Mini Review

BIOMEDICAL Journal of Scientific & Technical Research

ISSN: 2574 -1241

DOI: 10.26717/BJSTR.2024.55.008691

Cloud Storage of Data and the Crime of Storage of "Electromagnetic Records" under Criminal Law in Japan

Kouya Takara*

Institute of Library, Information and Media Science, University of Tsukuba, Japan

***Corresponding author:** Kouya Takara, Institute of Library, Information and Media Science, University of Tsukuba, Japan

ARTICLE INFO

Received: February 20, 2024

Published: March 01, 2024

Citation: Kouya Takara. Cloud Storage of Data and the Crime of Storage of "Electromagnetic Records" under Criminal Law in Japan. Biomed J Sci & Tech Res 55(3)-2024. BJSTR. MS.ID.008691.

ABSTRACT

In recent years, information has been managed in the cloud by companies and medical institutions alike. The legal nature of information in the cloud is not always clear. This paper clarifies the criminal law status of information in the cloud under Japanese law by referring to Japanese precedents and German legal arguments.

Keywords: Cloud Storage; Criminal Law; Penal Code; Japanese Law; Information Law

Introduction

The forms of storing information or data are becoming increasingly diverse, and cloud storage of data is widely practiced even from personal communication terminals. Storage of information in the cloud ranges from businesses to medical institutions. To avoid the risk of viruses and data loss, distributed systems for data storage have also been implemented, making data storage on networks safer and more reliable. In Japan, data has traditionally been combined with tangible objects to become the objective element of a crime under the Penal Code . This is the so-called tangible-object theory. In criminal law, when considering the use of various types of information or data for crime, it is necessary to solve the problem of the objectivity of these. Under the Penal Code and special criminal laws, there are certain types of crimes where the content of information leads to infringement, such as crimes related to sexual information (obscene information, child pornography, etc.) and defamation. While defamation is a type of crime that can be committed orally as well as in writing or by writing on the Internet, with regard to crimes involving sexual information, the problem has been whether or not the information is coupled with tangible objects. Crimes involving sexual information have been discussed in legal academia and practice since the dawn of online crime in the 1990s. This paper aims to provide insights into responses based on reasoning following the Penal Code in light of recent forms of data storage.

I focus my analysis on the offense of storage of illicit information, in which infringement is conditional upon on the offender intentionally storing the information, that is, the information is under the control of the offender.

The Concept of Digital Documents

In Japan, the crimes related to sexual information are those for public indecency under Article 174 of the Penal Code, obscene materials and obscene digital materials under Article 175 of the Penal Code, and child pornography–related offenses set forth by the Act on Regulation and Punishment of Acts Relating to Child Prostitution and Child Pornography, and the Protection of Children (Child Pornography Prevention Act) [1]. First, I will focus on the two crimes set forth in the Penal Code. The crime of public indecency under Article 174 of the Penal Code makes it a crime to perform an indecent act in public, that is, sexual acts under conditions that are exposed to unspecified or multiple persons . Here, the information is not stored on the spot, but only in the memory of the person who witnessed the obscene act. On

the other hand, the crime under Article 175 of the Penal Code involves the storing of obscene information on a medium, and traditionally, the provision (distribution) or display (public display) of the medium on which the information is recorded to unspecified or multiple persons. Article 175 of the Penal Code covers information that is connected to a material medium, that is, a tangible object. The statutory penalty for the crime under Article 175 of the Penal Code is higher than that for the crime under Article 174 of the Penal Code. This is due to the fact that the propagation of obscene information stored on tangible objects has a much wider range of accessibility, being highly disseminative, than performance of an obscene act, which can only be witnessed directly by a smaller number of people.

It can be said that the basis of Article 175 is that information is stored in tangible objects, which can be fixed and spread without alterations to the information . Since the emergence of online pornography, so-called cyber pornography, sexual information can be spread widely without alteration and without the physical medium being transported. It has been debated among criminal law theorists whether, under Article 175 of the Penal Code, the obscene information (the data) or the storage medium (such as a hard disk) is the object of the law, and court cases have also been divided in their rulings [2]. However, the Supreme Court's July 16, 2001, decision resolved the issue in practice in the so-called "Kyoto Alphanet Case," which concerned whether or not the public display of obscene material via the Internet would be a criminal offense. In this case, the Supreme Court held that "The hard disk of the host computer on which the defendant recorded and stored obscene visual information should be interpreted to constitute obscene material as provided under Article 175 of the Criminal Code," so that Article 175 of the Criminal Code did not apply to the data but only to the storage media, as tangible objects. In addition, the Court then ruled that the act of downloading video data online and making it available for viewers to play and view using video playback software was an act of public display of obscene material as defined under Article 175 of the Penal Code [3]. A similar interpretation can be found in Germany, which has been a model for Japanese criminal law.

