclusion of the inspection from the Inspector's Office and we provide its overview within the framework of this study.

2. CONFIRMED CASES OF THE USE OF ARTIFICIAL INTELLIGENCE BY PUBLIC INSTITUTIONS AND THEIR DESCRIPTION

Only a few of the target agencies for the study use artificial intelligence-based algorithms. Among these, the systems of the various institutions falling under the umbrella of the Ministry of Internal Affairs are noteworthy for their relative complexity.

2.1 MIA – FACIAL RECOGNITION SYSTEM OF THE EXPERT - FORENSIC MAIN DIVISION

The **Expert-Forensic Main Division** of the Ministry operates the POLYFACE application for automated face recognition licensed by *Papillon Systems,* which was purchased in 2013 from "My Mobile +" Ltd., with updates subsequently having been purchased 3 times in 2017, 2018 and 2019, as a result of which the Deep Learning functions of 3D photo-robot creation, video analysis, and machine learning were added to the program. The total cost of the procurement amounted to GEL 460,576. The program is a habitoscopic identification system that performs face recognition by comparing two specimens, including subjective portraits (photorobots).

According to the agency, the program is used by the Information-Analytical Department in accordance with the tasks facing the Ministry, including providing informational support for the registered cases under investigation and carrying out criminal proceedings. The headquarters of Papillon Systems are located in Russia, and its software products are *widely used* in Russian law enforcement agencies, as well as in Turkey, India, Nigeria, and several post-Soviet states.

2.2 MIA – PUBLIC SAFETY COMMAND CENTER (112) – LICENSE PLATE AND FACE RECOGNITION SYSTEM

LEPL Public Safety Command Center of the Ministry of Internal Affairs - "112" has introduced software for recognizing state license plates in addition to facial recognition software. The manufacturer of the state license plate recognition program is the international company *"ISS" - Intelligent Security Systems*, which manufactures a variety of digital products. Meanwhile, the Japanese company *"NEC"* is the manufacturer of the facial recognition program. According to the Ministry, both of the above programs are used to detect administrative offenses, safeguard public order, protect personal safety and property, and facilitate investigations. It should additionally be noted that the NEC facial recognition program, unlike POLYFACE, is integrated with a network of video cameras installed across the country and operates in real time, captures the biometric data of the persons reflected on the video material and compares them with the database of wanted individuals.[3]

The information provided directly by the Ministry of Internal Affairs of Georgia is general in nature and does not provide a complete picture of the full potential of smart cameras and/or to what degree this potential has been realized in practice. However, a joint analysis of the publicly available resources of the software manufacturers and the decision[4] made by the State Inspector's Service on the inspections carried out at the Ministry of Internal Affairs provides a fuller picture on this topic.

2.2.1 PROCESSING OF INFORMATION OBTAINED FROM SMART AND GENERAL VISION CAMERAS BY THE MIA

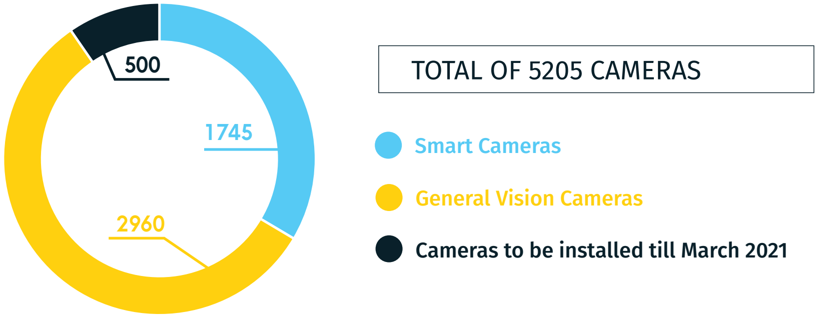
The Ministry of Internal Affairs of Georgia uses two types of "smart" and general vision cameras. According to the data from the Public Safety Command Center (112), 4,705 video cameras have been placed throughout Georgia, with 1,745 being (so-called) number recognition cameras and 2,960 being general vision cameras.[5] It should be noted that on December 10, 2020, the Ministry of Internal Affairs purchased additional 500 general vision cameras for a sum of 417,800 GEL, the installation of which, according to the contract, is expected to be completed in March 2021.[6]

[3] This conclusion on the functioning of the face recognition system is not supported by official documents received from the Ministry of Internal Affairs. However, their representatives confirmed this information via telephone call. In addition, this fact is also explained in one of the press releases published on the website of the Ministry. *See the link.*

[4] Decision of the State Inspector's Service NC-1/222/2019 of June 27, 2019, "On Completion of the Inspection of the Ministry of Internal Affairs of Georgia".

[5] See *data* of 112 Public Security Command Center of the Ministry of Internal Affairs.

[6] See *contract.* There is a high probability that these cameras have not been installed yet and the number of cameras may exceed 5,000 in the near future.



The technical description of the cameras indicates that they are in possession of high-resolution cameras, which would naturally make it easier to process captured images with the help of video analytics software. Notably, the same is determined by the decision of the State Inspector's Service. In particular, an inspection revealed that both smart and general vision network cameras allow clear, high-resolution images to be taken at any time of the day or night.

