IT & Internet - Turkey

Compliance and the cloud

Contributed by **ELIG**

October 14 2014

Topic proposed by: P Scott Rammell, Managing Attorney - Strategy, Tesoro Corp

With governments around the world currently addressing regulations on surveillance and privacy, attention is once again focusing on the compliance issues surrounding the security of data stored in the cloud. While the effect of these developments on business appetite for cloud computing solutions is unknown, they certainly raise interesting issues around client privilege, data ownership, and IT planning in general, to ensure that companies remain compliant with international regulation, and have left many wondering about the best approaches to contractual terms and positions.

What data security rules apply to cloud computing in your jurisdiction? Are specific security requirements for cloud initiatives under consideration? Has any authority issued guidelines in this regard?

Turkey has no dedicated data protection and security law. However, the draft Law on the Protection of Personal Data is awaiting ratification. In addition, Turkey has signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, which is also awaiting ratification.

Therefore, only the following rules apply to data security in cloud computing:

- Article 20(1) of the Constitution regulates the right to a private life. Article 20(3) specifically deals with personal data, stating that everyone has the right to request such protection. This right covers being informed of, having access to and requesting the correction and deletion of personal data, and being informed of whether the data is used in line with the stated objectives. Pursuant to this article, personal data can be processed only in cases envisaged by the law or with the individual's explicit consent.
- Articles 135 and 136 of the Criminal Code regulate the unlawful acquisition, storage and disclosure, trading or broadcast of personal data as a crime. Article 138 states that non-compliance with provisions regarding the erasure and destruction of personal data is a crime.
- Articles 23 and following of the Civil Code deal with the protection of personal rights in general. The Civil Code does not specifically regulate the protection of personal data, but rather leaves the matter to the discretion of the courts.

Once in force, the draft law will be the primary legislation governing personal data protection since, according to Turkish law, a special rule on a specific matter prevails over a general rule on the same issue.

No specific security requirements apply to cloud initiatives under Turkish law. Cloud computing services are not specifically regulated and 'cloud computing' is not defined. However, if the cloud computing business model is considered to be an electronic communications service under Turkish law, such initiatives may be required to obtain authorisation from governmental bodies, and at present may not transfer personal data abroad (this provision will become ineffective on January 26 2015 following a Constitutional Court decision). As yet, no authority has issued guidelines in this regard.

What are the implications of cloud computing for data sovereignty? Is sophisticated data encryption a meaningful solution to data sovereignty concerns?

The foundation of cloud computing is the concept of a merged infrastructure and shared services, carried by large groups of remote servers which are networked to facilitate centralised data storage and online access to computer services or resources wherever and whenever they are needed. Since cloud computing services are carried by networked and physical resources converging to carry multiple services to end users, they are spread over multiple jurisdictions at the same time.

In cloud computing, the location of the data and the jurisdiction under which the data falls may be unclear, or even unidentifiable. A party using cloud computing services may have no direct

Authors

Gönenç Gürkaynak

İlay Yılmaz

relationship with or even awareness of the organisation that ultimately stores and processes its data. This is because the cloud provider that a party deals with may itself use one or more other storage or processing providers.

Managers often disregard these issues due to the cost effectiveness of cloud computing services. However, data in the Cloud is continuously networked (cloud services are not closed-circuit services) and passes through multiple jurisdictions. Thus, any data trafficked over the cloud may be subject to data surveillance, monitoring or espionage activities, as well as the lawful acquisition of the data in administrative, criminal or civil investigations against the data trafficker carried out by courts and government authorities in a jurisdiction that is unknown to the data owner and pursuant to a case or investigation unrelated to the data owner.

The current approach towards mitigating these risks seems to be converging on the execution of policies, contractual governance, sophisticated data encryption methods and sovereignty of cloud services. While policies, contractual governance and data encryption methods might mitigate these risks to an extent, they are not as effective as sovereignty of cloud services. This enables both businesses benefiting from cloud computing services and users to foresee the potential legal issues that they may face in a certain jurisdiction which they have chosen.

Under what circumstances can governments (national and/or foreign) access data stored in the cloud? Must the information owner be informed before this happens? What are the rules of engagement in terms of transparency and accountability?

