Journal of Korean Law | Vol. 18, 413-431, August 2019

Notable Cases on Criminal Law

*Jinyoung Hong**
*translated by JKL student editors***

I. Conscientious Objection to Military Service: Constitutional Court Decision 2011HeonBa379 et al. Delivered on Jun. 28, 2018, and Supreme Court Full Bench Decision 2016Do10912 Delivered on Nov. 1, 2018 (whether the refusal of enlistment by conscientious objectors constitutes "justifiable grounds" according to Article 88, Paragraph 1 of the Military Service Act)

1. Former decisions

Article 5, Paragraph 1 of the Military Service Act (heretofore referred to as the "Military Service Categorization Provision") classifies military service into active duty service, reserve service, supplementary service, preliminary military service, and wartime labor service. Article 88, Paragraph 1, Subparagraph 1 (heretofore referred to as the "Penalty Provision") punishes any person who has received a notice of enlistment for active duty service and fails to enlist in the military, even after the expiration of the following report period from the date of enlistment without justifiable grounds by imprisonment with labor for up to three years. Previous Supreme Court decisions interpreted "justifiable grounds" as used in the Penalty Provision as that which is "in principle premised on

* Assistant Professor, Seoul National University School of Law

** Translation was done by the Journal's student editors (Ra In Kang, Yura Kim, Sangjoon Lee, Hojoon Choo)

the existence of an abstract military duty and affirmation of performance thereof, but shall be limited to conditions which could justify nonperformance of military duty materialized by the decision of the Commissioner of the Military Manpower Administration etc., such as diseases, which cannot be attributed to actions of the non-performer." According to this interpretation, refusing to enlist due to religious beliefs or one's inner conscience could not be acknowledged to be justified grounds. Therefore, conscientious objectors had no choice but to refuse enlistment and face criminal punishment according to the Military Services Act. Conscientious objectors who were punished as such amounted to 500~600 per year.

From the beginning of the 21st century, the view that such punishment was unreasonable and alternative military service should be introduced began to receive public attention. On Jan. 29, 2002, Judge Park Si-hwan of the Seoul Southern District Court requested for adjudication by the Constitutional Court on the constitutionality of the above Penalty Provision on the grounds that it may infringe on the freedom of conscience under Article 19 of the Constitution of the Republic of Korea. Furthermore, on May 21, 2004, Judge Lee Jeong-ryeol of the same court rendered a judgement of acquittal to Jehovah's Witness defendants who were indicted with charges of refusing to enlist, deciding that conscientious objection corresponded to the Penalty Provision's "justifiable grounds."

However, the Supreme Court and Constitutional Court did not agree with the lower court's new point of view. First, the Supreme Court Full Bench Decision 2004Do2965, delivered on July 15, 2004, upheld the Supreme Court's previous interpretation of the above Penalty Provision. A noticeable change was the admission that if "the right upon which a non-performer based his decision to evade enlistment is guaranteed by the Constitution and furthermore that right is acknowledged to have a superior constitutional value surpassing the legislative purpose of the above article," it should be seen that there exists justifiable grounds to refuse enlistment. This opened up the possibility to expand the scope of justifiable grounds compared to previous Supreme Court decisions. However, even in light of this interpretation, the Supreme Court did not view the right of conscientious objectors to realize their decision of conscience as superior to the constitutional value of national defense, considering national security

circumstances and the continuing military confrontation between North and South Koreas, and decided that conscientious objectors must still be punished according to the Penalty Provision.