Both smart and general view cameras are used for the detection of administrative offenses. With the former, an administrative violation can be detected automatically. In the latter case, the offense is manually recorded by the operators of the Public Safety Command Center (112 Centers).[7]

It is noteworthy that neither the website of the Ministry of Internal Affairs nor the website of the Public Safety Command Center contain detailed information on the processing of data received through cameras, although the abovementioned decision of the State Inspector provides important information regarding this topic.

The conclusions of the State Inspector reveal that when automatically detecting an offense, a smart camera will record in the database of the video analytics program the state number plate of the offending vehicle and a unique case ID as well as other data identifying the violation.[8] The identified case is then redirected to the General Database of Administrative Violations/offences, where various data related to the recorded administrative violation is filled out automatically.[9] It should be noted that this system of violations related to the databases of the Service Agency of the Ministry of Internal Affairs and certain data about the vehicle is filled out on an automated basis.[10]

[7] According to the website of the Public Security Command Center "112" of the Ministry of Internal Affairs, smart cameras can automatically detect the following violations: "passing a red light; double axis line crossing; traffic in the municipal transport lane; movement in the opposite direction of traffic; exceeding the speed limit."

[8] Date and time of the violation; type of violation; camera coordinates; the name of the server on which the data was processed and a link to the photo of the offending vehicle.

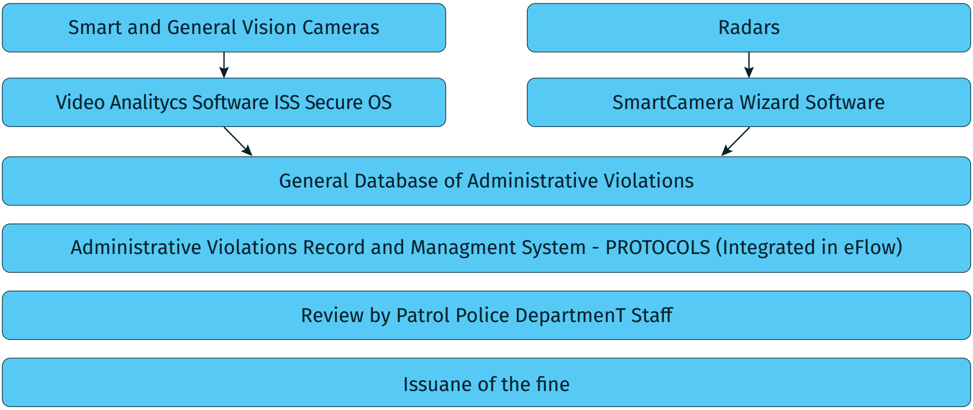
[9] Place and date of the administrative offense, and relevant article of the Code of Administrative Offenses of Georgia.

[10] Fields about the model, color and owner of the vehicle are automatically filled in from the database of the Service Agency of the Ministry of Internal Affairs.

A similar procedure is carried out in case of detection of an offense with the help of a general vision camera, although in this case, instead of an automatic method, the detection of the violation is carried out through the use of human resources (by an operator). Otherwise, the degree of data processing automation is the same, with the exception of the moment of direct detection of the offense. Notably, when the offense is captured with a general vision camera, "the same video analytics program that ensures the operation of smart cameras" is used.[11] Otherwise, the video data received by the Ministry from both smart and general vision cameras is processed through a unified analytical software.

In the case of the radar, only the instance of exceeding the set speed of movement is detected, after which the photo material and relevant data related to the case are automatically stored on the photo-video material storage server. After these recordings have been processed automatically (through special software - SmartCamera Wizard), the relevant data is uploaded together with the attached photo file to the General Database of Administrative Violations.

Prior to the issuance of a receipt for the fine, the employees of the Patrol Police Department double-check the data, in particular whether the state number plate of the vehicle and the instance of the administrative violation match the administrative violation reflected in the photo/video materials accompanying the document. In the absence of any errors, the officers of the Patrol Police Department will finally record the violation and draw up an appropriate receipt for the fine.


Smart and General Vision Cameras
Radars
Video Analitycs Software ISS Secure OS
SmartCamera Wizard Software
General Database of Administrative Violations
Administrative Violations Record and Managment System - PROTOCOLS (Integrated in eFlow)
Review by Patrol Police DepartmenT Staff
Issuane of the fine

From the data provided, it is noteworthy that the decisions (recorded cases) made by smart cameras are subject to pre-verification. Otherwise, the solution adopted by the artificial intelligence system is final and subject to preliminary human control.

[11] Decision of the Inspector, p. 6

2.2.2 FACIAL AND PLATE NUMBER RECOGNITION SYSTEM THROUGH "SMART" AND GENERAL VISION CAMERAS

To realize the potential of smart cameras, it is not enough to simply have the camera. While it is true that such video surveillance enables one to capture more electronic data by observing the physical environment, if it is not managed with proper software, the potential of smart cameras is almost completely lost. In other words, in practical terms, "smart camera is made smart through the right software" that uses artificial intelligence-based algorithms. Additionally, with well-developed software, a video analytics system has the potential to transform any camera with the right resolution into a "smart" camera. For instance, advanced facial recognition systems[12] do not require the use of any specific camera at all.

