Turkey: "Turkish Restrictions On The Internet"; The Highly Debated New Law In Turkey Enters Into Force And Is Subsequently Amended

Last Updated: 11 March 2014

Article by **Uğur Aktekin**, **Selin Sinem Erciyas** and **Bentley James Yaffe**

Gun & Partners

The Law Regarding the Amendment of the Decree Law on the Structure and Duties of the Ministry of Family and Social Policy and Other Laws and Decree Law ("Omnibus Law") that entered into force after being published in the Official Gazette of February 19, 2014 has become an important topic of debate due to the proposed amendments regarding online broadcasts and publications. The Omnibus Law contains amendments for the Law numbered 5651, on the Regulation of Broadcasts and Publications Made Online and Regarding the Countering of Crimes Committed via These Broadcasts and Publications ("Internet Publication Law"). These amendments have raised concerns of inordinate levels of state control over the use of the Internet, and the amendments have faced accusations of introducing streamlined mechanisms for state censorship.

Following widespread criticism of the Omnibus Law, new legislative measures to amend several provision introduced by the Omnibus Law were introduced as of publication in the Official Gazette of March 1, 2014.

1 Increased Responsibilities and Stricter Controls Regarding Access Providers, Content Providers and Hosting Providers

The amendments introduced by the Omnibus Law will implement the following additional requirements for companies and individuals engaged in providing Internet related services;

Content providers

- Content providers will be obligated to provide the Telecommunication and Communications Directorate ("Directorate") with the information they request, in the form that they request it presented in order to aid the Directorate in the execution of their statutory duties.

As content provider is defined as "any real or legal persons that create, amend or provide the information or data provided to users online", the scope of who will be obligated to provide the Directorate with information and data is extensive. As the amendment does not provide clear guidelines as to what information the Directorate may request and in what particular form they may request it transferred in, the inclusion of such a provision would seemingly cause an undue burden on any provider and creator of online content.

Hosting providers

- Once issued with a notification, hosting providers will be obligated to remove all offending content that falls under the scope of Articles 8 and 9 of the Internet Publication Law (both Articles will be explained below),
- Hosting providers will be obligated to store the traffic data for the services they provide for a duration that will be clarified with the publication of a later directive, but which will be between one

and two years. The hosting providers will also be responsible for the integrity and confidentiality of this stored Traffic data.
- As with content providers, hosting providers will also be obligated to provide the Directorate with the information that they request for the execution of their statutory duties.
- If the hosting providers are in violation of any of their obligations they will face an administrative fine ranging from ten thousand TRY to a hundred thousand TRY.

These increased traffic data storage measures will lead to concerns for hosting providers, as increased infrastructural burdens will require increased investment. Additionally, concerns remain that the reasoning for an increase in the duration of such traffic data has not been clearly stated. Even though the Directorate has repeatedly stated that this storage will not include personal digital data, unclear definitions might be regarded as increased opportunities for state surveillance.

The aforementioned subsequent legislative measures that came into effect on March 1, 2014, have provided a reduced scope for the definition of user traffic data and have made it necessary for a court order in the scope of an investigation or prosecution to be presented before the Directorate before such traffic data can be requested.

Access providers

- If issued with a blocking order, access providers will be obligated to block all access to the content, including any and all alternative means of access.
- As in the case of content providers and hosting providers, access providers will also be obligated to provide the Directorate with the information that they request for the execution of their statutory duties.

The amendments regarding access providers are particularly criticized due to the fact that an obligation to prevent all means of alternative will be placed on such parties. As, under the current Internet Publication Law access providers face administrative fines ranging from ten thousand TRY to fifty thousand TRY if they are in violation of their obligations, placing the burden or preventing all means of alternative access can be regarded as too broad and technically impossible task for any access provider to undertake.

Another amendment that will impose stricter controls on the aforementioned parties relates to notification process. The amendment would allow the classification of any communication to the aforementioned parties (domestic or foreign) via the communication tools on their websites or email or other means of communication directed to their contact information located through their domain name or IP address as an official notification. However, this amendment regarding the right of notification contravenes the current requirements under Turkish Law that regulate notifications made to parties. Allowing such online communication tools and emails to be classified as official notifications made to parties would seemingly undermine the certainty of attempted notifications and cause issues relating to a fair right of reply.

2 Establishment of The Association of Access Providers

One of the most controversial aspects of the Omnibus Law is the addition to the Internet Publication Law that establishes an organization called "The Association of Access Providers". This Association will be formed of all Internet service providers and access providers, and membership will be compulsory, with companies that are not members being banned from operation within Turkey. The centre of the Association will be in Ankara, and the charter and any such subsequent changes to the charter must be presented to the approval of the Directorate. The main duty of the Association will be the implementation of blocking orders issued under Article 9 and 9A of the Internet Publication Law, and the Association is tasked with the provision of any hardware or software required for such implementation. The Association will also serve as the representative of all of the parties engaged in Internet related services, with all notifications or blocking orders notified by the Directorate to the Association accepted as having been

made to the individual party/company that the notification or blocking order relates to. In their role of representative of the sector, the Association will also be able to appeal against any notification or blocking order made by the Directorate.

