Research Article

Received: 5 July 2023 / Accepted: 23 August 2023 / Published: 5 September 2023

Privacy vs Security: A Critical Review of Albanian Law and Citizen Rights

Ivas Konini

Iv Rokaj

Lecturer, Department of Criminal Law,
Faculty of Law, University of Tirana,
Tirana, Albania

DOI: https://doi.org/10.36941/ajis-2023-0128

Abstract

The present study contends that the lack of an exhaustive legal framework regulating the installation, use, and storage of data obtained from surveillance cameras poses a threat to public order and society in Albania. While security cameras can aid in preventing crime and enhancing citizens' safety, privacy concerns raised by surveillance must not be overlooked. Therefore, a balance between security and privacy should be set, and the legal regulations law must clearly define the purpose of the installation of cameras, delimiting security measures to accomplish their intended purpose. The actual main law for this area is titled "On Additional Measures for Public Security" and was passed by the Parliament on 2016. This law provides a good start for further progress if certain changes is specific areas of it can be changed. In the other hand, mere good intentions cannot serve as a justification for privacy violations and guidelines for the collection, storage, and use of data obtained from surveillance cameras must be established by this law or other regulatory means. This article highlights that the effectiveness of surveillance cameras in detecting crimes is limited, especially for those that are covert and sophisticated. As such, the law should provide clear instructions on the collection, storage, and utilization of data acquired through surveillance cameras to avoid unintended consequences and privacy violations. Ultimately, this research underscores the importance of balancing public safety with individual privacy rights in wiretapping and camera surveillance in Albania.

Keywords: *Albanian legislation, surveillance camera, privacy, security measures, crime detection*

1. Introduction

The tension between public safety and individual privacy is a significant issue in democratic societies. Individuals and their private life are increasingly being exposed to others and it is not always clear of which way is the best way to behave. The invasion of privacy has become a common issue as a result of technological advancements, primarily due to Google. This company mainly through Google Street View, enables individuals to collect and use sensitive data that may in hypothesis be used to violate privacy, such as portraits, car license plates, or personal objects in private residences. This has led to concerns about invasion of privacy, and some countries, such as Germany, India, and Canada, have either banned or restricted immensely the use of such technology. In Albania, there is a new concerning "trend" of illegal collection of individual data through the installation of surveillance cameras in private businesses and residential areas, without any regulatory oversight to prevent the

misuse. Currently, there are around two thousand surveillance cameras installed in Tirana, monitoring every citizen without any legal criteria to guide their placement or prevent the recording of images outside of the intended restrictive spaces. From a citizen's point of view, this service might appear advantageous in the short run, but it is important to consider the potential misuse of data, which violates individual freedoms and rights, leading to abuses and blackmail, which are difficult to quantify and are not presently reflected in statistics. The only law besides the Criminal Code that guarantees privacy rights of Albanian citizens is law no. 9887, dated 10.3.2008, "On the protection of personal data", which mandates that is essential that entities that have installed these cameras are held accountable and face legal consequences for enabling an unauthorized form of surveillance, contravening the relevant laws governing such processes.

The theoretical framework concerning the prevalence or not of the relationship between an individual's privacy and their public or private interest and the degree of reciprocal respect for them, it is the core of the issue. The theories concerning the answer to this question are numerous and varied. Some of them express an unlimited willingness in favor of the public interest by bypassing any limits in terms of respect for private life in name of protecting the lives of citizens or preserving national interest in the fight against crime. In the other hand, for another category these definitions are unacceptable and even dangerous in a democratic society. In the name of protecting human rights and freedom, a process that present such great intrusion, should not only serve to maintain national security and safety but must also meet some specific rules and be in accordance with the law. Most importantly, it must be protected from the abuse of power by both the state and society and their slogan, "those who are willing to sacrifice freedom for security deserve neither", rings true.

The conclusion is clear and indisputable: the necessity of regulating of the legal framework regarding the registration of identifying data through the installation of surveillance cameras would enable the intertwining of the private sector or business interests in enhancing security measures in the areas where they exercise their right to life and economic activity on the one hand and would enable competent police authorities to lawfully use identifying data that would serve to detect or prevent criminal activity on the other.

2. The Need for Installing Security Cameras

Today society and public order are under a real and permanent threat from criminal wrongdoers. In Albania, in the fight against crime there is no organic collaboration between specialized state entities and private individuals, which could lead to an increase in the effectiveness of detecting, preventing, and punishing criminal offenders. The presence of such cooperation depends largely on the level of democratization of the society.