The Ministry of Internal Affairs did not provide any information regarding the smart camera management system. Nevertheless, in the context of number plate recognition, it referred to a video analytics program developed by the ISS,[13] while in the context of the facial recognition system it pointed to specialized software purchased from a Japanese tech company.[14]

Both the publicly available information and the information provided by the Ministry of Internal Affairs indicate that the video analytical software under consideration is used only to detect the license plates of the vehicle involved in a given offense. This module is just one component of the ISS Secure OS program, which has more capabilities than simply identifying the vehicle number plate at the time of an offense.[15] Namely, the License Plate Recognition (LPR / ANPR) system developed by ISS uses an algorithm based on deep learning that is able to distinguish a car from other objects recorded on the camera and recognize the license plate. At the same time, its following functions should be highlighted:

a) This algorithm does not require a specialized camera to identify the license number. Any camera with a resolution greater than 1280x720 can be used to this purpose.[16] Notably, the resolution of the cameras purchased by the Ministry of Internal Affairs on the basis of the contract of December 31, 2020, is 2048 x 1536.

b) It does not only detect the license plate during an act of violation, but also has the function of searching by car number and other characteristics.

c) It has the capability to incorporate various search engine listings (e.g., wanted cars). Additionally, it allows operators to send automatic notifications regarding a vehicle discovered on a given list.

[12] Including the system used by the Ministry of Internal Affairs.

[13] Intelligence Security Systems (ISS), website: *https://issivs.com.*

[14] *https://www.nec.com/en/*

[15] Developed by ISS (License Plate Recognition (LPR/ANPR). *Capabilities* of video analytics or specific modules

[16] See the detailed technical *specifications* of the camera.

d) The program has a function of determining the direction of movement of the vehicle in advance.

e) The analytics program can be integrated (it can be connected) with external databases, and it can additionally be used with other applications (API Support).

This is only an incomplete list of the functions of the number plate recognition module. It should be noted here that the Public Safety Command Center (112) also uses a facial recognition system developed by the world's leading company (NEC). The manufacturer's website makes it clear[17] that one of the main advantages of its facial recognition system is its sophisticated algorithm rooted in artificial intelligence and data analytics. The most noteworthy aspects of this facial recognition system are:

a) It is able to recognize faces not only from high-resolution graphics, but also from low-quality video/photo material (24 pixels), even if the subject is wearing a hat, a scarf, or is in motion.

b) It operates successfully in public places and can scan thousands of faces every minute based on the data received from different cameras.

c) It has the ability to convert planimetric photos (2D) into three-dimensional (3D) space. After conversion, it turns the 3D image of the human head [360 degrees] and in the process artificially adjusts the various lighting and expressions and as a result allows facial recognition with 99% accuracy in almost any conditions.

Unfortunately, the Ministry of Internal Affairs did not provide any official information on the use of this facial recognition system. This information cannot be gleaned from publicly available officiall sources either.

2.2.3 LEGALITY OF THE MINISTRY›S USE OF VIDEO SURVEILLANCE SYSTEM – RESULTS OF THE STATE INSPECTORS AUDIT OF THE MINISTRY OF INTERNAL AFFAIRS

In 2019, the State Inspector's Service conducted an inspection of the Ministry of Internal Affairs. The use of a facial recognition analytical system was not the subject of the inspection, although it did cover the legality of processing video recordings stored by the Ministry within the ISS Secure OS Video Analytics. The results of the inspection are disturbing, as the State Inspector’s Service found violations at virtually every stage of data processing.

As a result of the inspection, the State Inspector found violations regarding the time frames

[17] See ***information*** posted on the NEC official website regarding the face recognition system developed by the company.

of data storage. The data and photo-video materials that were subject to deletion within days or months were in some cases stored on the server for years. According to the Law of Georgia on Personal Data Protection, data may be stored only for a period necessary for the purposes of data processing. Once the purpose for which the data is processed has been achieved, the data must be blocked, deleted, destroyed, or stored in a form that does not identify the person, unless stipulated by the law otherwise.

Notably, the Ministry of Internal Affairs did not record the activities carried out in the databases using the ISS Secure OS analytical program/using artificial intelligence. In other words, it was impossible to verify the legitimacy of individual cases of artificial intelligence use (tracking). This is especially problematic given the fact that the analytical program processes not only an instance of detection of an offense but also the continuous recordings of all smart or general vision cameras installed across the country.

Based on the results of the inspection, by the decision of the State Inspector, the Ministry of Internal Affairs was instructed to:

- Record all actions pertaining to any data existing in the video analytics program as well as in the database of the mentioned program.
- Record all actions pertaining to the photo/video files stored in the local personal computer of a center operator during the manual detection of an administrative violation with a general vision camera.
- Record all actions taken pertaining to video recordings stored on central video servers.
- Record all actions taken pertaining to photo/video files stored on the photo/video storage server.
- Record all actions taken pertaining to the existing data in the web application of the unified database of violations of the law, as well as in the database of said web application.
- Note all actions taken regarding the records of administrative violations stored in the electronic document management system.
- Determine the storage period of data obtained by photo/video equipment and delete/ depersonalize data after the specified period.

