

# Remote Access Investigation in Japan

Mariko NAKAMURA

## Abstract

Japan introduced the remote access investigation in 2011 to provide for necessary domestic legislation in adopting the Convention on Cybercrime. Since the remote access investigation is supposed to be conducted at the exact moment of search and seizure, it is unclear whether the same investigation may be conducted later. Additionally, if the subjects of this investigation are present in foreign countries, it is also unclear whether law enforcement may remotely access those subjects without permission of the given countries, or whether courts may allow evidence seized by such investigation. Therefore, this article discusses the remote access investigation and recent judgments related to these issues.

## Key Words

Remote Access Investigation, Digital Data, Cybercrime

## Table of Contents

- I Introduction
- II Overview of Remote Access Investigation
- III Precedents of High Courts
- IV Scholarly Discussions
- V Conclusion

## I Introduction

Japan introduced the remote access investigation in 2011, through the Act for Partial Revision of the Penal Code, etc. to Respond to an Advancement of Information Processing (Act No. 74 of 2011) to provide for necessary domestic legislation in adopting the Convention on Cybercrime (the Budapest Convention, hereinafter “the Convention”). The Convention requires member countries to reinforce the proceedings for search and seizure of computer data.

Since the remote access investigation is supposed to be conducted at the exact moment of search and seizure, it is unclear whether the same investigation may be conducted later. Additionally, if the subjects of this investigation are present in foreign countries, which is highly probable in this digital society, it is also unclear whether law enforcement may remotely access those subjects without permission of the given countries, or whether courts may allow evidence seized by such investigation. Therefore, this article discusses the remote access investigation and recent judgments related to these issues.

Part II of this article explains the remote access investigation and the reasons for its introduction. Part

III reviews precedents of High Courts regarding some types of remote access investigations. Part IV considers whether it is possible to conduct the remote access investigation with the consent of a user ; whether it is possible to conduct it with a warrant for inspection after search and seizure ; and whether it is possible to conduct it without either of gaining permission of a country where a server exists or requesting international assistance in investigation, and if not, whether this affects the admissibility of the fruits.

## II Overview of Remote Access Investigation

The new provision for the remote access investigation, which is Article 218 (2) of the Code of Criminal Procedure (hereinafter “the Code”), stipulates the following.<sup>1)</sup>

“Where the article to be seized is a computer, and with regard to a recording medium connected via telecommunication lines to such computer, it may be reasonably supposed that such recording medium was used to retain electronic or magnetic records, which have been made or altered using such computer or electronic or magnetic records which may be altered or erased using such computer, the computer or other recording medium may be seized after such electronic or magnetic records have been copied onto such computer or other recording medium.”

Although the construction of this article is complicated, the remote access investigation, put simply, assumes search and seizure of digital data contained in servers such as Gmail and iCloud. We can currently reserve digital data not only on personal computers themselves or recording media physically connected to the computers but also on servers by using networks. In this situation, it may be difficult to identify servers that contain necessary data to be seized, and even if possible, criminals could destroy evidence by transferring or deleting data before search and seizure or it would substantially interfere with operations of Internet service providers (ISPs) to seize servers themselves.<sup>2)</sup> Additionally, even when law enforcement agencies seize computers, it was not clear for them to be able to access data that is not saved on the computers themselves.

The remote access investigation, therefore, enables law enforcement to remotely access servers connected by networks to computers to be seized, copy necessary data to the computers or other recording media and seize the computers or recording media. For example, law enforcement can access storage servers or mail boxes that reserve files or e-mails created by computers to be seized, copy only necessary data to the computers or recordable compact discs (CD-Rs), and seize the computers or CD-Rs.

---

1) Translations of Japanese Codes in this article refer to Ministry of Justice : Japanese Law Translation, <http://www.japaneselawtranslation.go.jp/?re=02>, last accessed 2020/8/25.