In these circumstances, the state has a duty to demonstrate to society the advantages of relinquishing certain aspects of their private life, meaning that privacy must be respected (Constitution of Republic of Albania, 2007), according to all international standards (European Convention on Human Rights, 1953) but taking into account the challenges posed by such a requirement. In this sense, the regulation through the law of the installation of security cameras is more than just a civic request; it is a necessity in increasing the preventive effectiveness of crime, protecting citizen's life from criminal phenomena. The installation of cameras will have a deterrent effect on criminal activity, primarily through the psychological effect it will bring. Wrongdoers will be aware that when committing a crime, it will be filmed, and there is a higher chance that they will be detected by law enforcement authorities (Albanian Criminal Code, 2022). Therefore, wrongdoers will not have the ease with which crime are being committed nowadays, everywhere on the streets, they will give double thoughts to the actions they are performing in breach of the law. Furthermore, such a measure will also have counter-effects related to the sophistication of malicious activity by wrongdoers, who, in addition must also think about eliminating visual fixation by security cameras.

The concern lies in the infringement of privacy through the surveillance that these cameras will carry out, particularly for the law-abiding citizen who is removed from crime in general. When

discussing the violation of citizens' privacy, we must consider how society will react to collective, selective, and abusive surveillance. The risk is permanent, and the only guarantee for preserving privacy will be the law.

3. An In-Depth Analysis of Some Aspects of the Law on Surveillance Cameras

In September 2016, the law was passed in Albania titled "On Additional Measures for Public Security" which aims to ensure citizen safety by placing cameras and increasing collaboration between businesses, citizens, and the police to create an uncomfortable environment for criminal activity.

The aim of the law is to establish clear and specific rules that will lead to an increase in the effectiveness of detecting and preventing crime, for both the competent authorities in general and the state police in particular, which will automatically lead to higher standards of protection and guarantees for individual's life.

In principle, we agree that a law should be used to address the goal of ensuring public safety by fulfilling a fundamental demand of society. However, good intentions alone cannot justify violating individuals' privacy, and the law must establish clear boundaries for security measures to achieve its purpose. It is essential to conduct a comprehensive legal analysis to determine whether this demand complies with the law. There are numerous legal issues concerning the relationships between the goal and the means to achieve it, mainly: **i.** the proportionality of measures in achieving the expressed goal in this law **ii.** the legitimacy of the process and **iii.** the implementation method, and the preservation and processing of data.

The law should clearly define its purpose and the means to achieve that purpose.

This law aims to make it easier for the State Police to work and cooperate with public and private organizations to identify potential cases of law infringement on public/private areas, where security cameras have been installed. The goal is to protect people, property, and ensure public safety. However, the law should not be used to violate people's privacy. It should set clear limits for security measures to achieve its purpose.

The purpose of the law should be to create guidelines for installing extra security systems based on risk analysis by the police and handling data from that analysis. Unfortunately, the purpose of this law lacks clarity and cohesiveness with the rest of the legislation. It needs to be more defined and better matched to the goals of the law. It could be complemented with secondary legislation such as: regulations, guidance and other Acts usually approved by the Albanian Commissioner of Data Protection & Privacy.

To support this criticism, we are focusing to only one important aspect, which is the analysis and assessment of risk. Article 7 of the law sets out the risk factors for assessment where it is stated:

The State Police conducts a risk assessment analysis based on the following factors:

a) The activity of the subject, which has been the target of continuous criminal attacks;
b) Criminal incidents that have compromised the subject's security in the last 5 years;
c) Exposure of the subject's environment and activity to criminal elements;
d) The frequency of local and environmental visits by individuals with criminal and penal records;
e) The type of activity being carried out;
f) The distance of the location where the activity is carried out from the police unit or inhabited centers.

It is now globally known and accepted that the classification of urban areas based on risk analysis is a direct responsibility of the State Police authorities. The State Police is not obliged to seek cooperation from any social factors to carry out such a task. Therefore, the question that arises is where the necessity of cooperation between the State Police and public/private entities lies in this determination. Similarly, problematic are other requests of the law, such as the obligation to provide data obtained from State Police security cameras upon their request as stated in article No.129 of the law "On the State Police".

The obligation of state and private institutions to provide information:

1. State institutions and private entities that have or create databases for the identification of citizens, registration of citizens' immovable property, registration of vehicles and driving licenses, commercial entities and their imports or exports, telephone subscriber identification, device identification and location, etc., for maintaining public order and security, preventing and investigating criminal offenses, are required to provide access to such information to the police officers for its recognition and processing.
2. The Director of the State Police authorizes police officers to recognize and use such information.

Apart from the fact that this law does not clarify its purpose, the same problem arises regarding the determination of the means by which this goal should be achieved. The definition of the use of high-resolution CCTV camera systems, electronic devices for identification, or direct links to the command rooms of the State Police as stated in article No.9, of the law "On Additional measures for public security", only shows the ways in which this goal will be achieved, but not the means. As per our understanding, achieving the goal of the law cannot be limited to only technical tools, but requires a whole range of organizational measures, evaluation criteria, and data analysis. The law should define criteria for evaluating the data obtained from security cameras and ensure their usefulness for police investigations and prevention, without violating procedural laws. This is similar to the process of wiretapping, where the procedures and purposes of data collection are similar. Although the technical process of obtaining data may be the same, the use of the results obtained is the same, serving in preventing, detecting, and investigating criminal activities. Interference in an individual's private life can be justified by legal reasons, which is also allowed by the European Convention on Human Rights under Article 8/2. The only difference lies in the formal procedures used to obtain and use the data.