IDFI's information request letter sent to the Ministry of Internal Affairs included, among other things, legal acts/manuals or instructions pertaining to the use of artificial intelligence within the institution. The only legal act that contains more or less detailed regulations on the issue of the use of video surveillance system is the ***Order N328 of June 28, 2017,*** of the Minister of Internal Affairs of Georgia. The order regulates "the conditions and procedures for the placement and use of automatic photo- and video equipment on the vehicles without the appropriate identification marks and non-stationary (mobile) speed measuring devices in use by the Police of Georgia, as well as the conditions and procedures for data processing." According to the information provided by the Ministry of Internal Affairs, this order regulates the processing of information obtained by the Ministry through body cameras and cameras placed on vehicles, roads, or outer perimeter. However, two circumstances need to be taken under consideration. Firstly, this Order applies to the use of the surveillance system only for the purposes of contactless patrols (ensuring traffic safety). It does not regulate the use of the same system for, as an example, the detection of a crime or an attempt thereof, or for the purposes of identifying wanted persons and vehicles, all of which is in turn a function of the Public Safety Command Center (112). At the same time, according to paragraph 2 of Article 7 of Order N328, "the Ministry is obligated to ensure the recording of all actions performed in relation to the data/information stored in electronic form." The Ministry has had this obligation since 2017; however, as revealed by the inspection conducted by the State Inspector in 2019, the Ministry of Internal Affairs did not record the actions taken in relation to the processed data at all. This might have been caused by the fact that the person issuing public information misidentified the legal act and the Order does not apply at all to the processing of the data obtained by smart and general view cameras, including the processing through the use of ISS Secure OS analytics software. The Ministry violated the rules for processing its own information until at least 2019. All other legal acts identified by the Ministry of Internal Affairs are more general in nature and, in best case scenarios, only define the general legal basis and objectives for the processing of information through video analytical software. It does not at all have anything to say on the rules for the use of such analytical programs and the prevention of risks that arise a result of their use.

We do not know to what extent the above recommendations of the State Inspector's Service have been implemented in the Ministry, although, given that the Ministry has not provided any appropriate legal acts, we can assume that the practical reality of the use of ISS Secure OS has not changed in any significant way.

2.3 THE PROSECUTOR›S OFFICE OF GEORGIA – IBM I2 ARTIFICIAL INTELLIGENCE ANALYTICAL SOFTWARE

In response to a letter requesting public information on October 22, 2020, the General Prosecutor's Office of Georgia informed IDFI that artificial intelligence-based algorithms and systems were not found among its resources. However, during his presentation of the 2020 report on the activities of the Prosecutor's Office of Georgia to the Prosecutorial Council, the First Deputy General Prosecutor announced that ***the Prosecutor's Office of Georgia has started using artificial intelligence for the purposes of its investigations.*** After sending the public information request again, on February 5, 2021, the Prosecutor's Office of Georgia informed us that they had implemented IBM 2 analytic program.

According to the 2020 report of the General Prosecutor's Office of Georgia, the IBM I2 Analysis Program was introduced in the Prosecutor's Office of Georgia with the support and assistance of the Embassy of the United States of America in Georgia. The IBM I2 program allows its users to integrate banking and telephone statements and other information obtained from various sources of differing formats into the program. The program analyzes, sorts and structures data, and is able to detect connections between two or more networks, detect patterned behaviors and latent threats, and track criminal activity through automatization and visualization of dry data processed in a short period of time. It is possible to receive and process data in the system in real time. According to the report, the software is used for both crime prevention and timely crime investigation.

The information disseminated by the Prosecutor's Office of Georgia does not contain detailed data on the analytical capabilities of the program. IDFI's reviewed the publicly available information[18] about the program disclosed by the manufacturer and got acquainted with a presentation demonstrating the capabilities of the system. The study revealed that the software has various types of advanced analytical capabilities. Among these are:

- Easy data integration: it quickly and easily connects to internal and external databases;
- The program has the ability to detect hidden patterns and connections between large datasets;
- Geo-location investigation: it can be integrated with maps and enables geo-visualization of the investigation.
- Social network analysis: it allows analysts to study and analyze data structures, network communication flows, and identify key players and lines of investigation.

According to the Deputy General Prosecutor, this software helps prosecutors and investigators to make timely investigative or operational decisions and enables them to obtain effective results in a short period of time. At this stage, it is unfortunately unknown to IDFI to what extent and specifically in what direction artificial intelligence is used in this process. For example, which databases is this software connected to? What does its use for the purposes of crime prevention? Who has access to this software and other similar issues.[19]

[18] IBM Security Solution Brief Investigative analysis in Law Enforcement ***https://www.ibm.com/downloads/cas/OW3KJN1Y.*** You may be asked for authentication in order to access the document.

