

The Evaluation of the Prevention of Internet Access and the Provisions of the Law 5651

Contributed by Dr. Murat Volkan Dülger

Introduction

One of the most important technological developments of 1990ies is the internet. Internet, due to the rich resources that it has been providing to its users, has enormously expanded its area of use and today “No Life with No Internet” would not be any exaggeration. With no doubt, the resources provided by internet, beside for the legitimate purposes, have also been used by the ones who are in breach of the laws. Indeed, in some cases, these services of the internet facilitate such illegal actions¹.

During the last twenty years, internet increasingly entered into the daily life of the modern society and just as in the other technological inventions, the expansion of internet led to its misuse². Then the new crime types named as “information technologies crimes” were determined. Also, the classical crime types such as terrorist activities, defamation or fraudulent acts have been started to be committed via internet³.

In this article, the measures to be adopted in case of a breach or suspicion of a breach of criminal law provisions with the use of internet, more specifically the measure of the prevention of internet access shall be treated. Additionally, we shall examine “the law numbered 5651 regarding the regulation of publications made on internet and the fighting against the crimes committed via these publications” in respect of the regulation and prevention of internet communication.

I. The Provisions of the Law Numbered 5651

1. In General

The aim and the scope of the law numbered 5651 is determined under article 1 as “the determination of the undertakings and responsibilities of content providers, host providers, access providers and multiple user providers and the determination of principles and procedures for fighting against the crimes determined in the law committed on internet over content, host and access providers”.

The law provides the relevant regulations regarding the administration of content, host and multiple user providers and by doing so it creates a legal base for the regulation of internet in Turkey. However, the regulation of procedures for fighting against crimes on internet over content, host and access providers is not adequate with the aim of the law. Because fighting against crime cannot be done over these internet personalities. Fighting against crime can only be done via education, with well-established laws and the entire judicial mechanism.

2. The Obligation of Disclosure

The article 3 of the law numbered 5651 provides that content, host and access providers should disclose the relevant information determined per law on their own internet sites enabling the users to have relevant and up-to-date information about them. This provision is appropriate as it facilitates the determination of the perpetrator of a crime committed via such

¹ Murat Volkan Dülger, “Mass Media Means and Terrorism”, http://www.hukukcu.com/bilimsel/kitaplar/kitleiletisim_teror.htm, 02.04.2007.

² Murat Volkan Dülger, Computer Crimes, Seckin Publications, Ankara, 2004. p.9.

³ Murat Volkan Dülger, “The Effects of the Developments in Technology and Mass Circulation Media on International Terrorism”, Law and Justice Journal, İstanbul, Y.4, V.10, 2007, p.60-64.

internet site. However, the term of content provider has a rather large scope including the internet users who, for instance, attend to a forum on internet and share its ideas. Thus it would be more appropriate to use the term website owner or operator instead of content provider.

3. The Liabilities of Internet Personalities

a. Content Providers

The article 4 of the law numbered 5651 provides that the content providers shall be liable from any content that they present but shall not be liable from any content belonging to any third party. For instance the content provider shall not be liable from the content of a website to which it only provides a link.

b. Host Providers

As per the article 5 of the law numbered 5651, the host providers are not liable for controlling the content to which they host as to whether the content is illegal or not. This provision is appropriate as it is technically impossible for any host provider to control millions of data that they provide service.

On the other hand, the host providers are responsible to remove any content which are illegal provided that the removal demand is made per the articles 8 and 9 of the law and such removal is technically possible.

c. Access Providers

The article 6 of the law numbered 5651 provides the liability of access providers namely internet service providers. Accordingly once the access provider is informed that any of its users publishing any illegal content, it must remove such illegal content after receiving a removal demand pursuant to the provisions of the law and if such removal is technically possible. This is an appropriate regulation as the access providers, as a rule, are not liable from the illegal content but responsible to remove such content once it has been duly informed of the existence of the illegality and if such removal is technically possible.