Having such an organization, with compulsory industry-wide membership that is so closely connected and supervised by the Directorate could be interpreted as extending state control over the private sector parties engaged in the provision of Internet related services. Additionally, the establishment of such an Association requiring compulsory membership with membership fees to be determined based proportionally on each member's net sales will increase operating costs for companies providing these Internet services.

3 Blocking Order Applications

Under the current, pre-amendment version of the Internet Publication Law, blocking orders are allowed under Articles 8 and 9.

Article 8 regards the blocking of access to content that is illegal under the Turkish Criminal Code, and grants prosecutors and judges to issue blocking orders for situations where content relating to one or more of the stated catalogue crimes are featured.

The Omnibus Law has introduced two significant amendments to this Article, the first one being that judicial authorities can now issue a blocking order that is limited to a set period of time and will expire after such a time has passed. The second and more significant amendment has replaced the sanction of a prison sentence for access providers or hosting providers that fail to comply with the blocking order with a sanction of a criminal fine.

The Omnibus Law has completely redrafted Article 9 and has introduced an additional article titled Article 9A.

Article 9 relates to the cases where a legal or real person's personal rights have been violated. In such cases the person may apply to the content provider, the hosting provider or apply directly to the criminal court of peace. The content provider or hosting provider is obligated to answer the applicant within 24 hours, and similarly the criminal court of peace is obligated to evaluate the application within 24 hours.

If an application has been made to the court and if the court judges the application valid, a decision for a partial or full blocking of access can be issued and subsequently notified to the Association of Access Providers. The Association must then implement said blocking order within 4 hours of receipt.

While the decision of the court can be appealed, the blocking order will stand during such an appeals process.

Additionally, if the offending content that was the subject of the blocking order is featured on another website, the applicant may directly approach the Association for the blocking of such content without needing to seek a further court order.

The Omnibus Law introduces criminal fines as sanctions for those who fail to implement court issued blocking orders.

While such a process for a blocking application also existed under the previous Internet Publication Law, the applicant could only apply for a court issued blocking order if their notification to the content provider or hosting provider was not answered within two days.

However, the previous form of the provision also included stricter sanctions for cases of non-compliance with a court issued blocking order, in the form of a prison sentence ranging from six months to two years.

Article 9A as included in the Omnibus Law introduces a completely different process of blocking order application on the grounds of "violation of personal privacy". This process of application is limited to real persons, and in a situation that their right to personal privacy is violated by online content they are granted the right to directly apply to the Directorate for a blocking order.

If the Directorate decides to issue a blocking order, the subsequent notification to the Association must be implemented within 4 hours. The applicant must then apply to the criminal court of peace within 24 hours in order to gain a court issued blocking order. If the court does not grant such an order within 48 hours of application, the initial blocking order implement by the Directorate will automatically be removed. The decision of the criminal court of peace can be appealed through the courts. The new Article 9A also grants the Directorate the authority to block access to the content itself without notification to the Association, if it is deemed that a delay in blocking the content will prove detrimental to the protection of personal privacy. As per the initial provisions of the Omnibus Law, this blocking administered by the Directorate could be appealed by application to the criminal court of peace, with the Directorate not being required to seek prior judicial or administrative authorization before implementing such a blocking of content. However, with the introduction of the new legislative measure that came into effect on March 1, 2014, in the situation that the Directorate issues such a blocking of content, they must submit this decision for approval to the criminal court of peace within 24 hours. The judge must then rule on the matter within 48 hours.

The second administrative route for Blocking Order Applications can be criticized as empowering an administrative body that lacks the accountability of the courts with the right to directly block access to content and websites undermining the certainty and accountability of legal processes. Concerns can and have been raised over the granting of the Directorate the right to issue blocking orders at short notice and requiring the Association to implement such orders within four hours and even granting the Directorate the right to block content themselves, especially with regards to the potential of immediate action against any potential content that is critical of government and political figures.

The fact that the "right of personal privacy" is not sufficiently distinguished from the personal rights that are under the scope of Article 9, has strengthened such concerns and opposition to the new process of blocking orders. Another unclear definition relates to the blocking of content directly by the Directorate, where "if delay proving detrimental to the protection of personal privacy" has not been clearly defined. This is a particular area of concern, as the exact application of a process that should only be resorted to in exceptional cases seems to have been afforded a wider scope of application. Even in light of the new legislative measures that came into effect on March 1, empowering the Directorate to directly block content and subsequently apply to the courts for affirmation rather than permission can be seen as continuing the aforementioned problems of application and accountability.

Another change that has been implemented with the legislative measures that came into effect on March 1 is that in situations that require application to a criminal court of peace, in jurisdictions that have multiple criminal courts of peace, the court with specific jurisdiction will be determined by the Supreme Board of Judges and Prosecutors. While this new change seemingly serves to clarify problems relating to the determination of jurisdiction, the fact that the Supreme Board of Judges and Prosecutors has recently been assigned to the control of the Ministry of Justice as a result of another controversial law has called into question the issue of government and state control over the administration of the new Internet provisions.