[19] IDFI has again addressed the Prosecutor's Office of Georgia with a request for public information and continues to study this issue.

2.4 LEPL – GEORGIAN NATIONAL TOURISM ADMINISTRATION – AUTOMATIC ANALYSIS OF SENTIMENTS ("EMOTIONS ARE GEORGIA")

In 2017, the **National Tourism Administration** commissioned the advertising company "Windforce" for the advertising campaign "Emotions are Georgia". The campaign was developed by "Pulsar" Ltd. using artificial intelligence. Within the framework of the project, public posts published on social networks by people visiting Georgia were analyzed and categorized. Artificial intelligence was used in two directions: for the identification and categorization of objects, locations, landscapes, and other figures depicted in public photos, and the determination of the sentiments expressed within the texts of public posts (positive, negative, neutral) as revealed through their analysis. The final product is a collection of public posts published by tourists in Georgia in 2017; *the collection presents visual and text material that carry positive emotions*. According to the Tourism Administration, in order to secure personal data, two documents were developed, with the data being used on their basis. The documents state that the Administration obtained the written consent of the authors of all posts involved in the campaign.

2.5 LEPL - EDUCATION MANAGEMENT INFORMATION SYSTEM – ASSOCIATIVE DATA ANALYSIS

The **Education Management Information System** uses Qlik sense analytics system for data visualization and reporting. It integrates general education management information system and reporting (number of students and teachers in different contexts, such as according to school year, school dropout rates, etc.). The official website of the program reveals that it possesses the function of associative data analysis based on artificial intelligence, although the agency did not provide detailed information on how this function is used. According to the agency, a contract was signed with NGT Group Ltd. for the provision of data visualization, analysis and accompanying reporting software. The cost of the contract was 80,268.00 GEL. In addition, a contract was signed with NGT Group Ltd. for the purchase of one-year technical support service for the visualization, analysis and reporting analytical system Qlik Sense Pro User and the activities for the implementation of project assignments; the contract value is 22,390 GEL.

2.6 LEPL – NATIONAL CENTER FOR EDUCATIONAL QUALITY ENHANCEMENT – DLP AND TRANSLATION MEMORY MODULE

The **National Center for Educational Quality Enhancement** uses Office 365. This is a set of software from Microsoft that provides collaboration, office software support, and various online automation services. The system has a built-in DLP module based on artificial intelligence. DLP is a data loss prevention module that identifies sensitive and personal data through machine learning, classifies them, and performs automatic encryption whenever the risk of data loss is detected. It also provides automatic blocking of unauthorized intrusions into the system and automates various security processes.

According to the Center, the abovementioned platform helps the organization ensure the security of services (such as Email, Teams, SharePoint, etc.) that are in daily use. In case of detection of illicit activity, the program sends a notification to the person responsible for tech management, which helps the agency in making various decisions, such as the issue of blocking specific users.

The artificial intelligence component is also in evidence with the translation software ***SDL Trados Studio*** used at the National Center for Quality Development in Education. The software has so-called "Translation Memory", which is automatically filled in by translators/ editors through the addition of new terms and then automatically offers various sentence translation suggestions for translators, which is a simple example of machine learning.

The British company SDL owns the translation computer software SDL Trados Studio. According to the Center, the software is used to translate accreditation and authorization documents submitted by higher education institutions for international experts, as well as to translate accreditation and authorization conclusions prepared with the involvement of international experts from English to Georgian for higher education institutions. Again according to the Center, the translation process has been greatly simplified since the purchase of the server software, with the translation of the same number of documents being now done by only 7 translators instead of 15 as was the case previously. The Center also provided related normative materials describing the cases for which the Center will provide translation services. However, detailed information about the software is not available. It should be additionally noted that, according to the Center, the internal audit service has not conducted audit inspections of the functioning of information systems/ software/artificial intelligence systems.

3. THE PLACE OF ARTIFICIAL INTELLIGENCE IN THE LEGAL FRAMEWORK OF GEORGIA

After examining the current practices of the use of artificial intelligence by public institutions, we would like to briefly review some of the basic principles characteristic of ethical artificial intelligence in parallel with the basic provisions of the rule of law.

The term "artificial intelligence" is only mentioned ***three times*** among the normative acts found on the Legislative Herald of Georgia. None of them is a legislative act. Two of these normative acts address the issues of development/regulation of artificial intelligence-based services in the private financial sector[20], while one recognizes the status of "artificial intelligence" as a high technology in the field of entrepreneurial (startup) activities. The Georgian legislation says nothing about the use of artificial intelligence systems by public institutions, although this should not be taken to mean that public institutions are prohibited from using artificial intelligence. To determine the place of artificial intelligence in the Georgian legal framework, it is important to understand what artificial intelligence is in general terms.

There is no internationally recognized and accepted concept regarding the definition of artificial intelligence.[21] Nevertheless, the vast majority of existing definitions are based on a functional understanding of artificial intelligence. More specifically, these definitions distinguish artificial intelligence from other digital algorithms by its capabilities (degree of autonomy and adaptability). Different levels of artificial intelligence are rated according to the same criteria. Therefore, artificial intelligence is a variation of computer algorithms - one of the main achievements of technological development, the capabilities of which are increasing constantly.