It is unclear whether there is an international agreement that regulates the legal criteria for wiretapping. The definition of wiretapping is often based on legal analyses conducted by different countries, which makes it difficult to have a clear and precise definition that distinguishes wiretapping from other similar processes. Despite this ambiguity, we can use the wiretapping legislation in Albania to identify the legal criteria that set it apart from other processes with similar effects.

These criteria should be sufficiently clear to make the wiretapping procedure distinguishable from ambient recordings in public places. Audiovisual recordings in general and wiretapping in particular are characterized by three essential elements which are a fundamentally necessary condition of a legal process, these are:

- *Recording*, through a technical system, as the only element of data acquisition;
- *Storage* of data obtained from the process, through a clearly defined methodology;
- *Use* of this data for a legally defined purpose.

The three necessary elements to create a data system for a specific purpose must co-exist, furthermore the system itself can only be part of a process that requires an additional element:

- *Privacy* in the realization of the process, which procedurally implies whether the person subject to the process is or is not aware that their private life is being violated through an intervention, whether legal or illegal.

The four essential elements for wiretapping and camera surveillance are defined by the legal provisions in the Code of Criminal Procedure article No.221, and the law "On the interception of electronic communications". The first three elements are the same for both processes, but the fourth element, which is the secrecy of recording, constitutes the essential differentiating factor that distinguishes camera surveillance from wiretapping. In camera surveillance, it is mandatory to inform the citizen that they are being recorded sometimes asking for their consent, whereas in wiretapping, secrecy is mandatory. The citizen must be aware that their actions are being recorded and accessible to authorized authorities.

This passage emphasizes that claiming ignorance of the law is not a valid excuse for violating the privacy of individuals through surveillance cameras. The law is presumed to be known and individuals are expected to abide by it, regardless of whether or not they are aware of its specific provisions. Therefore, individuals cannot use their lack of knowledge about the law as a defense for their actions (Albanian Criminal Code, 1995). Whether an individual is aware or unaware of the recording process through security cameras has a significant impact on the legal classification of the recordings. The legal status of the recordings depends on whether they are considered routine recordings or part of a full-fledged surveillance process. This distinction is particularly important when it comes to formulating criminal charges. If the interception is deemed legal, it could have significant consequences for the legal doctrine of wiretapping. Based on the provisions of law, and considering the difficulty in proving that the recordings were made without an individual's knowledge, it is concluded that the results obtained from the registration process through security cameras have the same procedural value in a criminal process as those determined in the relevant provisions of the Code of Criminal Procedure.

The provisions in the law on camera surveillance allow for a new legal channel in criminal proceedings, in addition to the criteria for wiretapping procedures. This means that evidence obtained through security cameras can be used in a criminal process. The same applies to preventive wiretapping, which has the goal of preventing criminal activity. The entry into force of this law aims to have a direct effect on improving the quality of life in Albania by enhancing security and preventing criminal activities and other serious acts.

This Law introduces a new legal framework for surveillance, which differs from the existing types of surveillance in Albanian legislation. This new framework has unique characteristics in terms of how powers are delegated through the law. It is crucial for the law to clearly specify and define which recorded data should be classified as identifying data that can be used for a specific purpose. Also it should clearly prohibit the use of data that goes beyond the parameters of an identification procedure and transforms into a full surveillance process.

The risk of legal overlap between this new legal framework and the existing preventive surveillance process is high, given the similar ultimate goal of both processes. Law enforcers must exercise proper caution in distinguishing between the two types of surveillance to avoid any legal interference.

According to this law, The State Police should be the sole legal authority to determine the criteria for mandatory installation of surveillance cameras as an additional security measure, based on risk analysis assessment rather than on standard, obligatory and all-inclusive criteria.

It is important to define the specific purposes for which data obtained through surveillance processes via installed cameras can be used for additional security measures, investigation, and criminal proceedings. The recording, storage, and use of such data must follow precise procedures and be valid in relation to their intended purpose, particularly with regards to the sensitive nature of private life. It is crucial that these procedures are in place to ensure the procedural validity of the data's use in preventing criminal activity.