Following the Supreme Court decision, the Constitutional Court, in the 2002HeonGa1 decision, delivered on Aug. 26, 2004, ruled that the above Penalty Provision was not unconstitutional. In this decision, the Constitutional Court wrote that, while the freedom of conscience is crucial in guaranteeing an individual's maintenance of human dignity and expression of personality, national security is also an exceedingly important public interest, prohibiting the request of immoderate legislative experiments that would obstruct national security, and considering that the judgement of legislators upon the security situation of the nation must be respected, legislators have a wide discretion in deciding whether and in what form alternative military service should be implemented. Therefore, the Court saw that, considering the current national security situation, the social demand for equality in conscription, and the various restrictions that may accompany the adoption of alternative military service, the legislative judgment that it is inappropriate at the time to adopt alternative military service cannot be deemed to be clearly unreasonable or plainly wrong. However, at the same time, the Court stated that "now is the time to seek a national solution of our own through a serious social discussion with respect to how to take the conscientious objectors into account, instead of neglecting and ignoring their suffering and inner conflict," and recommended that legislators seek the adoption of an alternative military service that could balance the freedom of conscience of conscientious objectors and the issue of equality in conscription.

While, in accordance with the above Supreme and Constitutional Court decisions, conscientious objectors have typically been sentenced to an eighteen-month "fixed sentence,"[1] lower courts have rarely but continuously been giving sentences of acquittal and requesting adjudication on

1) According to Article 65 Para. 1 Subpara. 2 of the Military Service Act and Article 137 Para. 1 Subpara. 2 of the Enforcement Decree of the Military Service Act, those who are sentenced to one year and six months or more of imprisonment are transferred to wartime labor service and will no longer receive notices of enlistment. Therefore, lower courts have been giving eighteen-month sentences to conscientious objectors, nearly without exception, since 2001.

constitutionality, and such sentences of acquittal have dramatically increased since the mid-2010s, numbering about a hundred at the time of the below Constitutional Court decision. This is thought to have been the result of the spreading view in the judicial branch that the respect for legislators' freedom of legal formation cannot take precedence over the judicial branch's responsibility to protect minority groups, considering that there was no serious or earnest legislative discussion over alternative military service.

2. Decision of the Constitutional Court

The Constitutional Court, in the 2011HeonBa379 et al. decision, delivered on Jun. 28, 2018, reversed its previous views and ruled the current Military Service Categorization Provision, which does not provide alternative military service for conscientious objectors, as unconstitutional, and decided that the current provision will continue to be applied until it is revised by legislators to introduce alternative military service with a deadline of Dec. 31, 2019. The Court's reasoning was that excluding alternative military service from the military service categorization did not meet the principle against excessive restriction, specifically the rule of least restrictive means and balance between legal interests, for the following reasons:

> ① Rule of least restrictive means: Even if alternative military service is adopted, its impact on national defense capabilities cannot be seen to be meaningful, and if the government implements objective and impartial screening procedures and strict *ex post facto* supervision while securing fairness by considering the difficulty and length of active and alternative military services so as to remove any reason to evade active military service, it is possible to avoid the problems of screening difficulty and the increase of those who evade military service by falsely claiming conscientious objection. Therefore, the Military Service Categorization Provision does not satisfy the rule of least restrictive means.
>
> ② Rule of balance between legal interests: While the legal interests of "national security" and "equality in military service" that

> the Military Service Categorization Provision pursues are highly important, assigning conscientious objectors to public services rather than imprisoning them can better realize national security and public interest in a wider sense, whereas due to the lack of alternative military service in the Military Service Categorization Provision, conscientious objectors are subjected to a minimum of eighteen months of imprisonment and significant tangible and intangible disadvantages that follow. Therefore, the Military Service Categorization Provision does not satisfy the rule of balance between legal interests.

Meanwhile, only four Justices (Lee Jin-seong, Kim Yi-soo, Lee Seon-ae, Yoo Nam-seok) found the Penalty Provision to be partially unconstitutional, leaving it effective.[2] This is because, of the six Justices who agreed with the nonconformity to the Constitution of the Military Service Categorization Provision, Justices Kang Il-won and Seo Ki-seok had a different interpretation of "justifiable grounds" from the other four Justices. The four Justices who supported the partially unconstitutional opinion found the part of the Penalty Provision which penalizes conscientious objectors to be unconstitutional, based on the existing Supreme Court interpretation of the Penalty Provision. On the other hand, Justices Kang Il-won and Seo Ki-seok suggested that "conscientious objection must be seen as "justifiable grounds" since punishing conscientious objection without provisions for alternative military service is unconstitutional," and found that, since "penalization for conscientious objectors is only caused by the legislative defect of not having provisions for alternatively military service combined with the Supreme Court's interpretation that conscientious objection does not constitute "justifiable grounds" as in the Penalty Provision," it is sufficient to decide the Military Service Categorization Provision as nonconforming to the Constitution, and no decision of unconstitutionality is necessary for the Penalty Provision.