2) Law enforcement may also conduct a seizure of records created under a record copying order (i.e., “having a custodian of electronic or magnetic records or a person with the authority to access electronic or magnetic records copy the necessary electronic or magnetic records onto a recording medium or print said records out, and seize said recording medium”), which assumes those who are supposed to be cooperative with warrants, such as ISPs.

### III Precedents of High Courts

The first influential precedent of a High Court regarding the remote access investigation was a 2016 judgment of the Tokyo High Court,<sup>3)</sup> relating to cases of counterfeiting of private and official documents bearing the seal or signature of another, damage to buildings and arson of uninhabited buildings. The defendant was asked to forge documents, and ordered accomplices who applied to a job to vandalize or torch buildings. The police searched the defendant's residence and seized, *inter alia*, a laptop computer upon a warrant for search and seizure on charges of other cases. Although the warrant permitted copies through remote access to a mail server, the police could not conduct the investigation because the password for the computer had not been found out. Then, the police learnt of the defendant's access history on a Gmail account that was used for receiving orders for false documents on a website and got a warrant for inspection of the computer to access the mail server as a necessary measure,<sup>4)</sup> which is allowed incident to an inspection. The police accessed the Internet by a computer into which contents of the seized computer were duplicated, logged into the Gmail account by cracking the password and viewed and saved mails upon the warrant. The Tokyo High Court affirmed the court below to have excluded reports of the inspection as follows :

"The inspection of this case was to access a mail server from an Internet-connected personal computer into which contents of the personal computer of this case were duplicated and view and save e-mails, etc., which was a compulsory disposition<sup>5)</sup> that may not have been conducted upon a warrant for inspection. Moreover, because the server may be in a foreign country, it can be said that the police should have taken investigative measures of international assistance in investigation, etc. Therefore, although considering that the warrant for inspection into the personal computer was issued, which means that the infringement of the defendant's right had been judicially reviewed, and that the warrant for search and seizure of this case to seize the personal computer permitted remote access to copy the e-mails, etc. that were viewed and saved by the inspection, the illegality of the inspection is substantially significant."<sup>6)</sup>

---

3) Tokyo High Court, 12/7/2016. *See, e.g.*, Hiroki SASAKURA, *Jurist* (1518) 182 (2018), Yoshimitsu YAMAUCHI, *Kenshu* (832) 13 (2017), Ko SHIKATA, *Criminal Law Journal* (58) 143 (2018), Takashi UTO, *Hogaku Kyoshitsu* (445) 152 (2017) (all in Japanese text).

4) This is a procedure that may be conducted to accomplish the objective of inspection, which is explained in detail later ((2) of section 4).

5) Article 197 (1) of the Code provides that "[w]ith regard to investigations, examination necessary to achieve the objective of said investigation may be conducted; provided however, that compulsory dispositions may not be applied unless special provisions have been established in th[e] Code," which means that an investigation deemed to be compulsory must be conducted by following the specific procedure (in principle, with an appropriate warrant), as provided in the Code.

6) This is the standard of the exclusionary rule that the Supreme Court adopted for the fruits of illegal investigations, which is explained in detail later ((3) of section 4).

As explained above, the remote access investigation is provided only for search and seizure and there is no provision about it for inspection. An inspection is a procedure to verify the presence, nature, state or content of a subject and seems to be so extensive as to include remote access. However, any rights or interests that may be infringed by the remote access investigation are not only those relating to a seized computer, but also those relating to another computer such as a server that is often managed by a person other than the one who owns the seized computer. Although it is not clear whether the legislature intended to exclude the remote access investigation as an inspection when there is a warrant for inspection to specify a storage area of a remotely accessed computer, it is explained that the newly added remote access investigation is supposed to be conducted, only in advance of seizure, into a storage area of a computer that is used by nature as a unit with another computer to be seized.<sup>7)</sup>

