Abstract

Purpose: This study aims to discuss the roles and responsibilities of state agencies using drones to prevent terrorism, which threatens national security, which is distinct from general criminal offenses. In this regard, first of all, we will look at the recent development status of drones and the definition of legal concepts, and then discuss the rational operation plan of drone use in the field of national security. In the use of drones for counter-terrorism, in consideration of the legislative purpose of the Personal Information Protection Act, the principles of personal information protection, rights of data subjects, and responsibilities of the state must be observed, and evidence under the Criminal Procedure Act. It is necessary to review exceptional regulations because it is a national security violation that mainly infringes on national legal interests.

Method: Considering the increasing trend of drone use for crime prevention due to the recent development of advanced science and technology, the legality and requirements of drone use are discussed through literature research focusing on legal problems that can be a problem when using drones and related precedents.

Results: In the case of crimes that threaten national security, such as terrorism, laws can limit the basic rights of the people. For this purpose, if a state agency uses drones, a serious violation of the basic rights of the people’s privacy is involved. The legal basis for information and investigation activities must be clearly established.

Conclusion: Therefore, It is necessary to meet the actuality of the crime, the necessity and urgency of the evidence preservation in order for Intelligence and Investigative agencies to collect evidence using drones for crimes of national security violations such as terrorism and to be recognized for their proof ability.

[Keywords] Drone, Personal Information Protection, Terrorism, National Security, National Security Crime

1. Introduction

Today, the drone industry is showing explosive growth in the world, and its application field is also expanding to all fields of society, such as military, commercial, and agriculture, and the technology of drone equipment is being developed faster than expect. In this situation, the state not only needs to meet the expectations of the people to respond to crimes that threaten the lives, bodies, and property of individuals, but also proactively and actively responds to crimes that become more intelligent and specialized as time goes by. They have a great responsibility to defend their enemy values.

In particular, the need to approach national security crimes that threaten our society and the national community differently from general crimes is undeniable [1]. In the case of major developed countries, various police activities such as maintenance of public order and criminal investigations. Of course, drones are actively being used in the field of national security,
such as terrorist and spy tracking, and discussions on privacy invasion due to the use of drones are actively taking place.

However, despite the serious changes in the environment for the geographical, historical, military, and international political security of Korea, there is still a lack of academic discussions on the use of drones in the public sector\cite{2}. The use of in is absolutely inadequate. Of course, even if the basic rights of the people are restricted for national security or public order, the essential contents cannot be infringed. Therefore, for the preemptive and active role of the intelligence agency against the violation of national security that threatens the existence of our society and constitutional order It is effective to use state-of-the-art equipment such as drones\cite{3}.

This study intends to legally review the authority and responsibility of Intelligence/Investigation agencies for the use of drones in counterterrorism.

\section*{2. Review of Application of Personal Information Protection Act}

\subsection*{2.1. General principles of the personal information protection act}

\subsubsection*{2.1.1. Principles of the personal information protection act}

Article 3 of the Personal Information Protection Act stipulates the principles of personal information protection as follows. First, the personal information controller must clarify the purpose of processing personal information, and must legally and legitimately collect only the minimum amount of personal information necessary for that purpose. Second, the personal information controller must properly process personal information within the scope necessary for the purpose of processing personal information, and must not use it for purposes other than that purpose. Third, the personal information controller must ensure the accuracy, completeness and up-to-dateness of personal information to the extent necessary for the purpose of processing personal information. Fourth, the personal information controller must safely manage personal information in consideration of the possibility of infringement on the rights of the data subject and the degree of risk according to the processing method and type of personal information. Fifth, the personal information controller must disclose matters related to the processing of personal information such as the personal information processing policy, and must guarantee the rights of the information subject such as the right to request access. Sixth, the personal information controller must process personal information in a way that minimizes invasion of the privacy of the data subject. Seventh, if the personal information controller can achieve the purpose of collecting personal information even if the personal information is processed anonymously or under a pseudonym, if anonymization is possible, by anonymity, if the purpose cannot be achieved through anonymization, by a pseudonym make sure it can be processed. Eighth, the personal information controller must make an effort to obtain the trust of the information subject by complying with and practicing the responsibilities and duties stipulated in this Act and related laws.