Typically, adjudication on constitutionality of law is based on the Supreme Court's established interpretation of the law in question, which

2) According to Article 23 Para. 23 Subpara. 1 of the Constitutional Court Act, a vote of six or more Justices is required to rule a statute unconstitutional.

means the decision of constitutionality by Justices Kang Il-won and Seo Ki-seok, presupposing the Supreme Court interpretation to be incorrect, was very unusual. Some view this to have "effectively" been a decision of unconstitutionality for the Penalty Provision, but there is a large difference between the Constitutional Court giving and not giving an official decision of unconstitutionality in the holding. If there is a decision of unconstitutionality in the holding, the Penalty Provision would lose its effect retrospectively according to Article 47, Paragraph 3 of the Constitutional Court Act, allowing re-adjudications on former convictions (according to Paragraph 4 of the same article) and criminal compensation based on judgements of acquittal given at the re-adjudications. However, because the two Justices above chose the decision of constitutionality, the Penalty Provision was not found to be unconstitutional, and conscientious objectors who were given a final and conclusive conviction now cannot be rescued through re-adjudication and criminal compensation procedures. Furthermore, the interpretation of the Penalty Provision given by the two Justices are not binding upon the Supreme Court, so if the Supreme Court did not change its own precedent, the assertion that the former interpretation was incorrect was in danger of falling on deaf ears.[3] The Supreme Court decided to refer the case to the full bench on Jun. 18, 2018, immediately before the adjudication of the Constitutional Court, so the focus was on whether the Supreme Court would change its former interpretation of "justifiable grounds."

3. Decision of the Supreme Court

On the 2016Do10912 case on violation of the Military Service Act, referred to the full bench, the Supreme Court held a public pleading on Aug. 30, 2018 and decided on Nov. 1, 2018 to change its former interpretation, finding that "conscientious objection based on genuine

3) However, the "partially unconstitutional" opinion of the four Justices seems to be no different from the "limited unconstitutionality" decisions that the Supreme Court does not recognize, so even if there was a "partially unconstitutional" decision for Article 88 Para. 1 of the Military Service Act, it may be said that there would have been no effect on cases currently being heard or requests for retrials.

conscience constitutes "justifiable grounds" in the above Penalty Provision." In the decision, the majority opinion (nine Justices) found that, because the "justifiable grounds" clause is intended for the resolution of conflicts between norms that cannot be specifically enumerated by legislators, the normative clash and coordination between freedom of conscience and the duty of national defense ought to be resolved through the literal interpretation of "justifiable grounds" as this is where the conflict directly arises. Specifically, while the freedom of conscience is an essential condition to maintain the dignity of humans as a moral, spiritual, and intellectual being, permitting conscientious objection cannot be necessarily deemed as causing serious difficulties in efforts toward preserving national security and strengthening national defense, considering the nation's economic and defense power, the public's high level of security awareness, and other factors. Based on this finding, the majority opinion decided that "forcing genuine conscientious objectors to perform military service accompanied by participation in military training and bearing arms and punishing the same for nonperformance may be excessively restricting the freedom of conscience or distorting the inherent substance of such freedom." In conclusion, "uniformly forcing the performance of military service against conscientious objectors and imposing criminal punishment for nonperformance are not only unreasonable in light of the constitutional system that guarantees fundamental rights, such as the freedom of conscience, and the overall legal order, but also contravene the spirit of free democracy pertaining to the embracement and tolerance of the minority."

Four Justices gave a dissenting opinion, arguing that the legal reasoning given in the 2004 full bench decision still holds.

