SPECIAL ISSUE

PARADIGMS OF INTERNET REGULATION IN THE EUROPEAN UNION AND CHINA

BOUNDARY OF CRIMINAL RESPONSIBILITY OF INTERNET SERVICE PROVIDERS — A LESSON FROM THE QVOD CASE

CHEN Xuan∗

Abstract The Qvod case in 2016, in which the Chinese video-sharing site Qvod was convicted of the crime of disseminating pornographic materials for profits, provoked heated debates regarding the criminal responsibility of internet service providers (ISPs) in China. Using the Qvod case as an example, this paper first discusses the definition and the legal obligations of ISPs, and argues that we should decide the criminal responsibility of ISPs according to their functions and the content of their services. This paper further analyzes four major issues associated with the criminal responsibility of ISPs, including accomplice responsibility, accessory with neutral conduct, perpetrator by action or omission and ideal concurrence (Idealkonkurrenz).

Keywords the Qvod case, internet service provider, neutral assisting conduct, criminal responsibility

INTRODUCTION

In the internet age, cybercrime has become a serious societal problem. This issue has particularly been at the top of the political and legal agenda in China because of a fast-growing internet industry on the one hand, and an underdeveloped internet regulatory...
regime on the other. Against this backdrop, criminal law plays an important part in internet regulation in China. While in the field of criminal law, a large part of the discussion regarding cybercrimes and internet regulation has been focusing on the criminal responsibility of the internet service providers (ISPs). This is logical because most cybercrimes can only be carried out with the network platform and the technical support from the ISPs. In other words, the assisting behavior of the ISPs becomes the critical point in most cybercrimes.

However, it seems inadequate to apply the traditional criminal law theory in its current form to these cybercrime cases, as these cases pose fundamental challenges to the traditional theory. Criminal lawyers in China have been debating whether the traditional doctrines of imputation, accomplice and omission are still applicable in cybercrime cases. There is a growing opinion, in academia as well as among legislators, that the traditional principles of criminal imputations should be changed in order to adapt to the special situation in the cyberspace. The Qvod case in 2016 marked the culmination of such a debate in China, and this paper will therefore use it as an example to reflect on the discourses regarding the criminal responsibility of ISPs.

I. THE QVOD CASE

Qvod Technology Co., Ltd. was a Chinese video-sharing site. Established in 2007, Qvod provided users with internet video service by offering free Qvod Server Install and Qvod Player. Anyone can use Qvod to upload his/her own videos. By using the resource server program to generate the hash value and then the link of the video uploaded, it was also possible for the uploader to share videos with other Qvod users. In this way, Qvod’s central scheduling server has actually established a platform for sharing videos between the webmasters and users, and amongst the users themselves. In order to boost the download speed, Qvod also set up a platform with the core part of a cache tracker server. Through its own cache server and another operators’ cache server, Qvod then set up in total more than 1,000 cache servers. For videos, whose view numbers have reached certain level, the cache tracker server would send out an order so that the cache servers would grasp or save those videos. Thus, when they were downloaded again, the cache servers would provide users with the best path.

In this process, the cache server automatically saved a large number of pornographic videos due to the high frequency with which they were viewed and downloaded. As shown later during the investigation, in four seized Qvod servers, Beijing police extracted 29,841 videos and among them 21,251 were pornographic ones. To some extent, the

---

1 The case information is summarized from the decisions of the court of first instance and the appellate court. See (2015) 海刑初字第 512 号刑事判决书 (No. 512 First Trial Criminal Judgment of Haidian District People’s Court), Sep. 13, 2016; (2016) 京 01 刑终 592 号刑事裁定书 (No. 592 Final Criminal Judgment of Beijing 1st Intermediate People’s Court), Dec. 15, 2016.
cache server facilitated and accelerated the download and spread of the pornographic videos, which, according to Article 363 Section 1 of the Chinese Criminal Law, constituted the crime of dissemination of pornographic materials for profit. The four directly responsible managers of Qvod were aware of the existence of pornographic videos in their servers, but had not taken actions to fulfill their supervisory obligations.

