Organization for Security and Co-operation in Europe
The Representative on Freedom of the Media

Briefing on Proposed Amendments to Law No. 5651
The Internet Law of Turkey

January 2014

Since the enactment of Law No 5651 entitled *Regulation of Publications on the Internet and Suppression of Crimes Committed by means of Such Publication*[1] in May 2007 access to approximately 37,000 websites have been denied by court orders and administrative blocking orders issued by the Telecommunications Communication Presidency (TIB) by January 2014.[2] Currently, access to popular platforms such as Scribd, Last.fm and Metacafe is blocked from Turkey. Access to Wordpress, DailyMotion and Vimeo has been blocked temporarily by court orders during the last few months. A number of alternative news websites that report news on southeastern Turkey and Kurdish issues remain indefinitely blocked from Turkey. Furthermore, several users received fines, prison time or suspended sentences for comments made on social media platforms. In September 2013, during a retrial following an appeal, the renowned pianist Fazil Say received a 10 month suspended sentence for insulting religious values on Twitter. Furthermore, a legal challenge was launched in 2011 to annul the BTK filtering policy on the grounds that it lacked a legal basis. The Alternative Information Technologies Association argued at the Council of State level that the filtering system discourages diversity by imposing a single type of family and moral values. A decision is expected during 2014.

The blocking provisions of Law No 5651 has been subject to review by the European Court of Human Rights in December 2012. In the judgment of *Ahmet Yildirim v. Turkey* involving access blocking to the Google Sites platform in Turkey, the European Court of Human Rights, finding a violation of Article 10 of the European Convention on Human Rights, held that a restriction on access to a source of information is only compatible with the Convention if a strict legal framework is in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses. Despite this important decision access to Google Sites is still blocked in Turkey.[3] The European Court's decision is in line with a 2010 study published by the OSCE Representative on Freedom of the Media which called the Turkish authorities to quickly bring Law No. 5651 in line with OSCE commitments and other international standards on freedom of expression, independence and pluralism of the media and the free flow of information. However, rather than bringing the current law in line with the OSCE commitments and other international standards, the Government proposed further restrictions that raise major concerns that will be assessed below.

1 Law No. 5651 was published on the Turkish Official Gazette on 23.05.2007, No. 26030.

2 Official statistics are not published by the TIB or any other government authorithy. However, detailed non-official statistics can be obtained through http://engelliweb.com/istatistikler/

3 Four other applications are currently pending in Strasbourg with regard to the blocking of YouTube and Last.fm in Turkey.

Undemocratic legislative process

A draft law amending Law No. 5651 was submitted to the Parliament by a number of members of the ruling party on 14 December 2013. No consultation process had been conducted during the preparation of the draft law. Although a number of academic and NGOs complaints about Law No. 5651 were known in addition to international evaluations noted above, administrative authorities and parliamentarians of the ruling party ignored such criticism.

The legislative process for the proposed amendments was even more problematic. The draft amendments were assigned to the Planning and Budget Commission at the Parliament. Furthermore, the draft amendments were added into a mixed law package (*Torba Yasa*) which included irrelevant amendment proposals on the Family and Social Policy Ministry, the Anti-Terror Law, the Social Security and the General Health Insurance Law and many others. The Commission merged seven different amendment proposals into one package. As might be expected, as the merged proposal before the Planning and Budget Commission included too many irrelevant provisions, no real expertise could cover all of them. Despite this fact, a sub-commission merged all the proposals in a single draft bill in a very short period of time and the Commission finalized its work on the draft bill on 16 January 2014.

The final version of the draft which was submitted to the Plenary Assembly of the Parliament included 125 sections and amended 42 different laws, including Law No 5651, and was adopted in less than one month. No public debate took place during this process, thus all the critiques of the amendments to Law No. 5651 were ignored.

Proposed amendment on notification (Section 3 of Law No. 5651)

The raft aw provides a new rule about the notification process. Accordingly, those who carry out activities falling within the scope of Law No. 5651 can be notified via e-mail and other communication ways gathered from Internet websites, IP addresses, URLs and similar sources. **This means that in many cases legal proceedings might start even before the relevant party becomes aware of the situation**.

Proposed amendments on the liability of hosting providers

With the proposed new amendments to Article 5 of Law No. 5651, the liability of hosting providers has been extended. Hosting providers are going to be required to retain traffic data (communications

data) in relation to their hosting activities from 1 to 2 years. Previously, Law No. 5651 only required Internet Access (Service) Providers to retain traffic data for a period of 6 months to 2 years. Further regulations will clarify the classification and liability of hosting providers as well as the exact period of data retention requirements. Hosting providers will also be required to provide the accuracy, integrity and secrecy of the information requested by the Presidency (TIB) and should also comply with the required measures that are requested by the Presidency. **Hence, the Presidency will be able to request information without a court decision or a justified reason. This cannot be compared to or considered in line with similar provisions within the European Union, as these provisions clearly establish very strict and clear limits in order for public authorities to gain access to retained data[4]. No legal way to object to this request has been envisaged within the amendments.** Thus, the Presidency can arbitrarily obtain any kind of information from the hosting providers, which is a considerable threat to private life and secrecy of communications. In case of non-compliance, administrative fines can be applied between 10,000TL (approximately €3,000) and 100,000TL (approximately €32,000).