4. Comments

While it is clear that the legal decision of whether to punish conscientious objection is a problem of weighing between the constitutional freedom of conscience and the duty of national defense, there was disagreement among judges on whether this weighing and balancing of norms should be done at a constitutional level or through the literal interpretation of "justifiable grounds" at the level of specific application of the Penalty Provision. Judges who were of the former opinion requested for

adjudication by the Constitutional Court, while those who were of the latter opinion gave judgements of acquittal. Eventually, the Supreme Court resolved the dispute by treating it as a matter of interpreting "justifiable grounds."

It is not easy to determine what specific cases correspond to refusing to enlist on "justifiable grounds." On "conscience," the Supreme Court, based on the general definition of "a strong and genuine voice within guiding us that one's value as a human being will be destroyed if one does not act according to his or her conscience," adds that "conscience" in the context of "justifiable grounds" for conscientious objection must be a "devout, firm, and sincere belief." Because the lack of justifiable grounds must be proved by prosecutors as a constituent element of crime, defendants who claim conscientious objection must present *prima facie* evidence that their conscientious belief is devout, firm, and sincere, and prosecutors may prove the nonexistence of genuine conscience by impeaching the credibility of the presented evidence. In the case of this full bench decision, the majority opinion decided that the defendant's refusal to enlist may correspond to "justifiable grounds" stemming from genuine conscience and remanded the case for further proceedings, based on the grounds that the defendant, who was baptized on Nov. 16, 1997 at the age of 13 by influence of his father, a Jehovah's Witness, has been living according to his beliefs and refused to enlist since 2003 when he received his first notice of enlistment, and that the defendant's father and younger brother have also refused to enlist and have been penalized. However, further questions remain, such as whether sincere conscience can be acknowledged for types of conscientious objection other than Jehovah's Witnesses, whether sincere conscience can be acknowledged for selective refusal, whether the criteria for sincere conscience will change after alternative military services are adopted, and whether requiring defendants to prove the sincerity of their conscience erodes the purpose of guaranteeing freedom of conscience. Meanwhile, the form of alternative service that the government has pre-announced would allow conscientious objectors to stay at correctional facilities and assist correctional administration for 36 months, and if this bill is passed, there is a possibility of constitutional appeals claiming that the long period of service corresponds to punitive alternative service.

II. Supreme Court Decision 2017Do9747 Delivered on Nov. 29, 2017 (whether it is legitimate and permissible to search and seize the electronic data stored in a remote data storage medium)

1. Outline of the Case

An investigator with the National Intelligence Service ("NIS") found the e-mail addresses and passwords used by a suspect as a result of the search and seizure of the universal serial bus (USB) drive discovered in the vehicle registered in the name of the suspect.

Accordingly, investigative agencies applied for a warrant for search, seizure and inspection with the Seoul Central District Court, identifying the specified details as follows: items to be searched, seized and inspected as "of the total of ten e-mail accounts provided by Chinese companies A and B, which the suspect utilized as means of espionage communication with Bureau No. 225 of the North Korean Agency on Espionage against South Korea, e-mail accounts used from the point of their opening to November 24, 2015 related to the National Security Act violation charges; contents stored in various inboxes including that of incoming e-mails, various other categories including the saved drafts category, and various document files within the drive linked with the e-mail accounts, which have been sent or received, the hard copies of the contents, and data storage media where the contents are saved," places to be searched, seized and inspected as "personal computers (PC) for the Internet installed in the office of Korea Internet & Security Agency ("KISA") geographically located in Songpa-gu, Seoul," and methods of search, seizure and inspection as "recording a video on the Internet PCs installed in the office of KISA, a public institution certified as a national information communication center, logging in to the acquired e-mail accounts by inputting the e-mail IDs and passwords that the NIS found by the search and seizure to the log-in bars at the homepages of the Chinese companies A and B in the presence of an expert of KISA and an outside forensic expert, and afterward sealing and seizing the hard copy of the materials serving as criminal evidence of the National Security Act violation as well as the data storage media where the materials are

selectively saved."