The CEO of Qvod pled not guilty. He argued during trial that Qvod was neither the provider of pornographic videos nor a pornographic video sharing website; rather, their product was simply a player with P2P functions, and video cache was also common practice in the industry. He therefore believed that the principle of technological neutrality and the principle of safe harbor should be applied in this case and Qvod should not be held criminally responsible, even when pornographic videos were indeed distributed through their product.

In 2016, after two years’ investigation and trial, Qvod and its managers were convicted of the crime. The company was fined RMB¥10 million, while the four managers were sentenced to imprisonment for between three and three and a half years, with personal fines of between RMB¥200 thousands and RMB¥1 million.

The Qvod case drew great public attention. The trial was broadcasted online and over one million people watched it. Even after the case was closed, the debates provoked by it from the general issue of the relation between technological development and internet regulation, to the specific criminal law issue of neutral assisting behavior still continue. New provisions were added in the Criminal Law for these kinds of cases in the future (Article 286a). Despite these advances, there are still many controversial issues regarding the criminal responsibility of ISPs.

This paper aims to contribute to the ongoing discussion on this topic. It will first discuss the definition and the legal obligations of ISPs and come up with a proper method to determine their criminal responsibility. Then, it will further analyze four major issues associated with the criminal responsibility of ISPs, namely accomplice responsibility, accessory with neutral conduct, perpetrator by action or omission and ideal concurrence (Idealkonkurrenz).

II. THE DEFINITION OF AN ISP AND ITS LEGAL OBLIGATIONS

Generally speaking, any company that provides internet connections and services can be called an ISP. However, this definition is apparently too vague to provide judicial guidance. In fact, as is known to all, the smooth operation of the internet relies on each individual component. No conduct of one ISP can run without the help and support from other ISPs’ on technique or device. If we simply establish the objective causation between ISPs and the harmful results, perhaps every ISP can be held responsible.

Hence, if we agree the criminal responsibility of ISPs should be limited to certain extent, then the core questions that need to be addressed will be: How should we
distinguish between different ISPs in terms of legal obligations and elements of crime when we judge their criminal responsibilities? One possible distinction can be made according to the different functions of ISPs. In a report of the U.S. Department of Commerce, the functions of ISPs are divided into four categories: transitory communications (serving as an information carrier), system caching, storage of information on systems or networks at direction of users (hosting), and information location tools (searching). Based on their respective functions and services, different ISPs will certainly vary in their status, their control of information and their capacity to prevent crimes. Consequently, their legal obligations and criminal liability, especially the elements for omission crimes for them, should also be different.

However, the Chinese legislature did not tend to make any differentiation between different ISPs with regard to the extent and conditions of their criminal liability. Enacted in August 2015, the 9th Amendment to the Chinese Criminal Law has, for the first time, stipulates omission criminal liability for the ISPs. The newly-added Article 286a reads in its Section 1: “Any network service provider that fails to perform the information network security management obligation as prescribed in any law or administrative regulation and refuses to make corrections after being ordered by the regulatory authority shall be sentenced to imprisonment of not more than three years, criminal detention or surveillance in addition to a fine or be sentenced to a fine only under any of the following circumstances: (1) causing the spread of a large amount of illegal information; (2) causing the leakage of users’ information, with serious consequences; (3) causing the loss of criminal case evidence, with serious circumstances; and (4) any other serious circumstance.”

Although not written explicitly in the text, we can nevertheless find that the three circumstances listed in this article actually refer to different kinds of legal obligations and therefore different kinds of ISPs. The first one, “causing the spread of a large amount of illegal information,” normally refers to situations where ISPs do not actively perform their duties of content monitoring. Therefore, this should not apply to ISPs that provide internet hardware, access service or information storage service. The second circumstance, “causing the leakage of users’ information, with serious consequences,” generally applies to those ISPs providing information and data storage service. The third one, “causing the loss of criminal case evidence, with serious circumstances” only targets at ISPs who not only provide information and data storage service, but also are legally obliged to keep evidence.