\subsubsection*{2.1.2. Rights of the data subject}

The subject of personal information has the right to receive information on the processing of personal information in relation to the processing of his/her personal information, the right to select and decide whether to consent to the processing of personal information, the scope of consent, etc., and to confirm the processing of personal information. The right to request access to personal information (including issuance of a copy), the right to request suspension, correction, deletion, and destruction of personal information, and the right to be relieved of damage caused by the processing of personal information in accordance with prompt and fair procedures (Article 4 of the Personal Information Protection Act).
2.1.3. Responsibilities of countries, etc. within the scope of purpose

The Personal Information Protection Act does not explicitly stipulate information collected using drones. However, according to the provisions of Article 2, No. 1, the information collected through the drone is 'information about a living individual, and information that can be used to identify an individual through name, resident registration number, and video. In the case of includes easily recognizable by combining with information', it should be considered that it can be protected as personal information protected by the Personal Information Protection Act.

In addition, personal information controller refers to 'public institutions, corporations, groups, individuals, etc. that process personal information by themselves or through other people in order to operate personal information files for business purposes', so if a public institution uses a drone when collecting personal information, the Personal Information Protection Act may be applied. Information/Investigation agencies are also subject to the Personal Information Protection Act as a “public agency” specified in Article 2, No. 6 of the Personal Information Protection Act[4].

2.2. Whether the regulations on image information processing equipment apply

Looking at the definition regulations for image information processing devices under the Personal Information Protection Act(Article 2, No. 7), image information processing devices are 'continuously installed in a certain space to shoot images of people or objects, or use wired/wireless networks. It is a device that transmits through the system and is prescribed as 'device prescribed by Presidential Decree', but because drones are not continuously installed in a certain space, they cannot be included in image information processing devices for interpretation. Therefore, it would be difficult to apply the regulations on the installation and operation restrictions(Article 25) of image information processing equipment. Therefore, it can be interpreted that the personal information protection law is widely applied to drones that are suspended or patrolled in a specific airspace[4].

2.3. Admissibility of evidence for filmed images

2.3.1. Compulsory investigation vs voluntary investigation

When judging the legal nature of using drones for photographing or video shooting by state agencies(Intelligence and Investigative Agencies) targeting national security infringement offenses, discussions under the Criminal Procedure Act are developed over whether photography is a voluntary or compulsory investigation. Due to the development of science and technology, new investigative techniques such as photography and interception have appeared, and there are cases in which the subject's rights or interests are violated, although physical coercion or legal obligations are not imposed on the subject. As a result, the criteria for determining compulsory disposition, which divides discretionary and compulsory investigations, has changed. The concept of compulsory disposition, which was previously judged based on whether to impose physical coercion or legal obligations, is determined based on the infringement of important rights or interests. In the case of photography, even if the subject is not subject to physical coercion or legal obligations, and a covert and momentary method is taken to prevent the subject from being noticed, the rights or interests of the other party are violated, resulting in serious consequences in criminal proceedings. If so, it is a common belief in Korea that it should be interpreted as a forced disposition. Therefore, it is necessary to grasp the legal nature of taking pictures or videos using drones equipped with video equipment in the process of investigation as a forced investigation[5].

2.3.2. Warrantism and exceptional tolerance
In the case of permitting the use of drones by state agencies for national security crimes, the target, method, and permitted range should be specifically specified in the warrant. On the other hand, if the suspect is concerned about destroying the evidence, it is necessary to prescribe it as an exception because it requires an emergency and there is no time to receive a warrant. In this case, it would be desirable to request a warrant without delay. The same exceptions should be applied to cases where there is a concern that there is a serious threat to national security (e.g., terrorism).[6]

In addition, since drones can move in the air, they can only shoot specific targets that they want, and because they can continuously track and collect information, they are more likely to invade privacy compared to CCTV. Therefore, it is necessary to allow the drone to collect data only to the target or location specified in the warrant, and to prevent unlimited information collection by setting the period of information retention.