As to the remote access investigation across borders, the judgment is read as finding the investigation of this case illegal, also considering that the investigation may have been conducted across borders although it hedged by the phrase “it can be said” for the police to take investigative measures such as international assistance in investigation. This coincides with the idea that, when it is found that a recording medium of electronic or magnetic records to be copied exists in a foreign country and it is not a case where an access is permissible according to Article 32 of the Convention,<sup>8)</sup> it is deemed to be generally preferable to gain permission of the country or request international assistance in investigation while refraining from conducting the remote access investigation because it may cause trouble in relation to the sovereignty of the country.<sup>9)</sup> Since it is not unusual for servers to exist in foreign countries that are not often disclosed as confidential matters, the judgment may virtually close the door to the remote access investigation.<sup>10)</sup>

However, the following two precedents of High Courts appear willing to accept the remote access investigation across borders. One is a 2018 judgment of the Osaka High Court,<sup>11)</sup> regarding cases of display of obscene recording media containing electronic or magnetic records and public indecency, where the de-

---

7) Noriaki SUGIYAMA & Masayuki YOSHIDA, *Comments on the Act for Partial Revision of the Penal Code, etc. to Respond to an Advancement of Information Processing*, vol.2, Lawyers Association Journal 64 (5) 1049, 1092 (2012) (in Japanese text).

8) Article 32 (Trans-border access to stored computer data with consent or where publicly available) of the Convention, provides as follows :

“A Party may, without the authorisation of another Party :

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically ; or
- b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.”

9) SUGIYAMA & YOSHIDA, *supra* note 7 at 1095.

10) It is said that few remote access investigations have practically been conducted since the judgment (SHIKATA, *supra* note 3 at 148).

11) Osaka High Court, 9/11/2018. *See, e.g.*, Satoshi KURITA, *Kenshu* (849) 25 (2019), Tomohiro FUKANO, *Journal of Police Science* 72 (4) 151 (2019), Hiroshi NAKAJIMA, *Hogaku Seminar* (768) 130 (2019), Takashi UTO, *Hogaku Kyoshitsu* (462) 157 (2019), Makoto IBUSUKI, *Shin Hanrei Kaisetsu Watch* (24) 187 (2019) (all in Japanese text).

fendants ran sites of video posting and distribution and made obscene videos open to the public. The police searched the codefendants' company, and accessed servers from personal computers upon consents to copy or take pictures of digital data. The police also accessed servers from appropriate devices outside of the company upon consents to copy digital data. The servers were deemed to be managed by companies in the United States. Although the Osaka High Court found that the consents were not voluntary in this case, it basically affirmed the court below to have allowed the digital data into evidence because the process to acquire them was not significantly illegal. The following is the relevant portion of the remote access investigation across borders :

"There has been no international consensus about whether the remote access investigation, etc. by Japanese law enforcement into a recording medium such as a server in a foreign country upon a remote access warrant prescribed in Article 218 (2) of the Code violates the sovereignty of the country and Article 32 of the Convention ..... does not explicitly provide when such investigation is not permissible. However, some point out that, when it is found that a recording medium of electronic or magnetic records to be copied exists in a foreign country and it is not a case where an access is permissible according to Article 32 of the Convention, it is preferable to gain permission of the country or request international assistance in investigation while refraining from conducting the remote access investigation because it may cause trouble in relation to the sovereignty of the country. Therefore, there is room to think that it is internationally illegal for Japanese law enforcement to conduct the remote access investigation, etc. across borders, whether it is compulsory or not, without permission of the country through international assistance in investigation, etc., by violating the sovereignty of the country where the recording medium to be investigated exists. And when the investigation violates the sovereignty of the country and is internationally illegal, the illegality is also deemed to make it illegal under the Code.