The Georgian legislation does not prohibit a public institution from using technological progress to effectively exercise its powers. On the contrary, the lawful use of technological advances in public administration is welcome, as it greatly simplifies the achievement of the

[20] Meaning the banking and insurance sectors.

[21] An indication that this definition of artificial intelligence does not refer to AI singularity

legitimate goals for which the relevant institution has been established. At the same time, the rule of law requires that any action of a public institution comply with the requirements of the law. Therefore, in the conditions when the legislation of Georgia does not define specific requirements for the systems containing artificial intelligence, the specific cases of their creation or use will be regulated by the legislation that governs the relevant legal relationship. Specifically, artificial intelligence can be used in different legal relationships to achieve a variety of differing goals. Therefore, depending on the nature of the right that is being restricted and the content of the relevant regulatory legislation, different legal norms will need to be applied to each case of the use of artificial intelligence.

In this part of the study, we outline the basic legal principles established in the Georgian legal framework that must be observed in the development/use of artificial intelligence by public institutions, and which are at the same time integral elements of ethical artificial intelligence. We will also discuss the potential risks posed by the confirmed cases of the use of artificial intelligence in the public sector.

4. EFFORTS OF THE NATIONAL BANK OF GEORGIA IN REGULATING THE FINANCIAL SECTOR

In its response to IDFI, the National Bank claimed that the agency does not use artificial intelligence systems. However, it is important to highlight Order N151/04 adopted by the President of the National Bank on August 17, 2020. The purpose of this Order is to promote the establishment of a risk management framework for statistical, artificial intelligence, and machine learning models (hereinafter referred to as the model) and the effective management of the risks associated with it. Its effects extend to the representatives of the financial sector (e.g., commercial banks, microfinance organizations) through the measures taken so far. The mentioned Order defines the principles of risk management and administrative-organizational control mechanisms for these subjects at the stages of creation, outsourcing, and launch-development of these models when introducing statistical, artificial intelligence, and machine learning systems.

The National Bank informed IDFI that several commercial banks have developed a statistical model for evaluating income that is used in the lending process. This model allows the Bank to estimate a client's income and make a loan decision without any documented proof of said income, solely based on other information received from the client. According to the National Bank, before model began being used, the entities submitted a complete description of the model and a list of the data that the algorithm is based on in its operations. The National Bank reviewed, evaluated, and defined certain restrictions for the entities, although the reply received from the Bank does not specify what type of restrictions have been imposed on the participating entities.

The private sector, especially in the banking and insurance sectors, makes active use of artificial intelligence systems. The purpose of this study is to analyze the use of artificial intelligence by the public sector, although the Order N151/04 adopted by the President of the National Bank on August 17, 2020, should be considered the first attempt to regulate the use of artificial intelligence and machine learning within the country.

5. ARTIFICIAL INTELLIGENCE SHOULD SATISFY LEGISLATIVE REQUIREMENTS

According to the first and fourth paragraphs of Article 4 of the Constitution of Georgia, Georgia is a state governed by the rule of law, and state power is exercised within the limits established by the Constitution and the Law. This provision of the basic law of the State reinforces the principle of the rule of law, which in turn requires that any action of the State be in accordance with the requirements outlined by its legislation. Naturally, we will not be able to review all the legal requirements that have the potential to be used in relation to artificial intelligence, although we will focus on cases where artificial intelligence is used in violation of the law.

In the course of this study of the legality of the use of artificial intelligence, violations were identified in terms of protection of privacy/personal data. Namely, the Office of the Personal Data Protection Inspector did not study the use of the facial recognition system at all, although the agency found violations at virtually every stage of the operation of the video surveillance systems of the Ministry of Internal Affairs. At the same time, there are significant questions about the constitutionality of the introduction and use of artificial intelligence in the Ministry of Internal Affairs.

The above case indicates the need to comply with the requirements of the legislation. The requirement of lawfulness is also essential for the stability of the use of the artificial intelligence system itself. Specifically, if the development of artificial intelligence does not take into account all the requirements of the legislation and carry the possibility of easy adaptation to a changing legal environment, the use of the relevant electronic system will be significantly delayed, and a number of costly reforms may end in failure.

6. USE AND TRANSPARENCY OF ARTIFICIAL INTELLIGENCE

One of the requirements for ethical artificial intelligence is its transparency. More specifically, it must be open, and its working principles must be explicable and interpretable in layman's terms. Without transparency, proper legal or ethical oversight over artificial intelligence system is impossible.

There is no unified register of artificial intelligence systems in Georgia. The only way to get information about artificial intelligence algorithms used by public institutions is through public information requests.