2.4. Provision of personal image information to a third party

2.4.1. Provided to a third party within the purpose of collection

Even if image information is collected or used in accordance with Article 25 of the Personal Information Protection Act, provision of the image information to a third party is governed by Articles 17 and 18 of the same Act. In the case of public institutions, there are special provisions in the Act of Article 15, Paragraph 1, Item 2, which is a condition that permits provision to a third party in Article 17, Paragraph 1, Item 2. If it is unavoidable for the public institution under subparagraph 3 to perform the duties under the jurisdiction, it will be possible to provide it within the scope of collection[7]. This is because the collection, use, and provision of personal information in the public sector are subject to the principle of legal retention, and that public institutions are obligated to perform the duties stipulated by laws and regulations[8].

2.4.2. Provided by a third party

The reason why the Personal Information Protection Act puts normative clarity and purpose binding as a principle of protecting personal information is to allow the processing of personal information to a person who intends to collect and use personal information under an original purpose. Therefore, even if it is provided to a third party, it is limited to the purpose connected to the original purpose of collection, and more stringent conditions are placed on the provision beyond the purpose of collection. Therefore, in principle, the act of using personal information other than the purpose for which it was provided or providing it to a third party should be prohibited. Otherwise, the infringement of the rights of the information subject such as the right to self-determination of personal information or the right to correct or delete personal information due to the leakage and illegal distribution of personal information will be serious. However, as in Article 19 of the Personal Information Protection Act, if the data subject has given a separate consent or if there are special provisions in other laws, it is exceptionally permitted.

Even if you look at the case of the Personal Information Protection Committee, it can be seen that the use of the person who has been provided or the provision of it to a third party is strictly handled. In the case of the police, they are in charge of preventing, suppressing and investigating crimes in accordance with Article 2, No. 2 of the Act on the Performance of Duties by Police Officers, and receiving CCTV video information related to the missing persons from local governments for the search and investigation of the missing persons. In a case where it is questionable whether video information related to a runaway person, not a missing person, can be viewed by the guardian of the runaway person, the Personal Information Protection Committee meets the purpose of the crime prevention, suppression, and investigation for which the National Police Agency was provided, that is, runaway. It was judged that
a guardian could read it only if there was a reason to believe that a person's runaway was related to a crime[9].

2.4.3. Exceptions to collection and provision restrictions

The video information collected and used by CCTV is mainly related to Article 58, Paragraph 1, Item 2, “Excluding the application of personal information processed for national security purposes”[10]. This is because, in the event of a terrorist or national security emergency, if an integrated defense posture is needed, CCTV footage installed in various places becomes a very important support factor. In this case, the manipulation of CCTV, the subject of filming, the provision of video information to a third party, etc., are excluded from many regulations under the Personal Information Protection Act. Of course, the basis and purpose related to national security must be specific and clear.

The Personal Information Protection Committee also determined that local governments could use and provide CCTV video information from the integrated control center for national security purposes. For example, the integrated defense operations under the United Defense Act are directly related to national security, and to support this, the integrated defense support headquarters of local governments can use and search the image information of the integrated control center of the local government, and can operate CCTV[11]. In addition, it is said that local authorities can also receive video information from the integrated control center from local governments when necessary, such as in the case of training related to national security[12].

3. Review of the Application of the Criminal Procedure Act

3.1. Legality of filming and limitations of application

The Criminal Procedure Act stipulates in Article 199 that “Compulsory Disposition is limited to cases where special provisions are provided in this Act, and must be taken within the minimum required range”, but there are no special regulations for photographing or filming. In addition, when taking a picture using a drone, unlike general shooting, remote control and aerial photography are possible, so it will be possible to take a picture from a wider angle than that of existing national institutions. When a camera capable of shooting at night and a sensor capable of face recognition are combined, it is possible to collect a variety of information that is difficult to collect with conventional photography.

3.2. Admissibility of Evidence of images collected by drones

The Supreme Court ruled, “Everyone has the freedom not to be photographed without permission, but such freedom is not protected without limit from the exercise of state power, and considerable restrictions are imposed if necessary for the purpose of ensuring the security of the state, maintaining order, and public welfare. When the crime is being investigated by the investigative agency, if the crime is currently being committed or is immediately after the crime, there is a need and urgency to preserve evidence, and if the film is taken by a generally accepted method, the above filming will be performed without a warrant. It has been judged that it cannot be concluded that it is illegal to lose it”[13].