The article 6 also provides that the access providers shall preserve the traffic information which is recited by the relevant regulation for a period of minimum six months and maximum two years and shall provide the accuracy, integrity and secrecy of such traffic information. This provision is appropriate. Because despite it would create additional investment costs for the access providers in order to preserve such traffic information as determined by the regulation, preserving the traffic information would be very helpful in fighting against the crimes committed on internet and in finding the perpetrator of a crime.

d. Multiple User Providers

The article 7 of the law regulates the responsibilities of multiple user providers which are in fact providing access to public either for commercial or non-commercial purposes. The multiple user providers are responsible to take necessary precautions to prevent access to illegal content. However the law does not provide any sanction in case such responsibility is breached. In fact this type of responsibility has not been determined for access and host providers and there should not be such a responsibility for multiple user providers either. So it may be possible to say that article 7 of the law does not serve any purpose.

II. Prevention of Access under the Law numbered 5651

The law numbered 5651, beside the responsibilities of the internet personalities, regulates the legal conditions of the prevention of access.

1. The Crime Types Subject to the Prevention of Access

The article 8/1 of the law provides that it is possible to prevent the access to the publications on internet which create sufficient suspicion that these publications may be considered as provocation for suicide as per the article 84 of Turkish Criminal Code (TCC), sexual abuse of the children as per the article 130/1 of TCC, facilitation of the use of narcotics as per the article 190 of TCC, provision of substances harmful to the health as per the article 194 of TCC, obscenity as per the article 226 of TCC, prostitution as per the article 227 of TCC, facilitation of gambling as per the article 228 of TCC and the crimes against Atatürk per the law numbered 5816.

As per the wording of the article 8, it may be understood that the prevention of access may only be ordered in the condition of the existence of the above stated crimes without leaving any space for the discretion of the judge or the public prosecutor. Such strict wording of the law may be considered as appropriate at first glance, especially considering that the prevention of access is a serious intervention to the freedom of communication. However, this wording of the article prevents the application of this measure to the other crimes committed on internet but not recited in law which leads to the insufficient application of the prevention of access measure. Thus in order to pass beyond the limited application of the law, leaving necessary space to the discretion of the judge for the not-recited crime types would be beneficial.

Additionally, there are some other reservations in relation the crime types which may be subject to the prevention of access. Indeed, it should be questioned as to whether obscenity should be one of the crimes which may be subject to the prevention of access. Because the definition of obscenity differs from country to country and from time to time. Also some artistic, medical or scientific materials are not considered as obscenity⁴. Considering that the concept of obscenity does not have any clear definition, ordering the prevention of access by relying on such a vague term may lead to the misuse of this measure. Thus in addition to the article 226 of TCC, the law numbered 5651 should refer to pornography but not to obscenity⁵. Indeed in European Cyber Crime Agreement, instead of the term obscenity, the term pornography is used and the actions which shall be named as pornography are clearly defined.

Another important issue to consider is whether the pornographic materials in which the adults take place should be considered as a crime. In some countries where the freedom of speech is a well established and internalized concept, there exists an understanding as per which the adult pornography is not considered as a crime. Indeed, adult pornography may be criticized morally but should not be subject to the authority of state thus should not be considered as a crime. Of course, these thoughts are not applicable to child pornography for which the state should take every possible precaution to prevent.

Similar reservations are also valid for gambling. Gambling should be considered as a personal choice and should not be subject to the state authority. In fact, despite in Turkey gambling is considered as a crime, this does not really prevent gambling. Beside the illegal gambling activities within Turkey, the ones who are willing to gamble go to the neighbor countries where gambling is legal and leave an important economical input there. Thus, it should be considered to allow gambling activities but to regulate it regarding the age and income of the players.

⁴ **Dülger**, Regulations Against the Distribution of Child Pornography via Internet, Istanbul Bar Association Journal, V. 2004/4, p.1490.

⁵ **Dülger**, Computer Crimes, p.292.

It seems that rather than the general interest of the society and individuals, the legislators while enacting the law numbered 5651, emphasized the moral concerns which lead to the above stated strangenesses.