Following this analysis, criminal lawyers in China are, despite the vague legislation, trying to establish a reasonable standard to determine the criminal responsibility of ISPs. The starting point for this standard should be the functions and the content of services

---

ISPs provide. A classification in this regard will be helpful to decide what kind of role each ISP plays in internet crimes and their obligations and capacity to prevent the crimes. These should be the basis and prerequisite for us to decide the criminal responsibility of ISPs.³

III. FOUR ISSUES ON THE CRIMINAL RESPONSIBILITY OF ISPS

The Qvod case raised four important issues concerning the criminal responsibility of ISPs. These are not only theoretical questions in criminal law, but also the problems we might face in practice. This part will analyze these four issues in detail.

A. Accomplice Responsibility

The first theoretical question that the Qvod case involves is accomplice. Just like in many cybercrimes cases, Qvod’s assisting behavior constituted complicity. However, the tricky part in internet accomplice cases is that there is very often no intention liaison. This is problematic because, according to traditional theory, the existence of intention liaison is necessary for accomplice criminal liability. Facing this conundrum, in order to combat the ever-increasing cybercrimes, the Supreme People’s Court of China had to loosen the traditional standard and, albeit with restrictions, accept the theory of unilateral complicity.

In its interpretation in February 2010 (hereinafter referred to as “the 2010 Interpretation”), the Supreme People’s Court made clear that, in cases of disseminating pornographic materials, bilateral mental contact would no longer be a necessary element in determining assisting behavior and accomplice. Article 7 of the 2010 Interpretation provides, “as long as they are aware of the pornographic nature of the website, anyone who, for the purpose of making profit, supplies funds to pornographic websites, either directly or indirectly, by running advertisements on it or through other means, or provides financial settlement service for it,” shall be punished as accomplice of the crime of Article 363 Section 1 (dissemination of pornographic materials for profit).⁴ This means that now a knowingly one-sided assisting behavior would be enough to constitute complicity with the perpetrator. This judicial interpretation marks a break from the long tradition of Chinese criminal law theory, which denied one-sided accomplice. Then, in two later interpretations, the Supreme People’s Court extended this new theory to internet


⁴ 最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释 (Interpretation (II) of the Supreme People’s Court and the Supreme People’s Procuratorate of Several Issues on the Specific Application of Law in the Handling of Criminal Cases about Producing, Reproducing, Publishing, Selling and Distributing Pornographic Electronic Information via the Internet, Mobile Communication Terminals and Sound Message Stations), issued on Feb. 2, 2010.
gambling and internet hacking cases. In these two kinds of cases, one-sided assisting behavior will also be regarded and punished as complicity.

However, it is noteworthy that although the above judicial interpretations accepted one-sided accomplice, they did so in a limited way, imposing further conditions on its application. According to the traditional theory of accomplice, intention liaison is necessary, while the role of assisting in the commission of crime has no impact on whether that contribution is to be regarded as joint crime or not; this only plays a role in sentencing. The judicial interpretations, on the contrary, admit one-sided accomplice, while at the same time require that the circumstances in these cases must be more serious than common accomplice cases. To sum up, the judicial interpretations have adopted the following pattern when deciding one-sided accomplice in cybercrimes: “knowing that someone is going to commit a certain crime + providing special internet technical assistance + fulfilling special serious circumstances = constituting joint crime.”

The remaining problem is that the above three judicial interpretations only apply to the six specific crimes prescribed in them, whereas nowadays assisting behavior seems to be omnipresent in all kinds of cybercrimes. Therefore, the judicial interpretations cannot solve all the difficulties regarding accomplice criminal responsibility in cases where the internet has been used to provide assistance. The Supreme People’s Court should perhaps issue a general interpretation on joint crimes and accept one-sided accomplice in all crimes with internet assistance.