However, apart from when the country identifies the conduct of Japanese law enforcement and finds it internationally illegal, otherwise, there is a doubt that the sovereignty of the country is violated in the first place. Setting this aside, even if the sovereignty is violated, it is hard to imagine that the rights or interests of people concerned are infringed as long as the investigation is conducted practically complying with the Code ; and because ..... the remote access investigation, etc. of this case may be evaluated to have been conducted upon a warrant for search and seizure judicially reviewed in essence, it is doubtful that the defendants have the standing to argue the illegality. Moreover, because illegally obtained evidence is excluded only when the investigation is significantly illegal ..... and it is deemed unreasonable to allow it into evidence in terms of deterrence over illegal investigations in the future, the illegality of violating the sovereignty described above itself cannot be immediately a reason to exclude evidence obtained by the investigation."

The judgment seems to premise that the police could have lawfully conducted the remote access investigation across borders with a user's legal and voluntary consent,<sup>12)</sup> which may be a dictum because it found

---

12) Whether search and seizure may be conducted with consent is another question, which is discussed later ((1) of

the consents that the police actually gained involuntary. Despite the involuntary consents, it held that the illegality of the remote access investigation of this case was not substantially significant, considering the circumstances of the case and differentiating the illegality to be taken into account for the exclusionary rule as a national matter from the possible international illegality caused by the remote access investigation beyond the range of Article 32 of the Convention.

The other is a 2019 judgment of the Tokyo High Court,<sup>13)</sup> regarding cases of breaking into a residence, rape causing injury, robbery and theft. The defendant trespassed into a victim's residence and attempted to rape her causing injury in the process, and robbed her of money ; trespassed into another victim's residence and stole valuables ; and trespassed into another victim's residence without justifiable grounds. The police accessed a server of the defendant's Gmail account, upon consent of his then-girlfriend, from a tablet that she possessed and that was synchronized to the defendant's Gmail account set for his smartphone, and viewed his search history to take pictures of it. The Tokyo High Court found that there was a violation of laws and regulations in the proceedings of the court below to have allowed a report of the pictures because the investigation was compulsory and should have been conducted with a remote access warrant although it affirmed the court below because the violation had not affected the judgment.<sup>14)</sup> It also mentioned the remote access investigation across borders, as described below :

"Generally, whether the remote access investigation may be conducted when it is possible that a server exists in a foreign country is not provided under the Convention and has not gained international consensus. Even if it is preferable to request international assistance in investigation to remotely access in such a situation, conducting it without the request is not deemed to immediately affect a judgment about its illegality under the Code, aside from that this may cause a diplomatic problem. Therefore, the fact that the remote access investigation of this case was conducted without requesting international assistance in investigation is not a matter to be considered in judging the admissibility of the fruits."

Although the judgment found that the remote access investigation of this case was illegal because the investigation was conducted without a warrant, it showed a similar perspective to differentiate the illegality to be considered for the exclusionary rule as a national matter from the possible international illegality caused by the remote access investigation across borders.

#### IV Scholarly Discussions

Although there have been no judgments by the Supreme Court as yet, what can be deduced about the remote access investigation is that (1) it may be conducted with a remote access warrant, but it is still open

---

section 4).

13) Tokyo High Court, 1/15/2019. *See, e.g.*, Maki KATANO, Kenshu (850) 77 (2019) (in Japanese text).

14) A High Court shall reverse the court below when there are grounds set forth in certain provisions, including Article 379 of the Code, which offers one ground for appeal that "there was a violation of laws and regulations in the court proceedings and it is clear that that violation has affected the judgment."

to discussion on whether it is possible to conduct it with the consent of a user ; (2) it may be conducted in advance of seizure, but it is still open to discussion on whether it is possible to conduct it with a warrant for inspection after search and seizure ; and (3) it may be conducted across borders by gaining permission of a country where a server exists or requesting international assistance in investigation, but it is still open to discussion on whether it is possible to conduct it without either of them, and if not, whether this affects the admissibility of the fruits. This section examines scholars' opinions on these matters.