2. The Prevention of Access as a Protective Measure

Under Turkish Criminal Procedural Law, the protective measure is defined as a provisional measure taken by the judicial authorities who are competent to establish a decision in relation to the matter in urgent cases where any delay may cause unrecoverable damages and for providing the enforcement of the decision at the end of the trial. The protective measures may stay in force until reaching to a judgment. The prevention of access is regulated as a protective measure under the law numbered 5651.

The prevention of access decision, during the period of investigation, can only be given by a judge and during the period of trial, can only be given by a court. However, in urgent matters, during the period of investigation, the public prosecutors can also decide for the prevention of access. However, in such a case, the prevention of access decision of the public prosecutor must be approved by the competent judge within 24 hours. If the judge does not give its approval within the given period, the prevention of access decision of the public prosecutor shall be deemed cancelled. Also, it is possible to oppose to the prevention of access decision before the upper court by the interested parties.

Previously, the prevention of access was given by the judges under their capacity of creating law. With the enactment of the law numbered 5651, the measure of prevention of access gained a legal base. On the other hand, under the law, despite it is stated that in urgent matters the public prosecutors can also decide for this protective measure, considering that the crimes such as terror or organized crimes are not recited under law, the situations under which the public prosecutor can take this measure is questionable. In any event the approval of the judge of the possible decisions of the public prosecutors provides the necessary control mechanism.

The enforcement of the prevention of access decision shall be fulfilled by the Telecommunications Authority. The Authority after receiving the decision from the judge, court or public prosecutor shall dully send it to the relevant access provider. The access provider shall remove the access within 24 hours after the receipt of the demand from the Authority.

In circumstances where the public prosecutor abandons the prosecution, the prevention of access decision automatically becomes invalid. In such a situation, the public prosecutor shall request the cease of the prevention of access from the Telecommunications Authority which then shall inform the access provider for the ceasure of the prevention. On the other hand, after the abandonment of the prosecution by the public prosecutor, if such decision of the prosecutor is cancelled by the relevant criminal court, this does not affect to the cancellation of the prevention of access decision and if needed a second prevention decision should be given.

The acquittal decision shall create the same result with the abandonment of the prosecution and the prevention of access shall be cancelled by the access provider upon the request of the Telecommunications Authority.

On the other hand, if the accused is convicted, the continuance of the prevention of access poses a legal problem. As mentioned above, under the law numbered 5651 the prevention of access is determined as a protective measure which may stay in force until reaching to a judgment. In circumstances after the conviction of the accused if the access is still needed to be prevented, then the court should make a decision for the prevention of access which shall be then considered as a security measure. However, the prevention of access is not determined

as a security measure under TCC. Under these circumstances, without such a determination, pursuant to the principle of legality in crime and punishment, it should not be possible to order for the prevention of access. Thus the lacuna in this respect should immediately be filled by the legislators.

The executives of host and access providers who do not fulfill the prevention of access decision given as a protective measure within 24 hours shall be punished with imprisonment of 6 months to two years.

3. The Prevention of Access as an Administrative Measure

The law numbered 5651 beside the judicial measures, as mentioned above; under article 8/4 provides the prevention of access as an administrative measure. Accordingly, in circumstances where the publications made on internet of which content or host providers are in abroad may be considered as constituting the crimes mentioned under article 8/1 may be prevented ex officio by the Telecommunications Authority Communications Administration. The Administration may also ex officio use its competence against the content or host providers in Turkey provided that the publications on internet may be considered as constituting the crimes of sexual abuse of the children and obscenity. This decision of the Administration shall be executed by the relevant access provider within 24 hours upon duly receiving the decision of the Administration.

The prevention of access decisions of the Telecommunications Authority is an administrative decision which may be opposed before the administrative courts. However, this competence of the Authority is against the general principles of Turkish law. Under Turkish law, where necessary, it is possible for the administration to apply administrative measures. However, the administrative measures, just as in protective measures, should be provisional and should be applied to reach to another purpose. For instance, the prevention of access, determined as a protective measure, is provided in relation to the investigation and trial activities of the public prosecutor and the court and the conditions under which such measure shall be ceased are clearly determined by the law. But the regulation of prevention of access determined as an administrative measure under the law does not have any provisional characteristic and does not lead to any purpose as it does not provide the conditions under which this administrative measure shall be ceased.