The legal process of registering through installed cameras for additional security measures is different from preventive surveillance. Authorities have analyzed and concluded that Albanian legislation only refers to procedural surveillance (Criminal Procedure Code, 2017) and preventive surveillance (On the Surveillance of Electronic Communications, 2003) under specific provisions. Albanian legislation does not recognize other forms of surveillance, meaning that the use of data obtained from security cameras as part of additional security measures *cannot be used* for other forms of surveillance. This means that data obtained from security cameras cannot be used in the same way as data obtained from procedural surveillance or preventive surveillance. However, data obtained from environmental surveillance, when performed in accordance with the law, can be directly used as evidence in a criminal process. Such a fact is also accepted by the Art.226/3 of Criminal Procedure Code, which stipulates that surveillance documentation can only be used as evidence in a criminal process if it constitutes material evidence, which can only be constituted by recordings obtained from

environmental surveillance. The use of data obtained from surveillance cameras as evidence is prohibited, and the court orders its destruction unless it meets the requirements of Article 221, paragraph 3 of the Criminal Procedure Code.

The European Court of Human Rights (PECK v. THE UNITED KINGDOM, 2003), held that the use of covert surveillance in public places and its use against the plaintiff constituted a serious interference with his private life, despite the cooperation shown in the records. The court found this to be contrary to the requirements of Article 8(2) of the European Convention on Human Rights. Since the data obtained from security cameras have no procedural value in a criminal process according to the Code of Criminal Procedure and Article 5 of the law "On the surveillance of electronic communications", it raises the question of how this data can be used for a specific purpose.

The law mandates that data obtained through surveillance cameras must be handed over to the State Police upon request for investigatory purposes. However, since such data cannot be used in a criminal process as results of a surveillance procedure, the only option left is to use them as documents representing facts, persons, or objects according to Article 191/1 of the Code of Criminal Procedure. Therefore, such data will have the value of a document in a criminal process, but not as evidence obtained through surveillance. while the use of data obtained from surveillance cameras as documents representing facts, persons or objects is legally valid for use in a criminal process, the key issue is whether the process of securing such data involved interference with private life under conditions of knowledge. The legal distinction between surveillance and other recordings lies in this fact, and it is crucial to ensure that the use of such data does not violate the privacy rights of individuals.

The proposed law allows for the installation of cameras and data recording for certain groups of people, but it is not clear how far the cameras will be able to see and record. This means that people cannot tell if their privacy is being invaded or not. While people are expected to know and follow the law, this only applies to administrative processes, not criminal cases where evidence needs to be collected in a certain way to ensure fairness. The use of surveillance cameras in criminal cases needs to be balanced with privacy rights and must be done in a fair and reasonable way.

In a potential criminal case, it must be determined whether the crime was committed under conditions where the perpetrator was completely unaware. If not, the perpetrator would likely take steps to hide their identity. Therefore, in such circumstances, there is a risk that routine surveillance could devolve into illegal wiretapping, which could create procedural complications.

The debate between the prosecution and defense will necessarily develop around the procedural concepts of "the fact does not exist" and "the fact cannot be proven to exist," as the moment of "coming to knowledge" will always be an unproven element, unless accepted by both parties. With the latter, we must understand that the existence of the fact cannot be procedurally proven with the presented evidence. Both of these elements will be subject to argumentation during a criminal trial. In such a case, the court will be left with doubt about the existence of the fact and whether wiretapping was justified for use as evidence. None of the possibilities are excluded, and as a result, the existence of the fact in procedural terms remains uncertain. This is an essential element and a reason that arises from the impossibility of proving the fact, and as a result, the judge's assessment must be based on insufficient and contradictory evidence. In such a procedural situation, since the principles of constitutional norms and criminal procedural law dictate that any doubt goes in favor of the accused, the court must declare the process null and void.

The analysis described above is developed in the circumstances where there is a gap on the determination on the use of the obtained data.

The law provides for the installation of surveillance cameras in public and private areas based on legal criteria, *regardless of whether the subject has security issues*. Until now, the installation and use of cameras has been entirely voluntary, but now it is becoming mandatory. While the law has limitations on the subjects who must comply with it, in practice, the number of subjects required to comply is much broader. Specifically, this law requires the installation of surveillance cameras by subjects that meet the following criteria (On additional measures for public security, 2016):

- Subjects that have offices, work environments and commercial activities in places exposed to additional security risks, according to the risk assessment made by the State Police;
- Subjects that have more than 50 employees or frequent visitors on a continuous basis;
- Subjects that carry out commercial activities from 11:00 pm to 6:00 am;
- Subjects that have an annual turnover of over 10 million ALL (Albanian Currency);
- Subjects that operate in the field of gambling;
- Subjects that administer open or closed environments for children, such as schools, kindergartens, nurseries or play centers, and are considered a source of increased risk according to the police;
- Subjects that engage in public transport and the transport of hazardous goods.

The law stipulates standard criteria for mandatory installation of surveillance cameras for security purposes. However, the first paragraph of Article 4 of the Law on surveillance cameras states that the installation should be based on risk assessment carried out by the State Police. This means that the decision to install surveillance cameras as an additional security measure is entirely at the discretion of the State Police without stating any limitations on the State Police's right to assess the risk analysis, giving them unlimited discretion. Even if the law were to specify a limited group of subjects who are required to install surveillance cameras based on specific criteria, the criteria established in the provision are so broad that it practically forces the vast majority of subjects to comply with this legal obligation.