### (1) Remote Access Investigation with Consent

Article 32 of the Convention allows a Party to “access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system” without permission of another Party. Therefore, there is no violation of the sovereignty of a country where a server exists by remotely accessing data with a user's voluntary consent.<sup>15)</sup>

However, one of the rules of the National Public Safety Commission to be complied with by the police bans “voluntary search” without a warrant because it may become an issue of whether the investigation has been actually conducted with voluntary consent.<sup>16)</sup> Although there is no such provision in the Code itself, it is needless to say that the voluntariness of consent should be judged carefully.<sup>17)</sup> In executing a warrant for search and seizure, law enforcement may ask a person with authority to access a remote computer and download the necessary data,<sup>18)</sup> or do it themselves with consent. This leads to no infringement of his/her rights or interests if the cooperation or consent is found to be truly voluntary.<sup>19)</sup> Additionally, the rights or interests of those who manage servers do not appear to be virtually infringed when they do not have the authority to generally access data controlled by each user such as personal e-mail accounts.<sup>20)</sup>

### (2) Remote Access Investigation as an Inspection

Although law enforcement may conduct “necessary measures,” such as unlocking or unsealing, incident to

15) This view coincides with the investigative practice (FUKANO, *supra* note 11 at 161).

16) See, IBUSUKI, *supra* note 11 at 188 (implicitly criticizing the premise of the second case cited above).

17) Kazuo KAWAKAMI, et al. (eds), Dai Kommentar Keijisoshoho [Great Kommentar of the Code], 2nd ed., Seirin Shoin, Tokyo, Japan (2012), vol.4 at 548 (Masayuki IKEGAMI & Hiroshi KAWAMURA) (in Japanese text) (hereinafter “Kommentar”).

18) Article 111-2 applied *mutatis mutandis* by Article 222 (1) of the Code allows law enforcement who executes a warrant for search and seizure to “ask the person subject to the measure to operate the computer, or for some other form of cooperation.”

19) Masahito INOUE, *Computer Network to Hanzai Sousa* [Computer Networks and Criminal Investigations], vol.2, Hogaku Kyoshitsu (245) 49, 54 (2001) (in Japanese text).

20) See, SHIKATA, *supra* note 3 at 148-149 (referring to the rights or interests of ISPs in relation to the remote access investigation across borders) ; and Kohei KISHI, *High-Tech Hanzai to Sousa Tetsuzuki* [High-Tech Crimes and Investigative Procedures], *Sousa Kenkyu* 47 (10) 18, 20 (1998) (in Japanese text) (discussing who is to be subject to the remote access investigation in relation to inspection). See also, INOUE, *supra* note 19 at 57 (suggesting notification to the given country before or after the remote access investigation across borders).

search and seizure or inspection, or for seized properties, the remote access investigation does not seem to constitute the measure because it involves another computer that is often managed by a person other than the one who owns the computer to be seized or inspected. Therefore, the question here is whether it is possible to conduct the procedure with a warrant for inspection that specifies a storage area of a remotely accessed computer.

Some argue that the remote access investigation may be conducted with only a remote access warrant as provided by Article 218 (2) of the Code,<sup>21)</sup> but the legislature did not express its intention to exclude, or there is no provision to ban, other types of remote access investigations.<sup>22)</sup> Therefore, others argue that the remote access investigation may be conducted with a warrant for inspection, particularly describing the storage area to be accessed and inspected,<sup>23)</sup> which can address possible concerns about “searching” relevant files or e-mails as an “inspection.”<sup>24)</sup> This is possible precisely because law enforcement conducts the procedure after search and seizure and identifies where to be accessed.<sup>25)</sup>

As a procedural issue, a warrant for inspection must be shown to the person subject to the investigation, which seems to be important in the remote access investigation to make it known that a storage area of a server will be accessed and some data will be viewed and copied.<sup>26)</sup> Although it is not difficult to show a warrant to the person who has the authority to the storage area as a user,<sup>27)</sup> it could be difficult to iden-