The Seoul Central District Court issued a warrant for search, seizure and inspection, adding the condition to the aforementioned claim that "the suspect must be given an opportunity to participate in the search and seizure." In accordance with the warrant, after logging in to the e-mail accounts of the company A used by the suspect by inputting the passwords, the NIS investigator extracted, printed out and saved 15 e-mail messages and their attached files in relation to the National Security Act violation charges. (On the other hand, logging in to the e-mail accounts of the company B failed due to the occurrence of additional authentication items.)

2. Summary of the Decision

Search and seizure may be conducted against the owner or possessor of an object, and it also holds true when the owner or possessor is a defendant or suspect (*see* Articles 106(1)-(2), 107(1), 108, 109(1), and 219 of the Criminal Procedure Act). Moreover, search and seizure of electronic data stored in a data storage medium must be conducted by either printing out or copying only the part(s) relevant to the suspected criminal facts that are grounds of the issue of the warrant. However, the data storage medium itself may be seized provided that the method of printing out or copying within a set scope is deemed impossible or significantly impracticable for achieving the purpose of seizure (*see* Articles 106(3) and 219 of the Criminal Procedure Act).

An Internet service user can be deemed the owner or possessor of the given electronic data, under the service use agreement with the Internet service provider, who has the right of access to the e-mail account opened using the Internet service and its relevant server; is authorized to draft, revise, review, and manage electronic data such as an e-mail created on the given e-mail account; and is the holder of protected interests including the right of confidentiality and freedom of privacy with respect to the contents of the electronic data. Meanwhile, an Internet service provider, under the service use terms and conditions, takes the responsibility for maintaining and managing the server in which the electronic data is stored, allows the requester to gain access to the given server without confirming his identity

so far as the typed-in ID and password match those registered by the Internet service user, and thus generally permits transferring and copying the given electronic data to other data processing units such as computers interlinked via information and communications networks.

Consequently, under the statutory interpretation of the Criminal Procedure Act, it is permissible for an investigation agency to search and seize against a suspect as an Internet service user the electronic data such as e-mails stored in the suspect's computer or any other data processing unit. This corresponds to compulsory disposition of an object through which search and seizure of the electronic data is performed against the owner or possessor of them.

Furthermore, even in the case that the electronic data to be searched and seized does not exist in a computer or any other data processing unit located in the location for search as indicated in the search and seizure warrant but is stored in a remote server or any other storage medium which is managed by a third party and connected to the above-mentioned data processing unit via information and communications networks, there is no need to view the search and seizure of such electronic data differently. This is because the search and seizure conducted by the investigation agency still targets the electronic data owned by or in possession of the suspect as the agency, pursuant to a warrant issued in lieu of an access to the suspect's e-mail account; gains access to the remote storage medium using the same approach as the suspect ordinarily does, that is, by inputting the legitimately acquired e-mail ID and password of the suspect through the computer or any other data processing unit at the search site indicated in the warrant; and downloads the suspect's e-mail-related electronic data saved in the remote storage to the data processing unit at the search site or otherwise displays such data on the data processing unit's screen.

Even when an investigation agency accesses a remote storage medium and downloads the stored electronic data to the data processing unit at the search site or otherwise displays such data on the data processing unit's screen as mentioned hereinbefore, such an act is based on the authority for access and disposal of the suspect's electronic data granted by the Internet service provider and the general access protocol. Therefore, unless there are any special circumstances, it cannot be conclusively deemed a contravention

of the Internet service provider's intent.

Furthermore, in the light of the purport of the requirement under Articles 109(1) and 114(1) of the Criminal Procedure Act that a warrant specifically describes the place(s) to be searched, as well as the characteristic of electronic data that transfer and duplication of data can be easily done between data processing units or storage media insofar as they are interconnected via information and communications network, gaining access to a remote data storage medium connected via information communications network using a data processing unit located at the search site cannot be deemed broadening the scope of the place of execution permitted by the search and seizure warrant and violating the aforementioned provisions of the Criminal Procedure Act. The reason is that the search is conducted on the electronic data either downloaded to, or displayed on the screen of, the data processing unit located at the search site from a remote storage medium via information communications network, and the seizure is conducted by either printing out or copying the electronic data existing on the data processing unit within a set scope. Thereby the comprehensive series of procedure from search to seizure is wholly conducted at the place indicated in the search and seizure warrant.