The language used in the provision indicates that the risk assessment conducted by the State Police takes precedence over the mandatory criteria expressed in the relevant provisions. Both are legal elements expressed through this law, thus allowing the State Police unrestricted discretion to limit the fundamental freedoms and rights of individuals. Provisions do not clearly specify the scope and manner in which the Authorities can exercise their discretion to carry out a surveillance and interception process. According to the case law of the European Court of Human Rights, arbitrary interference by public authorities in human rights guaranteed by law through the granting of executive legal discretion to exercise unrestricted power constitutes clear arbitrariness. Therefore, the law must clearly define the boundaries of such discretion in relation to the extent of interference and ensure adequate protection against arbitrary interference with individual rights (Rotaru v. Romania, 2020).

4. Processing of Personal Data

The above analysis discusses the use of surveillance cameras for security purposes and the potential consequences of this on individuals' privacy. While the intention of the law is to prevent and detect criminal activity, the reality is that most crime occurs in a covert and sophisticated manner and may not be detected by cameras. Therefore, the use of cameras may only be effective in detecting a small percentage of ordinary crime.

There needs to be a balance between security and privacy, and the law should provide clear guidelines for the collection, storage, and use of this data to prevent any unintended consequences. It is important to mention here that currently Albania is transposing the (EU) 2016/679 Regulation of the European Parliament on General Data Protection Directive of the EU, in the local legislation with the aim to harmonize data privacy with the same standard of protection in the EU. The new low brings as a novelty stricter rules on data processing, storage, retention, transferring of personal data and higher penalties for subjects violating this rules. The concern is that in the process of constant filming, millions of recordings of individuals and events that have nothing to do with criminal activity will be obtained and stored. The fate of this data is unclear, but it will likely infringe on individuals' right to privacy. These recordings are assumed to be capable of permanent existence for at least the period they can be automatically deleted by the type of camera specified for installation, without taking into account the ancillary consequences that may arise in relation to the law "On the

protection of personal data" when it comes to the storage and use of this data. Considering the very high penalties provided in the new legislation transposing GDPR, we believe that subjects processing personal data will become more aware and responsible on the way they administer this data and strictly follow the obligation to erase data from camera as per the clause below, which stipulates that:

Additional security measures include:

a. The use of CCTV cameras with high resolution and infrared rays that store film images on an NRV/Server for up to 2 months. (Art.9, Law "On Additional measures for public security", 2016)

The Law "On the Protection of Personal Data" has been in force in Albania for some time, but it seems that both the public and the responsible institutions have limited knowledge about it. The Law "On Additional Measures for Public Security" states that personal data collected through the security systems will be processed in accordance with the existing legislation on personal data protection. This means that the use of personal data collected through these systems must follow the rules and guidelines set forth in the existing legislation. The same law includes a provision stating that data processing will be carried out in accordance with "On the protection of personal data" Law. However, the storage of such data must also be considered. Other countries have similar provisions regarding data processing. The provision mentioned states that the collected data will remain pending further processing for the purposes specified in the law. The Law "On the Protection of Personal Data" primarily concerns the role of the "controller", which refers to any individual, organization, or public authority that has control over personal data. The legal obligation to process personal data is tied to the status of "controller", which is obtained through the exercise of competencies specified in a particular law, rather than personal declarations or choices. However, the law being analyzed here does not specify who is obliged to exercise this right, only mandating that such data processing must comply with the Law "On the protection of personal data". Its provisions primarily focus on the obligation of the controllers to take additional security measures and provide information about the security certificate procedure. This certificate is obtained following this procedure: (On Additional Measures for Public Security, 2016)

1. The controller shall take security measures within 30 days from the official notification.
2. The local police shall verify if the controller has taken the prescribed measures and issue a "security certificate" within 15 days.
3. All actions provided for in this article shall be carried out after registration with the National Registration Center, in accordance with the provisions of the current legislation on the protection of personal data.
4. The issuance of the "security certificate" for buildings shall be made after the registration of the building administrators in the administrator's book of municipality.
5. The form and content of the "security certificate" shall be approved by order of the Director of State Police.

In simpler terms, the law we've been analyzing lacks clear definitions of important terms, making it difficult to apply in practice. The requirement for subjects to take security measures or obtain a security certificate does not automatically make them "Controllers" under the "Personal Data Protection" Law. Therefore, even though the camera surveillance Law, delegate responsibilities for processing data collected in accordance with the "Personal Data Protection Law", the subjects taking on these responsibilities may not have the necessary legitimacy to do so.