B. Accessory with Neutral Conduct

Another issue being discussed in the Qvod case is the so-called “accessory with neutral conduct.” Though lacking clear definition, accessory with neutral conduct, or neutral assisting conduct, generally refers to daily or business behaviors, which do not have any illegal purpose in themselves, nonetheless objectively facilitate the commission of crime of others (perpetrator). In the context of cybercrimes, internet neutral assisting

---

5 Art. 2, 最高人民法院、最高人民检察院、公安部关于办理网络赌博犯罪案件适用法律若干问题的意见 (Interpretation of the Supreme People’s Court, the Supreme People’s Procuratorate and the Ministry of Public Security on Several Issues concerning the Application of Law in the Handling of Criminal Cases of Internet Gambling), issued on Aug. 31, 2010.

6 Art. 9, 最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释 (Interpretation of the Supreme People’s Court and the Supreme People’s Procuratorate of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems), issued on Aug. 1, 2011.

7 YU Zhigang, 网络空间中犯罪帮助行为的制裁体系与完善思路 (The Criminal Sanctions against Crime Assisting Behavior in Cyberspace and Its Improvement), 2 中国法学 (China Legal Science), 9–10 (2016).

8 Id. at 16–17.

9 Id. at 23.

10 ZHANG Mingkai, 论帮助信息网络犯罪活动罪 (Study on The Crime of Assisting Information and Network Criminal Activities), 2 政治与法律 (Political Science and Law), 11 (2016).
conduct has become the main pattern of conduct. The peculiarity of internet neutral assisting conduct is, in contrast to traditional neutral conducts, it could exist in cases where there is no perpetrator.\textsuperscript{11} This raises many questions. For instance, should internet access provider, who knows that the third person will put illegal information on the website but does not prevent it in advance, or who knows that the third person has put illegal information on the website but continually provides further access service, resulting in the spread of illegal information, be criminally responsible as perpetrator or accomplice by acting or omission?\textsuperscript{12}

As some scholars point out, in China, there are currently three methods to criminalize internet neutral assisting conduct: (1) When there is a perpetrator and he/she could be arrested, then the internet neutral assisting conduct will be treated as accomplice to perpetrator; (2) when there is a perpetrator, however, it is impossible to prosecute the actual offender, or when there is no perpetrator at all, the internet neutral assisting conduct will incur criminal liability on the accomplice for further crimes, probably through expansive interpretation of these crimes; and (3) when there is a perpetrator, however, it is impossible to prosecute the actual offender, or when there is no perpetrator at all, but the internet neutral assisting conduct cannot be attributed to any existing crimes, then amendment must be made to the Criminal Law to criminalize the behavior in future cases.\textsuperscript{13}

These three methods have revealed the gradual development in China with regard to the accessory criminal liability in neutral conduct cases. The criminal policy behind this is clear: The Chinese legislature has adopted an active attitude of expanding the space of criminalization.\textsuperscript{14} This is not only antithetical to the German and Japanese theory and practice which expands the space of non-criminalization, but also too wide in the Chinese context. Hence, many Chinese scholars argue that when determining criminal responsibility in internet neutral conduct cases, it is more reasonable to implement a comprehensive method. In other words, we should analyze whether the ISPs have obviously and substantially raised the risk of commission of certain crimes. Only when the following two conditions are fulfilled, can the neutral conduct lead to criminal

---

\textsuperscript{11} LIU Yanhong, 网络中立帮助行为可罚性的流变及批判——以德日的理论和实务为比较基准 (The Development and Criticism of the Punishability of Internet Neutral Assisting Behavior — Based on the Relevant German and Japanese Theories), 5 法学评论 (Law Review), 41 (2016).