Considering the above circumstances, the search and seizure of those parts relevant to the suspected crime enabled by the search and seizure warrant issued in lieu of access privileges for the suspect's e-mail account and conducted on electronic data legitimately accessed, downloaded, and printed from a remote-access storage medium would be permitted as a legitimate enforcement of compulsory disposition of an object that is conducted within the minimum scope necessary for the smooth and appropriate execution of the search and seizure warrant and in a manner considered to be generally acceptable in light of its means and purposes, and would fall under the enforcement measures deemed necessary for the execution of search and seizure warrant pursuant to Article 120(1) of the Criminal Procedure Act. The fact that the remote-access storage medium is located overseas alone does not render this legal principle inapplicable.

3. Comments

When an investigative agency attempts to search and seize data stored

on an e-mail account, it is common for that agency to lack access information, such as the password, for that account. In such cases, the investigative agency would obtain a search and seizure warrant for the e-mail account pursuant to Articles 219 and 107 of the Criminal Procedure Act and then enforce the warrant against the Internet service provider to obtain information stored on the e-mail account. Furthermore, in cases where the relevant server, operated by an overseas Internet service provider, is located overseas, the standard practice would be to secure evidence by requesting cooperation from the country where the server is located through necessary international law enforcement coordination procedures in order to obtain information that is not voluntarily provided by the relevant Internet service provider.[4)]

However, in this Supreme Court case, the investigative agency had already acquired the information necessary to access the account by lawfully obtaining the suspect's email ID and password information through legitimate search and seizure procedures. There was a lack of precedent with respect to the possibility for the investigative agency to secure evidence through searches and seizures regarding electronic information, such as e-mails, stored on remote-access storage media by obtaining a separate search and seizure warrant from the court and accessing the e-mail account on behalf of the suspect (the so-called problem of 'remote searches and seizures') and the question of whether the investigator may obtain evidence in this manner without going through international law enforcement coordination procedures in the event that a server is operated by a foreign Internet service provider in a foreign country (the so-called problem of 'extraterritorial searches and seizures'). On the lower court level, a judgment that denied the permissibility of the above (i.e. the lower instance decision of the Supreme Court ruling at hand, namely Seoul High Court Decision 2017No23 delivered on Jun. 13, 2017) and another judgment that affirmed the permissibility of the above (Seoul High Court Decision 2017No146 delivered on July 5, 2017) competed, and the Supreme Court decision discussed here standardized the practice by

4) It is possible to obtain information, albeit limited to user information and access logs, from Microsoft, Google, Twitter, Facebook etc. by sending the Korean warrant and request form to the relevant Internet service providers.

ruling that remote and extraterritorial searches and seizures such as in this case are permitted. In reaching such a conclusion, the Supreme Court established that Internet service users have the status of "owners or possessors" of electronic information according to Internet service use contracts, allowing for Internet service users to be the subject of searches and seizures pursuant to Article 106(2) of the Criminal Procedure Act. Considering that there is little controversy concerning remote searches and seizures as to whether the investigative agency can have a suspect submit electronic data to the agency by directly accessing his/her own e-mail account, the Supreme Court appears to have determined that the investigative agency's direct access of the suspect's electronic information on behalf of the suspect, when within the effective scope of the warrant issued in lieu of the suspect's access privileges, is essentially no different from obtaining such information through the suspect. Moreover, the Supreme Court ruled out the possibility of holding cases such as the case at hand to be instances of extraterritorial exercise of criminal jurisdiction, by maintaining that the spatial scope of enforcement of searches and seizures permitted in the warrant cannot be deemed to extend overseas as long as the process of searching and seizing is conducted entirely within the spatial scope stipulated by the warrant.