Furthermore we have seen a very vague role of the Data Protection Commissioner as a key stakeholder grated by the law with the right and obligation to supervise the implementation of the "Law on Data Protection" and monitor subjects that fall under its scope. Increased vigilance and control by this Agency is fundamental to guarantee that subjects are not abusing with the data, keeping them longer than what is necessary to serve the purpose, misusing them, selling them etc.

The new Law being transposed actually gives to this institution a great power to punish those entities which are operating in breach of the Law with fines which go up to 4% of their annual turnover.

The analysis highlights another problem with the law, which is the potential risk of misuse of personal data in Albania. This is due to the fact that continuous, non-stop filming of all individuals, without any positive selection criteria, creates doubts about the validity of using the recorded data. Furthermore, recordings of individuals who are granted legal immunity cannot be used as evidence in criminal proceedings, even if there is suspicion of criminal activity. This is due to the Code of Criminal Procedure, which states that for criminal offenses judged by the Supreme Court, proceedings are solely conducted by the Prosecutor's Office, thereby excluding the use of such recordings as evidence. Even though there may be instances where knowledge of suspicious criminal elements is obtained illegally, the provisions of the two laws we are referring to still allow for control of these evidences.

The issue of data misuse is a subjective factor and cannot be used as a reason for data invalidity. However, when drafting a law, it is important to take into account the legal tradition and evaluate the legal effects of similar provisions in the field where the law will operate. Unfortunately, the delegated law for processing data obtained from security cameras has negative records of misuse. This includes both the lack of professionalism of the subjects who have a legal obligation to collect and process personal data, as well as the transferring and abuse of this data by them. Media as well has published data on various public figures in breach of national privacy legislation and also international conventions. Despite the persistent publication of personal data of public figures in the name of press freedom and the public's right to information, such actions continue to violate human rights.

In Albania, there have been instances of misuse and trafficking not only of personal data but also of classified materials, including the results of procedural surveillance. In some cases, individuals have sold wiretaps and other information to criminal groups for financial or moral gain. For example, in one case, an agent of the State Intelligence Service was found to have sold wiretaps to a criminal group to be used in criminal activities. This highlights the potential risks of data misuse and transfer, and the importance of ensuring proper controls and oversight over the collection and use of sensitive information.

According to reports, the expert who drafted the Law "On the protection of personal data" has visited a prestigious hotel in Tirana on three separate occasions in one month. On each visit, the hotel staff photocopied his identification document and took it away somewhere. When the expert asked where the copy of his document was being taken, the staff replied that it was standard procedure. There are many examples that support our argument that the misuse of personal data is a widespread problem in our country. This issue has been documented in all areas of life, and therefore, delegating the processing of sensitive data obtained through the use of surveillance cameras, which is a clear invasion of an individual's private life, cannot be considered a legal safeguard for the protection of their privacy.

Given this context, delegating the processing of sensitive data obtained through the use of surveillance cameras, which is a clear invasion of an individual's private life, cannot be considered a legal safeguard for the protection of their privacy.

The technical aspect of the issue is also uncertain. The "Personal Data Protection" law establishes a legal obligation to create a data archiving system. This law applies to the processing of personal data, whether fully or partially, through automated means, as well as the processing of personal data through other means that are kept in an archiving system (On the protection of personal data, 2008). According to the "Personal Data Protection" Law, personal data must be organized in an archiving system before it is processed. However, the relevant law for processing data obtained from security cameras does not include such a requirement, and there are no specific deadlines for the retention of this data. The use of a two-month deadline for the data, cited in Article 9/1, is only a qualitative characteristic of the cameras' capacity and not a legal deadline. This means that the law lacks legal criteria for the protection of data obtained from security cameras, and compliance would require significant human and financial resources. Therefore, the law is deficient in quality from this perspective as well.

So far, we have analyzed the credibility factor in relation to the functionality of the law on data

protection. However, legal judgment cannot be considered functional if it remains based on suspicion without the possibility of confirmation. Therefore, it is necessary to analyze the law's functionality in legal terms, meaning that it should exert full power within its territorial jurisdiction.

While it is mentioned above that the new law transposing GDPR foresees fines up to 4% of annual turnover for a subject that misuses personal data, the law "On Additional Measures for Public Security", considers all its provisions as a single unit, and any violation of these provisions is regarded as a violation of the law itself and its measures for public security. It provides for administrative sanctions, in case of violation, specified in its provisions. For large businesses, the fine ranges from 50,000 to 100,000 ALL, while for small businesses, it ranges from 5,000 to 20,000 ALL. The law also considers failure to take additional security measures as an administrative offense, punishable by a fine, even if it does not constitute a criminal offense sanctioned by article No.16, of the law "On additional measures for public security. Failing to protect and misuse of personal data are considered as administrative offenses, according to the law. However, the provision specifying this is vague and lacks clarity on when the violation should be categorized as a criminal offense. This ambiguity is further reinforced by the fact that the camera surveillance law delegates the handling of personal data to the "Law on the Protection of Personal Data", and violating this law is not considered a criminal offense.