---

21) UTO, *supra* note 3 at 152; and Yoshihiro SAOTOME, *A Study on the Issue of a Remote Access Seizure*, Nihon University Law Review (16) 61, 67 (2019) (in Japanese text). *See also*, Hiroki SASAKURA, *Cyber Kukan no Sousa [Investigations in Cyberspace]*, Hogaku Kyoshitsu (446) 31, 36-37 (2017) (in Japanese text) (suggesting a problem in conducting the remote access investigation as an inspection because a person subject to inspection may not file a request for rescindment or alteration, unlike in the case of seizure, according to Article 430 of the Code).

22) SASAKURA, *supra* note 3 at 183; SHIKATA, *supra* note 3 at 146-147 (expressing a concern about interpreting provisions related to information technology too strictly because this will prevent one from dealing with continual changes, which may differ greatly from the legislative intention); and Toshihiro KAWAIDE, *The Point at Issues on Criminal Procedure Act*, vol.5, Journal of Police Science 71 (9) 157, 171-173 (2018) (in Japanese text).

23) YAMAUCHI, *supra* note 3 at 19-20; SHIKATA, *supra* note 3 at 146-147 (explaining that Article 218 (2) was added because the remote access investigation incident to search and seizure may go too far if it is conducted without judicial review); and Yoshinori NAKANOME, *Investigation of Cybercrime crossing a National Border*, Security Science Review (22) 130, 142-147 (2020) (in Japanese text).

24) *See*, Masahito INOUE, *Computer Network to Hanzai Sousa [Computer Networks and Criminal Investigations]*, vol.1, Hogaku Kyoshitsu (244) 49, 62 (2001) (in Japanese text). *See also*, KAWAIDE, *supra* note 22 at 172 (arguing that inspection can include verifying the state and content of data through a network because it is not its essential element to physically verify the subject).

25) It is required that a remote access warrant contains “the scope to be copied out of the electronic or magnetic records with regard to the recording medium connected via telecommunication lines to the computer which is to be seized,” which is subject to a judicial review. However, this may be abstract to some degree. For example, it is possible to write “a storage area of a mail server that can be accessed by an account that is recorded in a mail soft installed in a personal computer that the defendant uses,” instead of identifying the concrete ID (Kommentar, *supra* note 17 at 856, 872 (Masayuki YOSHIDA)). Moreover, it is not required to specify the location where the server to be remotely accessed exists.

26) KAWAIDE, *supra* note 22 at 172.

27) *Ibid.* But *see*, SASAKURA, *supra* note 21, at 36-37 (suggesting a conflict between the remote access investigation as an inspection and the procedure of showing a warrant).

tify where the server exists or who runs it. As explained above, the rights or interests of those who manage servers do not appear virtually infringed when they lack the authority to generally access personal data. Hence, it can be said that there is no need to treat them as being subject to the remote access investigation in such a situation<sup>28)</sup> and the warrant procedure will be met by showing a warrant to the user.

### (3) Remote Access Investigation Across Borders

It is common in this global information society that servers exist in foreign countries. It may be difficult to locate where these servers are installed or to get answers from companies that manage them. Some, like the 2016 precedent cited above, argue that the remote access investigation, in analogy with the physical investigation, may not be conducted when a server exists in a foreign country because it may violate the sovereignty of the country, preferring to the international assistance in investigation.<sup>29)</sup> However, this view may virtually remove the significance of the new provision for the remote access investigation. Although it is obviously preferable to have international agreements regarding the remote access investigation across borders, others, like the 2018 and 2019 precedents cited above, doubt that there is a violation of the sovereignty of a country where a server exists, or at least take no account of the possible violation for the exclusionary rule applied in a national court.