The Criminal Procedure Act of the Republic of Korea was enacted when the objects of seizures were understood to be limited to spatially defined physical objects, which is rather disconnected from the current reality in which information can cross borders through virtual, digital spaces. The Supreme Court, then, can be seen to have responded to the reality of criminal investigation by proposing a most flexible interpretation of relevant provisions in the Criminal Procedure Act within the limits of textual interpretation, considering legislative insufficiencies in a digital era. While such a practical need cannot be denied, the question remains as to whether the concepts of 'owner' or 'possessor' allow themselves to be easily grafted onto the matter of electronic information, as well as the possibility of justifying the complete disregard of the extraterritorial nature of searches on electronic information stored on overseas servers in order to foreclose the interpretive controversy with respect to the spatial scope of the execution of search and seizure warrants. The duty of the legislator, then, would be to update and adjust relevant provisions in the Criminal

Procedure Act to provide a platform for the judiciary to strictly adhere to the principle of legality in the arena of compulsory disposition.

III. Constitutional Court Decision 2016Hun-Ma264 Delivered on Aug. 30, 2018 (constitutionality of packet sniffing)

1. Outline of the Case

The head of the National Intelligence Service (NIS) was issued permission to impose communication-restricting measures[5] across a total of 35 instances between 2008 and 2015 regarding the investigation of individual A's suspected violation of the National Security Act and enforced the restrictions with the purpose of wiretapping A's mobile phone, Internet cable connection, and other telecommunications methods. The above communication-restricting measures included six instances of wiretapping between October 9, 2013 and April 28, 2015 on the Internet connection service provided by SK Broadband Co., Ltd. and installed at B Research Facility under the Petitioner's name. These restrictions constituted what is known as "packet sniffing," a wiretapping method with which an investigative agency obtains information by intercepting 'data packets,' units of electric signals on which electronic information can be transferred over Internet connections.

With respect to the above, the Petitioner filed a petition for constitutional complaint claiming that the Petitioner's basic rights such as the right to confidentiality and freedom of communication, the right to confidentiality and freedom in private life, etc. were violated by Article 5(2) of the Protection of Communications Secrets Act, which served as legal basis for the six instances of telecommunication restriction measures implemented to wiretap the above Internet connection service registered under the Petitioner's name.

5) Under the Protection of Communications Secrets Act, "communication-restricting measures" are defined as any censorship of mail or any wiretapping of communications.

2. Summary of the Decision

Interception of Internet cables is conducted through packet interception, through which data packets travelling over Internet cables are captured and reassembled and the content thereof becomes accessible. This form of interception thereby restricts the secrecy and freedom not only of communications but also of privacy.

Given the widespread and daily use of the Internet, there is a need to permit the interception of telecommunications made through the Internet for the prevention of crimes that endanger national security, public safety, safety of property and life or for the investigation of crimes that have already occurred. Thus, the Court recognizes that the provision at issue serves a legitimate purpose and uses appropriate means.

Interception of Internet cables allows state investigative agencies to gain access to data pertaining to personal communications and the intimate realm of individual privacy. Therefore, legislative safeguards aimed at preventing the abuse of power and minimizing interference with fundamental rights by state investigative agencies are required not only at the stage when the court grants permission for communication-restricting measures but also at later stages, including during and after the execution thereof. In particular, when state investigative agencies conduct the interception of an Internet cable through packet interception, all the data travelling through that cable, including information concerning its users, are captured in the form of packets and transmitted intact to state investigative agencies. Hence, through such packet interception, an incomparably wider range of data is collected by state investigative agencies than through other communication-restricting measures. Therefore, supervisory or regulatory legal measures are strongly required to ascertain whether state investigative agencies have not collected or retained information related to a third party or irrelevant to the criminal investigation during and after the execution of interception, and whether they have used and processed data in accordance with the original authorized purpose and scope of such acts. Nevertheless, the act at issue does not contain any provisions on the procedure for processing a vast amount of data collected through interception by state investigative