In Japan, whether it is obscene information or information containing child pornography, a link between the information and the medium is required, and this has been maintained in recent legislation. Prior to the Penal Code, cyber pornography was explicitly regulated in the 2004 amendments to the Child Pornography Prevention Act, which made "electromagnetic records" subject to crimes of provision and public display. To begin with, an electromagnetic record is "any record which is produced by electronic, magnetic or any other means unrecognizable by natural perceptive functions and is used for data-processing by a computer" (Article 7, Paragraph 2, of the Penal Code) [4]. According to the legislator's commentary on the amendment to the Child Pornography Prevention Act of 2004 , this refers to electromagnetic information in the form of data recorded on a storage medium. Even if the content to be transferred itself is "data," the act of transmission is considered to be provision of child pornography because the electromagnetic record that is in the hands of the sender becomes an electromagnetic record in the hands of the recipient as a result of the transmission [5]. This is also true for electromagnetic records under Article 175 of the Penal Code, which prohibits similar acts, and electromagnetic records are data that is supposed to be "recorded" in a tangible storage medium.

At the time of the 1987 amendment to the Penal Code that established the crime of unauthorized production and use of electromagnetic records in Article 163, Paragraph 2, of the Penal Code, it was explained that "it is necessary to have a certain degree of permanence as records," permanence meaning that the information must remain unaltered for a long period. Thus, permanence required that the information must not alter over time [6].

Distributed Data Storage and Information Archiving

Cloud storage services are widely used to store information on cloud servers via the Internet instead of on hard disks. In Japan, as of 2019, 64.7% of companies are using the cloud at least partially , and there are various cloud storage services for general users. Cloud services are defined by the National Institute of Standards and Technology as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." This is a system that allows users to use the storage system online without being conscious of where the server is located, although there is a physical server [7]. The data stored by service users will exist on servers owned by service providers, but the information can be managed in a distributed manner. Article 175, Paragraph 2, of the Penal Code sets forth the crime of storage for the purpose of distribution to sell, which punishes the storage of obscene materials for the purpose of selling or the storage of obscene electromagnetic records. In addition, the Child Pornography Prevention Act provides for the crime of storage and storage for the purpose of provision (Article 7, Paragraphs 3 and 6), as well as the crimes of simple possession and storage, which punishes the possession of child pornography or storage of electromagnetic records containing child pornography for the purpose of satisfying one's sexual curiosity [8].

Storage of electromagnetic records means keeping such electromagnetic records within one's competence and control, which can be done by storing them on a rental server or on a remote storage medium that one can freely download. If you have a hard disk in your possession, it is not storage, but possession. The data in the cloud is an electromagnetic record as defined in Article 175 of the Penal Code or the Child Pornography Prevention Act [9]. In this case, could the

condition in which it is stored be considered storage? Even if the data is stored in a distributed manner on multiple server computers, if the data is stored in a single file format as playable data, this can be considered to be an extension of storage on a rental server [10]. This is because if the storage referred to in the crime of storage is to have the electromagnetic records in question within one's competent control, then even if the user does not own the server in question, there are electromagnetic records that the user can use and dispose of in the storage linked with the server, which is a tangible object, and are subject to the user's control. Here, the debates that took place during the revision of the Child Pornography Prevention Act apply directly [11]. Next, what if the data is dispersed across multiple files, each of which exists on a separate server in a format that is not playable as individual files. The fact that the user has the data in question within his/her competent control remains the same, but while the data stored on each server constitutes an electromagnetic record associated with a tangible object, the individual electromagnetic record must be combined to reproduce the illicit sexual content regulated by Section 175 of the Penal Code or the Child Pornography Prevention Act [12].

In other words, in the entire cloud system, where servers are networked together, illicit sexual information can exist as fixed information, but only through the non-tangible medium of the network. If we assume the application of Peer to Peer, in which data is shared between each node connected by a network, or a wide-area distributed cloud, in which data is stored in multiple network nodes in a widely distributed manner, it is unnatural to consider there to be a single storage medium [13]. On the other hand, users can freely play and view the complete information from a terminal connected to the cloud, and in cases where multiple users share information on the cloud, the data can be received by sharing a URL without the problem of missing attachments or attached data size, in contrast to the dissemination of complete data as an attached file directly by e-mail, etc. As we see in the implementation of 5G, communication traffic has increased, and information can be viewed on mobile devices. Today, data communication has become more stable than in the early days of the Internet, and it is hard to say that the fixity and disseminative nature of data transmission on cloud systems is lower than that of conventional storage media.