The first part of this view concerns the sovereignty. It is argued that it is possible to find no violation of the sovereignty, especially when those who manage servers such as ISPs do not have the authority to generally access personal data.<sup>30)</sup> In this situation, law enforcement agencies, without requesting ISPs to take any actions, merely access specific storage areas that are freely accessible by users, whose rights or interests have been judicially reviewed. Therefore, it seems that the rights or interests of those who manage servers will not be virtually infringed. For as long as this is the case, the remote access investigation across borders does not involve the sovereignty of their countries in cyberspace.

As to the latter part, the standard adopted by the Supreme Court to exclude illegally obtained evidence is that its illegality is substantially significant and that it is deemed unreasonable to allow it into evidence in terms of deterrence over illegal investigations in the future.<sup>31)</sup> Therefore, some question the idea of in-

28) KISHI, *supra* note 20 at 20-21 ; and Noriyoshi NAGANUMA, *Network Hanzai eno Tetsuzukihoteki Taio* [Responses of Procedure Law to Network Crimes], Jurist (1148) 212, 216 (1999) (in Japanese text).

29) SUGIYAMA & YOSHIDA, *supra* note 7 at 1095 ; INOUE, *supra* note 19 at 56-57 ; and Kimihiro IKEDA, *Denjiteki Kiroku wo Fukumu Shoko no Shushu/Hozen ni Muketa Tetsuzuki no Seibi* [Improvements of Procedures for Collecting and Preserving Evidence Including Electronic or Magnetic Records], Jurist (1431) 78, 82 (2011) (in Japanese text).

30) YAMAUCHI, *supra* note 3 at 22-25 (questioning what country's sovereignty is involved because it is difficult to endorse the concept of physical locations of servers, or even borders for cloud-stored data) ; SHIKATA, *supra* note 3 at 148-150 (differentiating this from a situation where those who manage servers keep some authority as to the contents or where law enforcement agencies access servers by exploiting the vulnerabilities) ; KAWAIDE, *supra* note 22 at 174 (arguing that there is no difference between the remote access investigation with consent and one conducted upon a remote access warrant, from the viewpoint of another country where a server exists) ; NAKANOME, *supra* note 23 at 134-142, 147-154 (considering the reasonable expectation of privacy in cyberspace) ; and Shuichiro HOSHI, *Memorandum on a Correlation between Criminal Investigations in Cyberspace and Borders*, Journal of Police Science 73 (4) 71, 81-86 (2020) (in Japanese text) (arguing that it may be odd to consider search and seizure of on-line data in analogy with physical search and seizure because there is no border control on the Internet).

31) The Supreme Court, 9/7/1978.

corporating the possible international illegality into the exclusionary rule, which is a domestic remedy for illegal investigations, or the idea of finding such illegality substantially significant enough to meet the standard of the rule.<sup>32)</sup> However, when an investigation across borders is identified and found internationally illegal by the given country, it is also argued that a court will exclude the fruits, finding the investigation significantly illegal<sup>33)</sup> or applying the concept of “procedural justice,”<sup>34)</sup> or as a result of restoration such as data deletion required as an international matter.<sup>35)</sup>

## V Conclusion

This article has discussed the legislation and case law surrounding the remote access investigation and how it can be conducted. It is also inevitable to consider international movements such as the General Data Protection Regulation (GDPR)<sup>36)</sup> of the European Union, and the Clarifying Lawful Overseas Use of Data Act (CLOUD Act)<sup>37)</sup> of the United States, in order to resolve problems related to the remote access investigation across borders. Additionally, the Council of Europe is working on an amendment of Article 32 of the Convention to create an international framework around it,<sup>38)</sup> which deserves continued and careful attention.

---

32) SASAKURA, *supra* note 3 at 183 (arguing that it should be discussed outside of the exclusionary rule how a violation of the sovereignty, which causes the state responsibility towards another country, is reflected in national court proceedings); YAMAUCHI, *supra* note 3 at 21-22 (arguing that a court should not find a violation of the sovereignty unless the given country, which is the only one that can judge whether its sovereignty is violated, identifies the investigation and finds it internationally illegal); FUKANO, *supra* note 11 at 163; SAOTOME, *supra* note 21 at 67-68; and KAWAIDE, *supra* note 22 at 174.