One especially noteworthy incident that was encountered in the course of the study was the fact that one of the target institutions considered not only the principles, capabilities and legal consequences of the functioning of artificial intelligence, but the very fact of its existence as confidential information. Namely, LEPL Financial Monitoring Service initially refused to provide any information regarding the systems incorporating artificial intelligence. The agency cited the confidentiality of this information as the legal basis for the refusal. Its letter stated that the Service uses only specialized software tools, the specifics, technical characteristics, architecture and/or the implemented algorithms of which are strictly confidential. Following an administrative appeal of the response by IDFI, an oral hearing was held, during which the public institution expressed the opinions that the information on whether or not it uses artificial intelligence software should be kept confidential. Finally, after the administrative complaint had been reviewed, the LEPL Financial Monitoring Service provided the requested information and noted that the agency does not use systems based on artificial intelligence.

The lack of information on systems containing artificial intelligence makes it impossible to exercise both legal and public control over them. For instance, the Ministry of Internal Affairs is in possession of a facial recognition system developed by one of the world's leading companies and can process biometric data of thousands of citizens every minute with 99% accuracy. The use of this artificial intelligence software is unknown to the public. Is it connected to all cameras located throughout Georgia? Does it store human biometric data on a permanent basis? And other relevant issues. This kind of information vacuum complicates both the ability to appeal to a common court and exercise the right to a fair trial, and the ability to exercise effective control over the constitutional and lawful use of relevant information systems.

7. COMPATIBILITY OF ARTIFICIAL INTELLIGENCE WITH DEMOCRACY AND THE RULE OF LAW

The main purpose of this request is to respect human dignity, freedom, and the right to information and self-determination. In particular, despite the short history of the use of artificial intelligence systems, there have been numerous cases of its abuse and incompatibility with the principles of a democratic state across global practice.

Particular attention should be paid to the risks of processing databases existing with the law enforcement and security sector by artificial intelligence. A striking example of this is the constant increase in the analytical capabilities of the Ministry of Internal Affairs based on artificial intelligence, in the absence of the necessary mechanisms to balance the risks that arise from reliance on these processes.

To illustrate the risks more clearly, we might consider the example of the Central Data Bank. Specifically, the LEPL - Operational Technical Agency of the State Security Service was authorized to establish a central data bank. In accordance with Article 11 of the Law of Georgia “On Legal Entity of Public Law - Operational-Technical Agency of Georgia”, the Agency shall establish a central bank of identification data. To this purpose, it is authorized to "have remote access to the electronic communications identification databases of the electronic communications company and to copy and store them." It should be noted that this database contains data identifying the Internet or telephone communication through the infrastructure of all electronic communications companies[22] operating in Georgia. According to Article 2, paragraph z^{69} of the Law of Georgia “On Electronic Communications”, the electronic communication identification data is “user identification data; data required to trace and identify the source of communication; data required to identify the addressee of the communication; data required to identify the date, time and duration of the communication; data required to identify the type of communication; data required to identify communication equipment or possible equipment of the user; data required to identify the location of mobile communication equipment”.

[22] According to paragraph $H^{60.}$ an electronic communications company is an "authorized entity whose activity and/or service is the provision and/or service of telephone networks and/or Internet networks."

In other words, the Central Data Bank of Georgia stores the identifying data of any telephone or internet communication carried out throughout Georgia. It should be noted that the constitutionality of the existence of the Central Data Bank has been appealed in the Constitutional Court of Georgia twice already. The Court has yet to issue a final decision in this case, although it is noteworthy that the representative of the Operational Technical Agency of Georgia, at one of the essential hearings for the case, identified the technical possibility of using automatic management tools (algorithms) in it as one of the reasons for the necessity of the existence of the Central Data Bank.

The information provided by this institution reveals that it does not use a system based on artificial intelligence. Nevertheless, the processing of data in the Central Bank using an artificial intelligence system poses a significant threat to a democratic state.

8. RISKS ARISING FROM ARTIFICIAL INTELLIGENCE SYSTEMS IMPLEMENTED IN PUBLIC INSTITUTIONS

The analytical systems available to the Ministry of Internal Affairs of Georgia give us a clear idea of the risks arising from the artificial intelligence solutions introduced in public institutions.

To this date, the number of surveillance cameras installed across the country ***reaches 5,000*** and increases from year to year, although the normative basis governing facial recognition technologies is still scarce and too general in nature. In relation to the processing of data obtained by smart cameras, only general acts such as the Law on Police, the Law of Georgia on Personal Data Protection, and the Code of Ethics of the Georgian Police were included in the regulatory acts provided by the Ministry. As mentioned previously, as a result of the inspection, in terms of just personal data protection, violations were detected at virtually every stage of data processing by the system. Some of them, in our opinion, show signs of clear intent. For example, the lack of the records on the activities carried out by the employees of the Ministry of Internal Affairs in the databases is such an inconceivable mistake from a legal and technical standpoint, that it raises the concern that this mistake was deliberate. When viewed through the context of the number of employees of the Ministry and the degree of secrecy of its activities, the risk of malicious misuse of artificial intelligence systems by the employees is quite high. As an illustration of the point, see the decision of the State Inspector's Office, which revealed one instance of ***an employee of the Ministry of Internal Affairs, with the help of another employee (his own sister), obtaining personal data from the databases of the Ministry of Internal Affairs for non-official purposes***. The lack of a system for recording the activities carried out in the databases makes the risks of employees using these systems for both illegal and non-official purposes exceedingly high.