1. The cases of processing personal data in violation of the provisions of this law constitute administrative offenses and are punishable by a fine imposed by article No.39, of the law "On the protection of personal data, as follows:

a) controllers who use personal data in violation of Chapter II "Processing of Personal Data" shall be fined from 10,000 to 50,000 ALL;
b) controllers who fail to fulfill the obligation to inform, as specified in Article 18 of this law, shall be fined from 10,000 to 30,000 ALL;
c) controllers who fail to fulfill the obligation to correct or erase data, as specified in Article 19 of this law, shall be fined from 15,000 to 30,000 ALL;
d) processors who fail to comply with the obligations specified in Article 20 of this law shall be fined from 10,000 to 30,000 ALL;
e) controllers who fail to fulfill the obligation to notify, as specified in Article 21 of this law, shall be fined from 10,000 to 50,000 ALL;
f) controllers or processors who fail to take data security measures specified in Article 27 of this law shall be fined from 10,000 to 15,000 ALL.

2. Legal persons, for the above-mentioned offenses, shall be fined twice the amount determined in point 1 of this article.
3. The maximum fine is doubled in cases where there is a violation of Article 16, paragraph 2 of this law and when data is processed without authorization, as per letter "b" of paragraph 1 of Article 31 of this law.
4. The fines are imposed by the Commissioner when it is found that the obligations set forth in the law have been violated.

The analysis has shown contradictory indications regarding the use of provisions with dual standards, which would complicate the implementation of the law.

Now, let's compare the sanctions provided in the two laws with similar cases of criminal provisions.

When it comes to wiretapping, those who misuse the obtained data may be subjects to one or more criminal offenses, depending on the circumstances. These criminal offenses include:

i. “Unlawful Interference with Privacy” under Article 121 of the Criminal Code, which carries a penalty of a fine or imprisonment of up to two years;
ii. "Disclosure of Private Secrets" under Article 122 of the Criminal Code, which carries a penalty of a fine or imprisonment of up to two years;
iii. "Obstruction or Violation of Confidentiality of Correspondence" under Article 123 of the Criminal Code, which carries a penalty of a fine or imprisonment of up to two years;

iv. "Disclosure of Secrets by Citizens" and "Disclosure of Secret Acts or Data" under Articles 295 and 295/a of the Criminal Code, which provide for fines and imprisonment of up to 2 years, as well as fines or imprisonment of up to 5, 3, 6, or 8 years.

The comparison between the penalties for criminal offenses related to wiretapping and the administrative sanctions for violating personal data protection laws reveals a contradiction in the legal system. Criminal charges against individuals for violating wiretapping laws carry severe penalties, while those who violate personal data protection laws face only administrative sanctions. This discrepancy and does not reflect the seriousness of violating an individual's privacy and fundamental rights. The main principle is that the law must ensure equal treatment for all citizens, but when the penalties for violating wiretapping laws are much more severe than those for violating personal data protection laws, we believe that there is an immediate need for regulatory intervention, which could be done through the new Law being adopted, transposing GDPR, by imposing higher and stricter fines/penalties.

5. Conclusions and Recommendations

The law, according to the defined parameters, has many quality limitations related to:

- The prediction in the law of legal spaces regarding the determination of the criteria that trading subjects must meet to install surveillance cameras, depending solely on the risk assessment by the state police;
- The recordings made by these cameras must only present video footage and under no circumstances can audio recordings be made.

Recommendation: The law on surveillance cameras should be reviewed and revised to include clear criteria for their placement, prohibit audio recording, and ensure individual privacy rights are protected. It should be easily understandable to all stakeholders.

The law aims at enhancing public safety and security by allowing the State Police to work with public and private organizations, however is not clear and well-defined in terms of its purpose and means to achieve that purpose. The law must define clear principles and rules to: i. ensure that cooperation between the State Police and private entities in practice is achievable and ii. the obligation to provide data by entities/subjects etc., obtained from security cameras needs to be further clarified. The new law transposing GDPR will provide also for technicalities on how these data should be transferred, roles & responsibilities on the individuals that have the right to access these data, the means of transfer and other security measures to ensure that the data are not misused or dispersed. Additionally, the law should establish clear boundaries to ensure that individuals' privacy is not infringed upon while pursuing its objectives.

Recommendation: The law should be revised to align its purpose with its goals, set clear limits for security measures, avoid duplication of existing obligations, and ensure cooperation between State Police and public/private entities. A well-defined law will enable effective collaboration to protect people, property, and ensure public safety while respecting individual privacy rights. It might be the case that the data Protection Commissioner office approves guidance and practical advices to be followed by both parties state Police and Lao private entities when carrying out the process for data transfer etc.