While confined to "communications data," the combined effect of the proposed measures can provide a complete dossier on private life, raising serious privacy implications. The proposed measure is explicitly wide and the details are to be established with secondary legislation, including the retention period. **Therefore, combined with the requirement for the Internet Access (Service) Providers to retain such communications data, as explained below, Law No. 5651 will encourage mass interference and will enable the Presidency to request and collect data on the entire population of Internet users from Turkey without any judicial review or process**.

Proposed amendments on the liability of access providers

With the proposed new amendments to Article 6, Access Providers will be required to take necessary measures to block access to alternative access means, such as proxy websites.[5] These alternative methods are not clearly defined by the proposed amendments. This lack of clarity is especially important considering that under Article 6(3) of the law, Access Providers can be fined up to 50,000 TL (approximately €16,000) on the grounds that they failed to take necessary measures to block access to alternative access means.

Access Providers will also be required to guarantee the accuracy, integrity and secrecy of the

[4] See Articles 7 and 8 of the EU Directive 2006/24/EC.

[5] Within this context it should be noted that access to Ktunnel.com has been blocked in Turkey since November 2013 by a court order.

information requested by the Presidency (TIB) and should also comply with the required measures that are requested by the Presidency. As in the case of the amendments regarding hosting providers, the limits and reasons for requests have not been set out.

Amendments made to Articles 5 and 6 will enable the Presidency (TIB) to gather communications data about all Internet users without any legal limits or restrictions. Since the users never will be able to know when and how this information is gathered, the Presidency will have unlimited discretion in this field. However, in the context of covert measures of surveillance, the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.[6]

Formation of an association of access providers

The proposed amendments include a new Article 6A which creates an Association of Access Providers. The main purpose of the Association is to centrally ensure compliance of blocking decisions that are outside the scope of Article 8.

The Association will be recognized as a private legal entity and the headquarters of the Association will be based in Ankara. The by-laws of the Association will be subject to approval of the Authority (ICTA - Information and Communication Technologies Authority). The Association will be composed of all Internet service providers (within the ambit of the Electronic Communication Law No. 5809) and other corporations that provide Internet access from within Turkey. The Association will be required to coordinate co-operation between these entities.

The Association will be set up within 3 months following the enactment of the proposed measures. Membership to the Association is compulsory. Access providers or other Internet service providers, which do not apply for the membership of the Association within the first month following the establishment of the Association will be fined. Fines will be assessed at 1 percent of the net sales proceeds of the previous civil year. **Access providers who do not become members of the Association will not be able to provide access services**.

Blocking orders that are outside the scope of Article 8 (see below) will be directly sent to the Association for execution. Notification of blocking orders made to the Association will be regarded as made to all access providers. The Association may appeal against the blocking decisions that are

6 See *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, *Reports* 1998-V, p. 1925, § 46 (iii).

sent to the Association.

Although the draft law defines the Association as a private legal entity, considering its powers and duties, it is a public law entity in Turkish law. Membership to this entity is compulsory and members are required to pay monthly dues to the Association which will be decided according to their profits. The Association will also not be free to draft its own by-laws, as approval of the ICTA is necessary for it to go into effect. **Therefore, this new body cannot be seen as an entity established byfree will.**

Proposed amendments on the liability of mass use providers

With the proposed amendments Liability of Mass Use Providers (Internet cafes, etc.) has been extended. All Mass Use Providers will be responsible for retaining the logs and communication data of their users regarding access and blocking of illegal content and taking the precautionary measures in accordance with further regulations to be established by secondary legislation. **These new provisions are not clear and leave full discretion to the administration, which is a clear violation of the legality principle.** Infringement of Article 7 provisions will result in an administrative fine between 1,000TL (€320) and 15,000TL (€48,000) or an injunction to cease activity for up to three days with a decision of the local civilian authority, e.g. governors and mayors.

Proposed amendments on Article 8 concerning sanctions

Article 8 of Law No. 5651 establishes a blocking measure for websites. Although this provision has been harshly criticized by the European Court and found in violation of the European Convention on Human Rights in *Ahmet Yildirim v. Turkey*, the blocking measure was not amended. However, with the current proposed amendments the sanctions set forth in the Article were amended while not making changes to the blocking measure. Currently, responsible persons of hosting or service providers who fail to carry out the blocking decisions are subject to imprisonment from 6 months to 2 years. According to the proposed amendment, they could only be subjected to a fine. **However, such punishment would still be disproportionate.** Furthermore, in practice, prison sentences up to 2 years are also converted to fines. Two years imprisonment in practice can be converted to 770 days of fines.