Preliminary Discussion on Distributed Storage of Information

I would like to examine two aspects of information distributed across the cloud and which cannot reproduce illicit sexual content by itself. The first is whether the data itself is illicit information and can be regarded as an electromagnetic record associated with a physical storage medium, and the second is whether the entire cloud system can be regarded as a tangible object. The first point is that it is not necessary for the data in question to reproduce illicit content by itself. In this regard, the German view on cache data is instructive. In Germany, in a case where the accused searched for child pornography by browsing the Internet and the child pornography information was stored on his computer as a cache, the German Federal Court ruled that the storage of the cached data constituted storage of child pornography (Article 184, Paragraph b4, of the German Penal Code at the time of the case) due to the fact that the child pornography information could be searched at any time unless the cached data was automatically deleted by the computer system [14] . There is some criticism of this ruling, since cached data is data that is not intentionally saved by the visitor and that is automatically deleted because they have not been deliberately saved . In addition, there are cases of caches not containing video or image data. However, in this case, the illicitness was recognized on the basis of the fact that it was possible to search child pornography sites using the cached data and reproduce child pornography on the basis of this data, so the storage of the data in question was considered to be storage of child pornography.

Currently, the act of searching for child pornography is legally considered a crime (Article 184d of the German Criminal Code). When we think about data in the cloud, the data can be moved or deleted at the user's will and can be stored for a long time. It is stored permanently as long as the server is functioning. In this respect, the data is more permanent than cached data. However, from the perspective of illicitness, although said data is essential information for reproducing illicit sexual information, it is not possible to reproduce illicit information without the other data that was dispersed, and it is not possible to reproduce illicit information through searches and other means based solely on the said data [15]. If this is the case, cloud data cannot be considered in the same way as cached data. As long as the data alone is unable to access the illicit content contained within, the use of said data is limited and it is questionable whether the data can be considered to be within one's competent control. Second, would it be possible to consider the entire networked cloud system as a tangible object, and the associated data that can be combined together as a whole as an electromagnetic record? In this regard, there are still some references in the early legal cases on cyber pornography. In a ruling in the Yokohama District Court, Kawasaki Branch, July 6, 2000 (not listed in the official law reporter), it was held that the defendant's use of an e-mail system to send obscene image data to multiple people constituted a crime of displaying obscene material under Article 175 of the Penal Code [16].

This ruling was reached in a situation in which, at the time of this case, the transmission of obscene electromagnetic records had not been clearly defined in Article 175, nor had such Supreme Court's decision been indicated in practice. Here, the Court held that, "The obscene image data recorded and stored on the defendant's computer is sent in the same format to the receiving mail server of the destination through the Internet e-mail system, and the same image can be reproduced on the display of the computer of the person who has the

receiving mail address [17]. Under the circumstances in which such a system has become widespread in society in general, it can be said that the entire e-mail system functions as an information medium, like a videotape, and has come to have the same degree of fixity and disseminative nature as obscene image data embodied in a tangible object [18]." The fact that said data being present in the e-mail system, that is, the medium, which is indispensable for information transmission, can be equated with storage in tangible objects indicates that the concept of tangible objects is broadly interpreted to include the e-mail system [19]. The Internet is operated on a best-effort basis, and it is not guaranteed that information will always be sent to the other party. In e-mails, attachments and other files may be lost during the transmission process, and the data transmission conditions at that time were more fragile than it is today. Under such circumstances, it is problematic to equate an e-mail system with tangible objects.

There was also criticism of considering the "state" of interconnected computers of the Internet as an "object." It would be unreasonable, both literally and practically, to say that the network itself and the e-mail system, which cannot be said to guarantee the preservation of information, are tangible objects. However, unlike the loss of e-mail attachments, Cloud storage services have been judged that a certain duty of care is imposed on the provider, and some cases of liability for damages have arisen . It can be said that information on cloud storage is legally guaranteed to be stored securely by contract. Unlike the e-mail system, which only connects computers and transmits information, cloud storage is a service that is designed to store information. One of the advantages of information being managed in a distributed manner is the possibility of recovering information from other data in the case of partial loss of data due to server shutdowns, etc. At least in the mindset of the users, the intention is to manage data more securely than by storing data in a storage medium on hand . Even if cloud storage is constructed by multiple storage media and connected via a network, and the system itself cannot be said to be "tangible," it provides a similar fixity to the stored information. The problem that once arose in the decision of the Kawasaki Branch of the Yokohama District Court will not be a serious drawback in the distributed management of information via cloud storage.