agencies other than Article 11, which imposes a confidentiality obligation to any public official who has been engaged, and Article 12, which restricts the use of materials acquired through communication-restricting measures. Under Article 9-2 of the act at issue, the prosecutor should notify a subscriber to telecommunications of the fact that the communication-restricting measures are executed but does not need to notify the subscriber of the grounds for the execution of such measures, and the subscriber is not even notified of the above fact in the case of prolonged investigation or when the prosecutor determines to suspend an indictment, adding to the difficulty in objective regulation and *ex post facto* control. Additionally, under Article 12 Subpara. 1 of the act at issue, the contents of telecommunications acquired through wiretapping may be used to investigate, prosecute, and prevent crimes that are related to the crimes as to which the court authorized the execution of the communication-restricting measures. Therefore, the Court cannot exclude the possibility that state investigative agencies may abuse their power to collect information about a specific person, including his or her whereabouts.

In light of the above, the provision does not satisfy the principle of the least restrictive means since it specifies the interception of Internet cables as one of the communication-restricting measures merely on the ground that such interception serves criminal investigative purposes, although no legal safeguards are in place to prevent the abuse of power and to minimize infringement on the fundamental rights by state investigative agencies during and after the execution of such interception. Moreover, the balance between the public interest to be attained by the provision and the private interests to be infringed by the provision is considered not to have been struck, since authorizing the interception of Internet cables would pose a serious threat to the secrecy and freedom of communications and privacy of individuals. Accordingly, the provision violates the principle of proportionality and thus infringes on the fundamental rights of the complainant.

3. Comments

The Protection of Communications Secrets Act of the Republic of Korea was established on December 27, 1993, in order to generally regulate the

secrecy and freedom of communication. The establishment of the act at issue is the result of shared vigilance on secrecy and freedom of communication due to the so called "Chowonbokjip Wiretapping Case." Under Article 5(1), the Protection of Communications Secrets Act bans "communication-restricting measures," which include inspecting contents of mail and wiretapping telecommunications, in principle, and only permits communication-restricting measures when necessary for investigating or preventing certain crimes given the permission granted by the court. Under Article 2 Subpara. 2, the act at issue defines "telecommunications" comprehensively as "transmission or reception of all kinds of sounds, words, symbols or images by wire, wireless, fiber cable or other electromagnetic system, including telephone, e-mail, membership information service, facsimile and radio paging," which can be evaluated as a legislative safeguard for avoiding a legal vacuum with respect to newly emerging means of communication following the advancement of science and technology. Packet interception has been used by the National Intelligence Service for investigating violations of the National Security Act since 2004, and the Supreme Court, deeming packet interception to be a kind of telecommunications, has allowed packet interception which fulfills the requirement prescribed in Article 5(1) of the Protection of Communications Secrets Act unless there are special circumstances. However, there has been criticism that there exists no regulatory legal measure with respect to post-processing of the data despite the vast amount collected through packet interception, which is much more than through other communication-restricting measures, and as seen above on summary of the decision, the decision of the Constitutional Court seems to accept such criticism.

In addition to his claim of infringement on the secrecy of privacy and freedom of communications, the petitioner of this case also claimed that packet interception violates the warrant requirement prescribed in the Constitution since it is no better than allowing a general warrant, which is constitutionally prohibited, because the provision lacks specific descriptions of the subject (person or thing) of the interception. The Constitutional Court, considering that the claim of violation of warrant requirement can be contained within the claim of infringement on the secrecy of privacy and freedom of communications, did not rule on the

claim separately. However, it seems that the Court implicitly rejected the complainant's claim of violation of warrant requirement by affirming that investigation agencies should be able to investigate through interception of internet cables and, on this premise, issuing a decision of nonconformity to the Constitution. In accordance with the decision of Constitutional Court, legislators bear the responsibility for eradicating the unconstitutionality of Article 5(2) and making reasonable provisions for monitoring or regulating the use of data obtained through the interception of internet cables, and the provision would be tentatively applied until the legislature amends it by March 31, 2020.

***

***