\textsuperscript{12} CHEN Hongbing, 网络中立行为的可罚性探究— —以 P2P 服务提供商的行为评价为中心 (Study on The Punishability of Internet Neutral Assisting Behavior — On the Judgement for the Behavior of P2P Provider), 11(3) 东北大学学报(社会科学版) (Journal of Northeastern University (Social Science)), 258 (2009).

\textsuperscript{13} See LIU, fn. 11 at 43.

\textsuperscript{14} The 9th Amendment in 2015 also added Art. 287b to the Chinese Criminal Law, which reads: “Whoever, while being obviously aware that any other person is committing a crime by using an information network, provides internet access, server custody, network storage, communication transmission or any other technical support, or provides advertising, payment settlement or any other assistance for the crime, shall, if the circumstances are serious, be sentenced to imprisonment of no more than three years or criminal detention in addition to a fine or be sentenced to a fine only.”
liability: (1) The assistance provider must be aware that his/her assistance will be used to commit crimes and these certain crimes must have been committed; and (2) according to the nature of the assisting behavior, it is highly possible that the third party who receives such assistance would commit such a crime.\textsuperscript{15}

\textbf{C. Perpetrator by Action or Omission}

In its judgment, the court finally convicted both the Qvod company and its responsible managers of the crime of disseminating pornographic materials for profit (Article 363 Section 1). The case’s outcome, the conviction of this crime, is generally accepted. Despite this, there have been different views about the nature and scope of the prescribed sentence in this case: Is it an active crime or a passive crime, or even both?

In general, “disseminate” means to spread or bring into circulation, through broadcasting, lending, renting, transporting and many other ways. Therefore, normally, the act of dissemination of pornographic materials implies active behavior. When disseminating such materials through internet, the typical cases are establishing pornographic websites or displaying pornographic materials online. However, it is undeniable that this can also be done passively, namely by omission. This can, for example, occur, when ISPs refuse to fulfill their monitoring obligation over pornographic and other harmful materials.

Article 4 of the above mentioned 2010 Interpretation deals with the case of disseminating pornographic materials by omission. According to this interpretation, if “the founder or directly responsible managers of a website” are aware that other persons are disseminating pornographic materials on their website, but they, for profit, allow or connive at such behavior, then as long as the amount of the files or the profit reaches a certain level, the founder or directly responsible managers of the website will be convicted of the crime of disseminating pornographic materials for profits in accordance with Article 363 Section 1 of the Criminal Law.

Going back to the Qvod case, it is the opinion of the court that Qvod has committed the crime in both active and passive ways. On the active part, the court pointed out: Although Qvod built up their platform on the basis of P2P technique, they still have full control over key issues of how to use this technique and how to set the rules of their service. However, Qvod decided not to make any user or content restrictions on video upload until they were punished by the regulatory authority. Furthermore, when they set up the cache server and design its cache conditions for storing videos, the only standard they chose was the click-through rate, which led to the results that a large number of pornographic videos were stored in their server and hence were spread more quickly. Based on this, the court decided that Qvod was also actively involved in the process of disseminating pornographic materials. On the passive part, the court reminded of the

\textsuperscript{15} See LIU, fn. 11 at 48.
intrinsic risk of P2P technique of being used to transmit and spread pornographic videos or pirated copies. Therefore, Qvod has the legal obligation of internet security management. It should further actively bear, to a higher degree, the duty of care to prevent this risk. The evidence in this case has, however, shown that Qvod was resistant or lax in performing its obligation, even after being penalized by the regulatory authority. By not fulfilling its duties, Qvod caused the harmful result of the wide and speedy dissemination of pornographic videos online.16

This paper disagrees with the above court opinion and argues that the pattern of Qvod’s conduct in this case only involves omission. Unlike directly providing pornographic videos or creating a pornographic videos sharing platform, the conducts of grabbing and storing videos are the normal functions of the server and the player. Therefore, grabbing and storing pornographic videos, or even the result of the wide and speedy spread of pornographic videos per se, cannot be the reason why the conduct of Qvod should bear criminal responsibility. Rather, it is mainly because Qvod did not fulfill the legal duty of ISPs to monitor and delete pornographic videos, and this omission objectively facilitated and accelerated the spread of pornographic videos.