In addition, the Supreme Court riled, “The filming of a video of the defendants meeting with North Korean spys in Japan or China was made because it was necessary to preserve evidence of the meeting of the defendants, and filming was generally permitted. It was judged that it could not be considered illegal because it was done in a way that was out of significance or it was a forced disposition without a warrant.”[14].

3.3. In case the investigation agency secures the evidence collected by the drone
In principle, the domestic majority theory is taking the position that it is reasonable to assume that the law of exclusion of illegal collection of evidence is applied to the collection of evidence of the cause of death. This is because, as long as there was a violation of the evidence collection procedure, it is essentially not a matter of whether the subject of the collection is an investigative agency or a private agent. However, since the law of exclusion of illegal collection and evidence stipulated by the Korean Criminal Procedure Act has the main purpose of suppressing illegal acts by investigative agencies, it is unreasonable to apply the same principle to the collection of evidence by death. It is also true. Considering these points, even evidence collected illegally by an investigative agency is not excluded in all cases, and if the contents of the violation do not infringe the actual contents of due process, the definition of discovery of substantive truth. Theories and precedents agree that the ability to testify can be acknowledged with a request.

If the subject of video shooting using drones is the cause of death, it will be the act of shooting the crime scene directly. However, taking into account the actuality and directness of the evidence and the efficiency of collection, it is uniformly disallowed to adopt it as evidence for criminal proceedings. However, it should be considered that the law on the exclusion of illegal collection evidence applies when the cause of the cause of the death of the evidence-gathering ‘significantly and essentially violates the moral or privacy rights of others.’ Cases of serious and essential infringement of the right to privacy should be embodied in realistic legislation.

4. Reasonable Operation Plan of Drone

For “personal information requested to be collected or provided for the purpose of analyzing information related to national security” in Article 58 (1)2 of the Personal Information Protection Act, personal information requested for collection or provision for the purpose of information analysis related to national security even in order not to apply to the country, the minimum types or behaviors and types of information related to national security must be specified. Through this, it is expected that the public’s trust in Intelligence or Investigative Agencies will be improved as well as the relief of vague fears of infringement of personal information for national security or inspections.

When conducting Intelligence/Investigation activities on national security infringers, guidelines for using drones should be implemented taking into account general matters (Articles 3-5 of the Personal Information Protection Act) that do not fall under the grounds for exclusion. That is, ①clarity of the purpose of personal information processing, which falls under the principle of personal information protection(Article 3 of the Act), legitimacy and legitimacy of information collection, prohibition of use for other purposes, accuracy, completeness, up-to-dateness, safety, anonymity Infringement minimization is guaranteed, and personal information controllers must comply with legal responsibilities and obligations, and the rights of data subjects such as the right to request access must be guaranteed. ②In terms of the rights of the information subject(Article 4 of the Act), the right to receive information on the information processing of the personal information subject, the right to select and decide whether or not to consent and the scope of consent, the right to request access(including issuance of a copy), The right to request suspension, correction, deletion and destruction of personal information, and the right to remedy in accordance with the prompt and fair procedure of damages should be protected. ③In the responsibilities of the state, etc. within the scope of the purpose(Article 5 of the Act), the government and local governments take measures to prevent harm caused by prohibition of collection of personal information other than the purpose of personal information, misuse, abuse, and indiscriminate monitoring and tracking, etc. Laws and ordinances should be enacted and revised in accordance with the purpose of the law, improving the laws and regulations to protect the rights of people, improving
unreasonable social practices, respecting, promoting and supporting autonomous personal information protection activities.

5. References

5.1. Journal articles


5.2. Books


5.3. Additional references


6. Contribution

6.1. Authors contribution
<table>
<thead>
<tr>
<th>Initial name</th>
<th>Contribution</th>
</tr>
</thead>
</table>
| YSL          | - Set of concepts ☑  
|              | - Design ☑  
|              | - Getting results ☑  
|              | - Analysis ☑  
|              | - Make a significant contribution to collection ☑  
|              | - Final approval of the paper ☑  
|              | - Corresponding ☑  
|              | - Play a decisive role in modification ☑  
|              | - Significant contributions to concepts, designs, practices, analysis and interpretation of data ☑  
|              | - Participants in Drafting and Revising Papers ☑  
|              | - Someone who can explain all aspects of the paper ☑  |