However, the proposed legislation states that responsible persons will be subject to a fine from 500 days to 3,000 days. One day of a fine can be up to 100 TLs. Thus, according to the proposed new

rule, a person could be fined up to 300,000 TL (€95,000) for non-compliance with the execution of a blocking order. **This is obviously disproportionate and, although it initially appears to be a relaxation of the penalties provided in Article 8, the proposed amendments provide potentially harsher penalties for both hosting and service providers.**

Proposed amendments to Article 9 on the violation of individual rights

Within the scope of Article 9, the proposed amendments also provide for URL-based blocking orders, which would be issued by a judge of a Criminal Court of Peace. In exceptional and necessary cases, the judge may decide to issue a blocking order for the whole website if the URL-based restriction is not sufficient to remedy the violation. The judge is required to issue his decision within 24 hours of the initial request to the Court. Judge-issued orders would be sent directly to the Association for execution.

If content is removed by the time the Association is notified, the decision of the judge will be void. Otherwise, access providers should comply with the order of the Judge within 4 hours of notification. Fines would be applied in case of violations of the above mentioned requirements. As previously mentioned, fines could reach 300,000 TLs (€95,000). Furthermore, content and hosting providers will be required to respond to violations of individual rights requests within 24 hours, down from 48 hours as currently provided in law.

With this amendment, a shift from a notice-based removal and liability system to a URL-based blocking system is evident. In practice, blocking will be the measure that will be requested more often and alleged violations of individual rights claims will result in a considerable number of URL-based blocking orders. Individual Twitter and Facebook accounts, as well as YouTube videos or accounts, may be the subject of such URL-based blocking orders to be issued by criminal courts.

Proposed new measure on privacy violations

The proposed amendments include a new blocking measure in Article 9A which addresses individual privacy violations. According to this new provision, individuals and legal entities who claim that their privacy has been violated through the Internet may request access be blocked by applying directly to the Presidency. Individuals and legal entities are required to provide detailed information regarding the alleged privacy violation, including the exact URL where the violation occurred as detailed explanation of the violation. Upon issuing the blocking decision, the Presidency

directly notifies the Association and access providers should comply within 4 hours.

Presidency-issued blocking orders will be URL-based and will only involve the exact location of the allegedly infringing content. Individuals and legal entities that claim their privacy has been violated are then required to apply to a judge at a Criminal Court of Peace within 24 hours. The judge is then required to issue a decision within 48 hours and send the decision directly to the Presidency. Otherwise the blocking order is void and removed by the Presidency. The decision of the judge can be challenged by the Presidency in accordance with provisions of the Criminal Procedure Act. This amendment contains an anomaly as this provision might be understood as merely the Presidency but not the content providers or other stakeholders can challenge the decision. This means that the decision of the Presidency, once approved by a judge at a Criminal Court of Peace, can never be challenged legally. If the content is removed by the time the Presidency is notified, the decision of the judge will be void.

According to the proposed new measure, if any possible delay will result in adverse consequences regarding the protection of privacy or rights and freedoms of others, then **the Director of the Presidency can, ex officio, issue a blocking order**. In this case the Presidency will execute the order. Objections to such a blocking order can be made to a Criminal Court of Peace. Administrative restrictions on freedom of expression of this kind could violate Articles 26 to 30 of the Constitution and Article 10 of the European Convention on Human Rights regardless of whether appeals can be made to a court of law. **Laws designed to restrict freedom of expression should not grant administrative authorities like the Presidency (TIB) excessively broad discretionary powers to limit expression or content. If the provisions become law this will enable the issuing of politically motivated blocking orders and such a discretionary power may have a chilling effect on freedom of expression. Vaguely drafted provisions such as these are vulnerable to broad interpretation and therefore they could be applied by the authorities to situations that bear no relationship to the original purpose.** A 2011 OSCE Report on *Freedom of Expression on the Internet* recalled that courts of law are the guarantors of justice which have a fundamental role to play in a state governed by the rule of law. **In the absence of a valid legal basis the issuing of blocking orders and decisions by a public authority or the Director of such an authority other than courts of law is therefore potentially problematic from a freedom of expression perspective.**

Conclusion

When Law No. 5651 was originally drafted, the government announced that the main aim of the law was to protect children from harmful content on the Internet. **However, the implementation and application of the aw has shown that, rather than protecting children, the law has been systematically used to block access to legitimate content, therefore seriously violating the right to freedom of expression. Finding that the implementation of the Law No. 5651 had violated Article 10 of the European Convention on Human Rights** in *Ahmet Yildirim v. Turkey* the European Court of Human Rights held that a restriction on access to a source of information is only compatible with the Convention if a strict legal framework is in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses. Despite this finding, instead of improving freedom of expression on the Internet, the Turkish government has introduced a bill which considerably threatens fundamental freedoms. If the provisions become law, they will impose a disproportionate burden upon the Internet Service Providers and Hosting Providers. Also, the new measures **will encourage mass interference and will enable the Administration to request and collect data on all Internet users from Turkey without judicial review. The amendments to protect individual rights and privacy will result in new blocking measures while leaving unfettered discretion to the administration.**

Overall, these measures are not compatible with OSCE commitments and international standards on freedom of expression and they have the potential to significantly impact free expression, investigative journalism, the protection of journalists' sources, political discourse and access to information over the Internet.