If this is the case, it is within the scope of reasonable interpretation to consider data that is linked to the entire cloud system and capable of being reproduced as electromagnetic records. Therefore, even if the data is dispersed across the cloud, if the data can be played back by the user, this is considered to be a case of competent control over data with a fixed nature, which may constitute the crime of storage under Article 175, Paragraph 2, of the Penal Code or the Child Pornography Prevention Act.

Conclusion

In the above, I have examined the recordability of digital data on cloud storage using the crime of storage of illicit information as the case. There are cases in which data on cloud storage is ruled to be electromagnetic records, and other cases where cloud service providers suspend users who upload child pornography data. However, legal issues remain in principle, and there is still no clear discussion on how to deal with cases in which information is managed in a distributed manner. In this regard, if the decentralization of information in cloud computing progresses, it will be linked to other information and communication technologies, such as the blockchain mechanism. Then, the discussion of electromagnetic records in the cloud will not only be a matter of criminal law but also an issue that could spill over to other areas where information is stored, such as protection of data and personal information and management of information assets. In this paper, I have applied traditional criminal law theory to show that information stored as distributed data can be evaluated under criminal law as an object of criminal acts. Although this paper only focuses on Article 175 of the Penal Code and the Child Pornography Prevention Act, I hope that it will contribute to the development of legal discussions in the future.

Acknowledgements

This work was supported by JSPS KAKENHI Grant Number 20K13385. I would like to thank Editage (HYPERLINK "http://www.editage.com"www.editage.com) for English language editing.

References

1. (2024) Ministry of Justice: Japanese Law Translation.
2. (1955) Osaka High Court Ko-keishu 8(5): 649.
3. Hisashi Sonoda, Kansai Daigaku Hogaku Ronshu "On the Electronic Presence of Obscenity: "Cyber Porn" Ni Tsuite No Kei-ho Kaishakuron (Waisetsu No Denshiteki Sonzai Ni Tsuite: Interpretation of Criminal Law on "Cyberporn")" 47(4): 43.
4. Hanreijiho (1997) Okayama District Court. The Law Times Report 1641: 158.
5. (Hanreijiho) Typical court cases are as follows. Osaka District Court, 3 October 1997, The Law Times Report (Hanreijiho), No.980, p.285; Osaka District Court, 19 March 1999, The Law Times Report), No.980: 285.
6. (2001) Supreme Court (Japan), Keishu 55(5): 317.
7. (2001) Federal Supreme Court (Germany), BGHst 47: 55.
8. Mayumi Moriyama, Seiko Noda, (2004) "Understanding the Revised Child Prostitution and Child Pornography Prohibition Law (Yoku Qakaru Kaisei Jido Kaishun / Jido Porn Kinshi Hoh)", Gyosei, pp. 96-97.
9. (1987) Minutes of the House of Representatives Committee on Legal Affairs, 108th Congress, No.4.
10. (2021) See, Ministry of Internal Affairs and Communications, Japan, "WHITE PAPER Information and Communications in Japan 2021 (Joho Tsushin Hakusho 2021)", pp. 313-314.
11. Peter Mell (2011) Timothy Grance. "The NIST Definition of Cloud Computing", p. 2.
12. Takayuki Matsuo (2016) "Cloud Joho Kanri No Horitsu Jtsumu(ver.1)", Kobundo, p. 6.
13. See, Mayumi Moriyama Seiko Noda, p.98-99.

14. (2006) Federal Supreme Court (Germany), 10 October 2006, NStZ 2007, p. 95.
15. See, Tatjana Hörnle (2010) Anmerkung zu OLG Hamburg v. 15. 2. 2010 [betr.: Begriff des Besitzes in § 184b Abs. 4 StGB", NStZ, p. 704.
16. (2000) Yokohama District Law Court, Kawasaki Branch, 6 July 2000, (Not listed in the case law col-lection).
17. See, Hisashi Sonoda, Yokohama indecent image e-mail attachment case (Yokohama Waisetsu Gazo Mail Tenpu Jiken), Bessatsu NBL 79: 75.
18. Hanreijiho (2009) Tokyo District Court, 20 May 2009, The Law Times Report 1308: 286.
19. (2020) Oracle and KPMG, "Oracle and KPMG cloud threat report 2020", p. 8.

ISSN: 2574-1241

DOI: 10.26717/BJSTR.2024.55.008691

Kouya Takara. Biomed J Sci & Tech Res

Submission Link: https://biomedres.us/submit-manuscript.php