Additionally, per the wording of the law it is understood that the competence of the Authority to order for the prevention of access as an administrative measure is provided to assist the judicial authorities. However, the law provides the same competence to the public prosecutors as well. Thus there is no need to give such a competence also to the administration which is in fact an anti-democratic provision.

Another point to criticize for this regulation is the procedural differences between the administrative measure and protective measure regarding prevention of access. Indeed, the prevention of access provided as a protective measure can only be decided by a judge or a court. Even the decision given by a public prosecutor in some urgent situations must be approved by a judge within 24 hours. However, the prevention of access decision given as an administrative measure is not subject to the approval of a judge. The prevention of access means the prevention of communication which is an important cease of one of the democratic rights of the citizen. Thus the cease of this right with an administrative decision which shall be given by an administrative agent who probably would not have any legal formation, would create suspicions in relation to the appropriateness of such decision. Besides this administrative decision enters into force without any second control and the only way to oppose this decision is to file a lawsuit before the administrative courts which would take a significant amount of time to complete. Considering the importance of communication in

today's world, the regulation leading to the cease of communication only with a decision of an administrative agent cannot be approved.

Another issue in the law which is against the general principles of Turkish Criminal Law is that if the Telecommunications Authority, after deciding for the prevention of access against a publication on internet, can determine the ID of the persons responsible for the publication, should file a criminal complaint before the relevant public prosecutor office. Under Turkish law, the administrative authorities are liable to file a criminal complaint if they determine an action which creates the suspicion of a crime. For filing such criminal complaint, the determination of the action is sufficient and there is no need to determine the ID of the suspects. The determination of ID's of the suspects should be done by the judicial authorities. So this regulation is creating a system contradictory with the general provisions of Turkish criminal law.

The prevention of access decision given by the Telecommunications Authority shall be executed by the relevant access provider within 24 hours after duly receiving the decision of the Authority. The access providers which does not execute this decision within 24 hours shall be punished with a pecuniary punishment between 10.000 YTL and 100.000 YTL (approximately 5555 Euro and 55.555 Euro) and even after the decision of pecuniary punishment, if such access provider does not obey the prevention of access decision of the Authority, then the Authority may cancel the license of the access provider. The punishment of the cancellation of the license is only determined for the administrative measure under the competence of the Telecommunications Authority. There is not any cancelation of license punishment regulation for the protective measures under the competence of the courts. In a democratic country, the competences of the courts should be broader than the competences of the administration; thus this regulation should be considered as against the normal necessities of a democratic country.

3. Removal of the Illegal Content from the Publication and the Right of Reply

The article 9 of the law numbered 5651 provides the right of the removal of the illegal content and the right of reply of the persons of whom rights are breached via the publications on internet. Accordingly, the law tries to establish a solution for a very common problem encountered on internet. In fact this provision is a reflection of the Turkish Press Law.

Per the article 9, the person of whom rights are breached via the publication on internet, can apply to the content provider or in case it is not possible to reach to the content provider, to the host provider and claim the removal of the illegal content and the publication of his/her response for a period of one week. The content or host provider shall comply with such claim within a period of two days and if not the applicant may deem that the content or host provider refused the right of reply.

This provision may create problems in circumstances where the content or host providers are in abroad as these would be outside of the jurisdiction of the law and it may not be possible to execute any sanction against an entity in abroad. This problem may be solved by international agreements covering the issue.

Additionally, under Turkish law, it is provided that the host provider cannot intervene within the content to which it provides service. However, as per the article 9 of the law 5651, the host provider may be in a position to intervene within the content for the removal of the illegal content. In fact, the removal of the illegal content would not be any breach of the aforementioned provision of Turkish law. But most of times, as the host providers do not have the relevant codes to reach to certain pages of a website; they have to close the website totally. Thus, the closure of the pages of a website other than the one bearing an illegal

content would constitute the breach of the prohibition of intervention of the host providers which would create criminal liabilities for them.