33) Toshihiro KAWAIDE, *Computer Network to Ekkyo Sousa* [*Computer Networks and Investigations Across Borders*], Tadashi SAKAMAKI, et al. (eds), Inoue Masahito Sensei Koki Shukuga Ronbunshu [Festschrift in honor of the Seventieth Birthday of Masahito INOUE], Yuhikaku, Tokyo, Japan (2019) at 414 (in Japanese text).

34) IBUSUKI, *supra* note 11 at 190. *See, e.g.*, the Supreme Court, 6/20/1995 (suggesting a possibility to exclude out-of-court statements that were made by witnesses who were deported before trial and that were supposed to be admissible as hearsay exceptions, from the viewpoint of “procedural justice,” if, for example, the prosecution took advantage of situations that witnesses would be deported and could not make statements at trial in the future).

35) Kuniji SHIBAHARA, et al. (eds), *Keizai Keiho* [Economic Criminal Law], Shojihomu, Tokyo, Japan (2017) at 572 (Hiroki SASAKURA) (in Japanese text).

36) *See, e.g.*, Kaori ISHII, *EU Data Hogoho* [EU Data Protection Law], Keiso Shobo, Tokyo, Japan (2020) (in Japanese text). *See also*, Shuichiro HOSHI, *GDPR to Keijishiho Shirei/PNR Shirei no Sokan* [*A Correlation between the GDPR and Directives 2016/680 and 2016/681*], *Jurist* (1521) 20 (2018); and Makoto IBUSUKI, *Ekkyosuru Data, Ekkyosuru Sosaku* [*Data Crossing Borders, Search Crossing Borders*], *Law & Technology* (82) 45, 51-57 (2019); and Kazuyoshi SUZUKI, *Cybercrime Investigation: Focusing on Transborder Access*, vol.2, *Hogaku Shimpō* 126 (3, 4) 1, 2-9 (2019) (all in Japanese text).

37) *See, e.g.*, IBUSUKI, *supra* note 36 at 49-51; SUZUKI, *supra* note 36 at 2-9; Ko SHIKATA, *Beikoku CLOUD-ho no Igi to Wagakuni no Kadai* [*The Significance of the U.S. CLOUD Act and Challenges in Japan*], *Journal of Police Science* 73 (1) 48 (2020) (in Japanese text); and Ko SHIKATA, *Kokkyo wo Koeru Internet-jo no Sousa ni kakaru Kenpo Mondai* [*Constitutional Issues Related to Online Investigations Crossing Borders*], Go KOYAMA, et al. (eds), *Nichijo no Naka no “Jiyu to Anzen”* [“Freedom and Security” in Daily Lives], Koubundou, Tokyo, Japan (2020) at 250-270 (Ko SHIKATA) (in Japanese text). *See also*, Kazumichi TSUTSUMI, *Beikoku ni okeru Cyber Hanzai Sousa* [*Investigations of Cyber Crimes in the U.S.*], *Criminal Law Journal* (51) 33 (2017) (in Japanese text).

---

38) Cybercrime Convention Committee (T-CY), Criminal justice access to electronic evidence in the cloud : Recommendations for consideration by the T-CY (<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>) (last accessed 2020/8/25). *See also*, IBUSUKI, *supra* note 11 at 189 (suggesting that it is necessary to take the amendment into account when considering the remote access investigation across borders) ; and Makoto IBUSUKI, *Cyberspace ni okeru Shoko Shushu to Digital Shoko no Kakuho* [*Collecting Evidence in Cyberspace and Preserving Digital Evidence*], Horitsu Jiho 83 (7) 84, 88 (2011) (in Japanese text).