The information posted on the electronic resources of the Ministry of Internal Affairs about the functioning of license number identification systems is only general in nature. We encounter the same problem in the written response issued by the Ministry. Meanwhile, the official information on the use of the NEC facial recognition system is a black box, the closed existence of which carries significant risks of human rights violations.

The Ministry of Internal Affairs is increasing the number of video surveillance systems and video-analytical capabilities annually. On its own, this does not constitute a problem. However, the introduction of artificial intelligence systems by the Ministry of Internal Affairs indicates that the Ministry considers them ordinary software and the dangers of abuse of increased analytical capacity thereby remain unaddressed.

As a comparison, the potential dangers of artificial intelligence-based video surveillance systems are most clearly illustrated by the example of China, which uses state-of-the-art detection technologies and extensive video surveillance networks and analytics software to track citizens and detect various crimes. Local lawmakers in several ***major U.S. cities*** (e.g., San Francisco, Boston, Portland) have completely banned the use of facial recognition technology by law enforcement as a result of the threats and risks the technology poses. ***The EU is also considering a temporary, 5-years ban*** in order to give lawmakers the time and means necessary to develop adequate regulations.

Along with the Ministry of Internal Affairs, we should also consider the system based on sentiment analysis that was used by the National Tourism Administration for a PR campaign. In particular, the ability to automatically evaluate sentiments in public posts using similar technology. The creation of such a system of artificial intelligence and the analysis of political posts has the potential to have a significant impact on ongoing democratic processes in the country.

Despite the use of artificial intelligence having been confirmed in only a small number of public institutions, a concerning trend has emerged. Specifically, the intelligence agencies (State Security Service, Financial Monitoring Service) that, due to the nature of their functions and operations, should, as a general rule, need increased analytical capabilities to effectively detect and respond to external threats, do not have artificial intelligence-based analytical systems at all. On the other hand, the implementation of artificial intelligence systems is actively underway in the Ministry of Internal Affairs and the Prosecutor's Office.

It is important to start an active public discussion and introduce preventive regulations to accompany the spread and development of new technologies. With the introduction of artificial intelligence to the public sector, the risks of abuse of increased analytical capabilities need to be balanced. Both the protection of basic human rights and the implementation of the principles of a democratic state require that more information be disclosed regarding the artificial intelligence systems used in the public sector and the principles of their operation. In the absence of such knowledge, the public does not have the opportunity to effectively safeguard their rights. For example, it is impossible to learn about the use of a state-acquired facial recognition system, thus making it significantly more difficult to exercise the right to a fair trial effectively, as individuals have no information about the possible processing of their biometric data.

CONCLUSION

The introduction of artificial intelligence systems in the Georgian public sector is at an early stage of development, although in the private sector there are many successful examples of the use of this technology, such as remote verification systems, automatic document identification systems, communication automation programs, and many other tools. This sector has become particularly profitable in the face of the pandemic due to increased demand for remote services. Therefore, the potential for large-scale use of artificial intelligence in terms of increasing efficiency and cost-effectiveness in various processes has already become evident. However, there are also risks that can arise as a result of systemic misuse, technical glitches, and mismanagement of personal data.

Artificial intelligence is not just another electronic assistance tool. It substantially increases the governing capacity of the state, thereby increasing the temptation for its illicit use. This risk is particularly high in developing democracies. The study revealed that law enforcement agencies are the only area in the public sector where the process of introducing artificial intelligence is stable, which serves as an indirect indication of the imminent nature of these risks.

The present study highlights the lack of normative acts regulating artificial intelligence systems and documents defining ethical norms in the target agencies. In order for the public sector to be able to make the most of these technologies, access to information and transparency regarding the systems is critically important, along with technological readiness, so that the public be informed about the peculiarities of the functioning of these systems, to exclude the risks of bias, and make it possible for an external observer to discuss the possible shortcomings of the system and for it to gain a high degree of trust. The study has shown that information on the use of artificial intelligence is so scarce that it is difficult not only to control its use but also to exercise the right to a fair trial.

The public sector has two major roles to play in the development of artificial intelligence, and it therefore faces a dual challenge. Firstly, the public sector should promote the formation of a national ecosystem for national startups and industry aimed at the exploitation of AI, attract investors and donors, use AI applications in different sectors, and achieve socio-economic growth and prosperity through artificial intelligence. Simultaneously, for the development of artificial intelligence, the government should create a regulatory framework that balances and reduces the threats, risks, and challenges associated with artificial intelligence systems; one that provides effective mechanisms for enforcing the adopted legal and ethical standards. It is also important to outline procedures for auditing the operations of artificial systems, to define responsibilities, and to make the results of such inspections available to the public. It is important to take appropriate steps in this direction from the very beginning of the introduction of artificial intelligence.

INSTITUTE FOR DEVELOPMENT OF FREEDOM OF INFORMATION (IDFI)

20, T. SHEVCHENKO STREET ☎ + 995 32 2 92 15 14

info@idfi.ge www.idfi.ge