4. General Criticism Against the Omnibus Law

The Omnibus Law has been criticized by many parties, including NGOs, special interest groups and opposition parties in the course of its enactment in parliament and while waiting for approval of the

President. The most vocal opponents of the provisions of the Omnibus Law relating to online broadcasting and publications have been The Turkish Industrialists' and Businessmen's Association (TÜSİAD), the Istanbul Bar Association and the Turkish Bar Association.

After the passing of the Omnibus Law by Parliament, many of these parties and foreign NGOs and representatives of the EU had written letters to the President, asking him to send the Omnibus Law back to Parliament. One of the more comprehensive of these letters were drafted by the Digital Turkey Platform, a platform formed by the Turkish Informatics Foundation, TÜSİAD, the Informatics Association of Turkey, the Turkish Electronic Industrialists Association and the Association of the Manufacturers of Electronic Products under the scope and framework of the Digital Europe Initiative.

Even though the President has stated that he recognizes areas of concern within the Omnibus Law, his passing of the law would seemingly indicate that many of the civil rights and industry related concerns featured in the criticism and letters have been overlooked.

A primary area of opposition has been that the Omnibus Law is disproportionate in terms of the aims that the government has stated were behind the drafting process. Criticism has been leveled at the disproportionate powers granted to the courts and governmental institutions in the guise of ensuring that personal rights and privacy are safeguarded. TÜSİAD has also highlighted that the provisions of the Omnibus Law that remain vague and not clearly defined will place companies operating in this sector under a burden of adhering to unpredictable and, at times, technically impossible provisions. Critics have argued that in a country such as Turkey, where internet access costs are already at a high level, the introduction of vague provisions and increased technical burdens will only serve to increase the price of access and coverage.

Another area of criticism regards the perception of the provisions of the Omnibus Law as increasing the state's ability to influence, censor and surveil internet access and internet content. Statements issued by the Turkish Bar Association has emphasized that the additional powers granted to the Directorate threatens the principle of freedom of expression on the internet.

Opposition parties have also voiced their criticism of how the Omnibus Law was prepared; particularly highlighting the fact that the Parliamentary Committee that prepared the Omnibus Law was not made up of individuals qualified or knowledgeable in the required technical areas and because the Committee and government have seemingly failed to incorporate the results of a recent Parliamentary Study conveyed on the topic of Internet use.

Representatives of the European Union have also voiced concern at the more restrictive provisions of the Omnibus Law, particularly regarding the collection of personal data and issues of online censorship. The President has stated that he understood these concerns, and in his statement made after approving the Omnibus Law, he stated that these concerns would be addressed with new legislative measures to be released after the Omnibus Law came into effect.

The Minister for Transportation and Communication detailed which changes will be implemented by these legislative measures. The Minister has explained that the definition of traffic data would be reduced in scope and that a request for such traffic data would be conditional upon a court order. Additionally, it was stated that when the Directorate directly blocks access to content in situations where a delay will be detrimental, the Directorate must then refer this blocking to a court for approval within 24 hours. Then blocking of the content would be removed if the Directorate fails to refer the blocking to the court within the set time, or if the court rules against the blocking. The Minister also stated that he had conferred with the leaders of the opposition parties and that there was already bi-partisan support in place for the drafting and passing of such new legislative measures. These changes were passed by Parliament and came into effect upon publication in the Official Gazette on March 1, 2014.

However, some of the aforementioned NGOs had criticized the President for passing a law that he has openly acknowledged to be lacking in some areas, rather than vetoing the Omnibus Law to send back to the Parliament for further debate and amendment. Additionally, criticism of the proposed new legislative measures have also been made on the grounds that they do not cover all of the controversial aspects of the amendments brought by the Omnibus Law. Additional concerns have also been voiced regarding the authority of the determination of the competent criminal courts of peace being granted to the Supreme Board of Judges and Prosecutors.

5. Conclusion

While it is true that Turkey must develop in areas of security and protection of the individual with regards to online content and online services, the current provisions of the Omnibus Law seem to introduce heavy handed methods of application that tip the balance of favor away from the protection of the individual and more towards the protection of the interests of the state.

The strict and streamlined processes of court and Directorate issued blocking orders seem open to abuse in a country like Turkey where the judiciary and supervisory governmental bodies have been shown to be highly politicized.

An additional, state supervised Association that unites all of the private sector is also an area of concern for any real or legal person engaged in content, hosting or access providing services within Turkey. The requirements of the Association and the additional obligations placed on hosting providers and access providers have the potential to make the industry more expensive to operate in, for both foreign and domestic companies.

Numerous calls of opposition to the provisions of the Omnibus Law, by both national and international NGOs and special interest groups only highlights the extent to which these proposed provisions may function in clamping down on civil liberties and maintaining state sanctioned censorship and control over online content.

Footnote

1 The Minister stated that the new definition for Traffic Data will include "IP address, start and ending dates, services used and if applicable, user information and the amount of data transferred".