If there is omission in this case, is it typical omission or non-typical omission (echte oder unechte Unterlassung)? By convicting Qvod of the crime of disseminating pornographic materials for profit, the court has evidently treated it as a non-typical omission. For a non-typical omission, the key issue would be the source of the obligation for Qvod as an ISP. Traditionally, the theory of “formal obligation” was applied in non-typical omission, which argues any written obligations issued beyond the criminal law can be the source of omission. According to this theory, when an ISP violates administrative law and promotes the realization of a crime (such as the crime of distributing pornographic materials), it should be punished as omission. The formal obligation theory has, albeit, been criticized because it ignores the target of criminal law.

Recently, more and more scholars advocate the theory of “substantial obligation” which argues that only guarantors have the duty of action. The source of the obligation can largely be divided into two groups: (a) obligation of protecting specific legal interests and (b) obligation of monitoring specific sources of danger. Criminal liability related to ISPs is mainly the second group. In these cases, we should first make clear whether the concrete ISP can be seen as the guarantor, and the criterion to use here is what the law requires them to do on the one hand, and whether it can really control the risk factually and technically on the other hand. Both the legal obligation of security management and the technical ability to control can vary among different types of ISPs. In the Qvod case, Qvod was technically and fully able to monitor videos uploaded to their platform. When they found pornographic materials, they were also fully able to delete them immediately. Therefore, Qvod not only had the security management obligation, but also possessed

16 See the appellate court decision on Qvod case, fn. 1.
actual control over pornographic videos on their platform.

\[ \text{D. Ideal Concurrence (Idealkonkurrenz)} \]

As was mentioned earlier, as a reaction to the Qvod case, the legislator added Article 286a in the Criminal Law to punish ISPs if they refuse to perform their legal obligations of internet security management. We have already discussed this amendment from the perspectives of accomplice liability. It is worth noting that this marks a departure from the traditional accomplice liability theory.\(^{17}\)

However, this new provision will raise another issue for future cases, namely the issue of ideal concurrence (Idealkonkurrenz). If a similar case occurs again, then the actors will commit two crimes at the same time: Like Qvod, they will be convicted of the crime of disseminating pornographic materials for profit (Article 363 Section 1); according to the new law, they will also be convicted of the crime of refusing to perform network security management obligations (Article 286a Section 1).

Article 286a deals with this issue in its Section 3, which provides: Whoever commits any other crime while committing the crime of Article 286a Sections 1 and 2, shall be convicted and punished according to the crime with the higher penalty. In the case described above, since the penalty in Article 363 is higher, the perpetrator will be identified as disseminating pornographic materials for profit.\(^{18}\)

\[ \text{CONCLUSION} \]

The Qvod case was a textbook example for the relation between internet and legal regulation, or even more generally, between technology and law. On the one hand, law should not hinder the development of internet technology; on the other hand, internet technology should not be allowed to become the shield for crime. The most important lesson from the Qvod case is that ISPs should never willfully turn a blind eye to the pornographic and other harmful contents in their websites or servers, otherwise they will be held criminally responsible. However, as lawyers, we should always bear in mind when deciding legal liability, criminal law should always be the last resort and the prevention framework should always be given priority over the system of penalization.

\(^{17}\) TU Longke, 網絡服務提供者的刑事責任模式及其關係辨析 (Patterns of ISP Criminal Responsibility and Their Relationships), 4 政治與法律 (Political Science and Law), 109 (2016).

\(^{18}\) CHEN Xingliang, 快播案一审判决的刑法教义学评判 (Criminal Doctrinal Comment on the First Instance Judgment of the Qvod Case), 29(1) 中外法学 (Peking University Law Journal), 26 (2017).