In circumstances where the content or host provider does not comply with the right of reply within two days, the applicant by deeming that his/her application is refused, may apply to the competent criminal court of peace within 15 days. The criminal court of peace would establish a decision regarding the claim of the plaintiff within three days.

Upon the application of the plaintiff if the criminal court of peace decides for the removal of the illegal content and the publication of the response of the plaintiff, the host or content provider must obey to the decision of the court within two days upon being notified of such decision. In circumstances where the host or content provider does not obey the decision of the court, it shall be punished with imprisonment of six months to two years.

Conclusion

There are different opinions in relation to the regulation and control of internet in Turkey as in other countries. But all agree to the fact that the legal grounds for internet are rather insufficient. On the other hand, with the expanded use of internet, the number of illegal activities realized on internet or via internet is increasing constantly.

In Turkey, the legislators tried to satisfy the increasing need for a legal regulation of internet with the “law numbered 5651 regarding the regulation of publications made on internet and the fighting against the crimes committed via these publications”. However, despite of the existence of very appropriate provisions of the law, this law bears some provisions against the nature of the internet and the principles of a democratic state.

The main criticism which may be forwarded against the law would be the limitation in the crime types which are subject to this law. Despite this law was prepared under the social pressure occurred due to the crimes of sexual abuse of the children tracked especially with the expanded use of internet, it is obvious that the crimes committed on or via internet cannot be limited to the crime types recited under this law.

Parallely, as per the law, the prevention of access decision as a protective measure can only be determined in the existence of the crimes determined under the article 8/1 of the law. This provision besides leading to the automatic application of this measure against the crimes recited under article 8/1 makes the application of this protective measure nearly impossible against the other crimes which are not recited under the said article.

Additionally, despite the provisions ruling the prevention of access as a protective measure may be considered as appropriate considering that such decision may only be given by a judge or court or must be approved by a judge even if it is given by a public prosecutor, the continuance of the prevention of access poses a problem after the completion of the trial process. Because in circumstances after the conviction of the accused if the access is still needed to be prevented, then the court should make another decision for the prevention of access (which shall be then considered as a security measure) as the protective measures may stay in force until reaching to a judgment. However, the prevention of access is not determined as a security measure under Turkish Criminal Code. Thus without such determination, pursuant to the principle of legality in crime and punishment, it should not be possible to order for the prevention of access in a judgment.

Also, the competence granted to the Telecommunications Authority to decide for prevention of access as an administrative measure is against the general principles of Turkish law. The administrative measures should be provisional however the prevention of access determined as an administrative measure under the law does not have any provisional characteristic as it

does not provide the conditions under which this measure shall be ceased. Also, the absence of a secondary control would create suspicions in relation to the appropriateness of the prevention of access decision as this decision would be given by an administrative agent without any legal formation. Additionally, the only possible way to oppose this administrative measure is to file a lawsuit before the administrative courts which would take significant amount of time. Considering the importance of time on internet services, a regulation which provides the intervention of a lawsuit process does not suit to the purpose of the law.

Beside the above stated lacking points of the law numbered 5651, the law provides a number of important provisions beneficial in fighting against the crimes committed on or via internet. In this respect, the obligation of disclosure determined for content, host and access providers is considered as beneficial for the determination of the perpetrator of a crime committed via such internet site. Also the obligation determined for the access providers to preserve the traffic information for a period of minimum six months and maximum two years is appropriate for following the illegal activities in a website.

In conclusion, the law numbered 5651 was enacted to create a legal ground for internet communication and with some of its provisions it has provided important benefits for fighting against the crimes committed on or via internet. However, with some of its provisions providing excessive and uncontrolled powers to the administration, the law has moved out from its purpose. Thus it would be necessary to re-examine these provisions with the participation of the legal practitioners and sector representatives.

For further information on this topic please contact Volkan Dulger at Dulger Law Firm by telephone (+90 212 217 82 98) or by fax (+90 212 217 79 34) or by e-mail (volkan.dulger@dulger.av.tr)