The only authority that should be allowed to install security measures and use the results from security cameras should be the State Police, based on a risk assessment analysis on a case-by-case basis. General criteria lead to excessive and covert surveillance in the name of security, and the State Police should be the only entity to have the powers on deciding on the installation of security systems based solely on risk assessment analysis. Other general criteria should be removed from the law and may be used only as guiding criteria operational purposes by the Police in assessing risk analysis.

Recommendation: It is recommended that laws and regulations related to surveillance should be revised. The focus should be on ensuring that the privacy rights of individuals are protected while still providing for public safety and crime prevention. The responsible use of surveillance

technologies is paramount, and the State Police should be commended for their efforts in ensuring that their deployment is limited to specific environments and cases, with no room for misuse or abuse. In this view the new law under transposition, should set new criteria, surveillance cameras are considered necessary in a certain area this should be done in compliance with strict rules, incl. here for example a clear notification in a visible pace which notifies citizens on the existence of the cameras, or such as for example in hue spaces such as big enterprises. Shopping centers etc., expressed consent by employees/customers for being monitored by camera through paper, digital means, apps etc.

Having clear guidelines for the use of data obtained through surveillance and recording processes is essential for protecting individual rights and ensuring a fair legal process. Without such guidelines, there is a risk of data misuse and violation of individual rights. By improving the provisions of the law, both in terms of form and content, the use of surveillance and recording data can be effectively regulated. Therefore, it is important for the government to consider these recommendations carefully and make necessary revisions to the law to ensure the protection of individual rights.

Recommendation: Based on the above analysis, it is recommended that the new law on "Data protection" transposing the GDPR Directive of the EU, currently under revision by the relevant Commissions of the Parliament" should take into consideration and provide clear guidelines for the use of data obtained through the surveillance and recording process. The law must provide guidelines on limitations on the use of data, which could potentially violate individuals' rights, ensure that the use of data obtained through surveillance and recording is properly regulated through secondary legislation and frequently monitored by the competent Authorities. This will help to safeguard individuals' rights and ensure that the legal process is fair and just.

In accordance with the law proposed for approval, additional security measures should be taken, such as the use of high-resolution CCTV cameras with infrared rays and storing the film images on an NRV/Server for a maximum of 2 months. It is also recommended that the legal implications and consequences of storing and using personal data in compliance with the law on personal data protection be considered.

Recommendation: To ensure that citizens' rights are protected, it is recommended that additional guarantees be provided for data obtained through legal surveillance processes, such as CCTV footage. To safeguard citizens' rights, this could involve reviewing and revising current laws and regulations, consulting with legal experts and stakeholders, and implementing training and education programs for relevant personnel. The treatment of surveillance data should be more stringent than personal data under data protection laws, to prevent unintended consequences and negative effects on innocent citizens.

In conclusion, below we present a brief summary of the key changes to the law:

- The installation of cameras should be accompanied by a notification requirement.
- The obligation to install cameras should only apply to specific categories based on fixed criteria.
- The installation and use of these cameras should be under the financial and technical responsibility of the state police. The state should never delegate security to private entities. The state collects taxes, and from these taxes, it should also invest in national security.
- Collection and use of data should be done exclusively by the police. Involvement of administrators/owners of entities in these recordings would make the use of recordings unreliable, regardless of whether they intervene or not.
- Hackers can easily intervene in this data, and under these conditions, data misuse will be a major problem. In many countries on the continent, data misuse is a matter for the appropriate courts.

6. Acknowledgment

All non-English materials used in this manuscript for academic purposes only are translated from Ph.D. Iv Rokaj

References

Albanian Criminal Code, (1995). https://qbz.gov.al/preview/a2b117e6-69b2-4355-aa49-78967c31bf4d.

Criminal Procedure Code of Republic of Albania, (2017). https://www.pp.gov.al/rc/doc/kodi_i_procedures_penale_28_07_2017_1367_5285.pdf.

European Convention on Human Rights, (1953). https://www.echr.coe.int/Documents/Convention_ENG.pdf.

On Additional measures for public security (2016). https://www.idp.al/wpcontent/uploads/2020/11/Ligji_nr_192016_PER_MASAT_SHTESE_TE_SIGURISE_PUBLIKE.pdf.

On the protection of personal data, (2008). https://mb.gov.al/wp-content/uploads/2018/02/ligji_9887_per_mbrojtjen_e_te_dhenave_personale.pdf.

On the Surveillance of Electronic Communications, (2003). https://www.pp.gov.al/rc/doc/ligj_per_pergjimet_e_komunikimeve_825.pdf.

On the State Police, (2014). https://www.asp.gov.al/wp-content/uploads/2022/12/Ligji_PSH-1.pdf.

PECK v. THE UNITED KINGDOM, (2003). European Court of Human Rights. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22003-687182-694690%22]}.

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (2016). https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Rotaru v. Romania. (2020). European Court of Human Rights. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58586%22]}.

The Constitution of the Republic of Albania, (2017). https://klp.al/wp-content/uploads/2020/02/Kushtetuta-2017.pdf.