The Constitution adopts the principle of territoriality. Therefore, any foreign government can access data stored in Turkey only by following the legal procedures established by extradition treaties (if any) and international regulations.

As stated above, the cloud computing business model may be considered to be an electronic communications service under Turkish law. In such case the service provider must submit information, documents and data to the authorised authorities within the timeframe set out in Article 19 of the Regulation on the Authorisation for Electronic Communications.

Further, under Article 7 of the Law on Police Powers (2559), authorised authorities may request such information from electronic communications service providers in the following cases:

- matters of national security;
- organised crime regarding drug trafficking or manufacturing;
- organised crime regarding illegal profit or crimes committed via threat or violence; and
- crimes committed against the government.

Article 7 states that the authorised authorities are the courts. However, it also states that in urgent cases, by written order of the director of the General Directorate of Security or the head of the Police Intelligence Department, communications via telecommunications services can be located, monitored and recorded, and signal information can be evaluated. Data may also be requested during an investigation or prosecution by the public prosecutor, the courts or other authorised authorities determined by the laws. Certain laws also entitle some authorities to conduct raids and access data on site, such as government tax auditors and authorised persons of the Competition Authority. There is no requirement that the data owner be informed before accessing the data.

Cloud computing initiatives might be considered to be "hosting providers" under Article 2(m) of the Law on Regulation of Broadcasts via the Internet and the Prevention of Crimes Committed through Such Broadcasts (5651). That law defines 'hosting providers' as "real persons or legal entities that provide or run systems to contain services and content". Under Articles 5(3) and (4), a hosting provider must:

- keep the traffic information of services that it hosts for a period set by regulation (but no less than one year and no longer than two years);
- maintain the accuracy, integrity and confidentiality of such information;
- deliver any information requested by the Presidency of Telecommunication and Communication in the requested form; and
- take any measures ordered by the presidency.

Non-compliance with these provisions will trigger administrative fines.

Article 20(3) of the Constitution clearly states that personal data can be processed only in cases provided for by law or with the individual's explicit consent. The above explanations are the cases set down by law.

These authorities are government authorities are subject to the transparency and accountability regime for government authorities established by the Constitution. For instance, the presidency may be subject to the supervision of the National Assembly, the Court of Accounts, the State Supervisory Council and the Ombudsman, depending on the specific supervision requirements.

However, there are no rules of engagement in terms of transparency and accountability when accessing data stored in the cloud as Turkey does not have fully fledged data protection legislation setting out these rules. That said, a natural or legal person is entitled to obtain information from

governmental authorities by the Constitution.

What are the implications of cloud computing in case of litigation? What are the implications for privilege?

The implications of cloud computing in litigation practice mainly affect criminal law and digital forensics areas. Issues include:

- whether search warrants can be issued for data stored in the cloud;
- how such warrants should be exercised;
- how the data in the cloud should be copied; and
- how an online search warrant can be exercised.

Turkish legislation does not specify client privilege in terms of personal data. Under the Constitution, everyone has the right to request the protection of their personal data. This right covers being informed of, having access to and requesting the correction and deletion of personal data, and being informed as to whether the data is used in line with the stated objectives. Pursuant to this article, personal data can be processed only in cases envisaged by the law or with the individual's explicit consent.

Therefore, if any personal data processing is carried out within the scope of Turkish law, privilege becomes irrelevant.

How can risks relating to cloud services be mitigated (eg, contractual safeguards, insurance etc)?

In order to mitigate the risks related to cloud services, a user must first choose which cloud service to use (eg, a source infrastructure for software development, a software delivery mechanism or a data storage service) and then determing the right cloud architecture for the relevant needs.

There are three main cloud service models:

- public clouds – multi-tenant architecture that provides pay-per-use, scale-on-demand benefits along with standardised configurations, security protections and service levels, but little configuration;
- private clouds – built exclusively for multiple business units or functions within a single company, which controls and configures the cloud's infrastructure, security and capacity; and
- hybrid clouds, which offer the functionality of a public cloud alongside the security and control of internally hosted environments.

Individual users mainly use public clouds. Therefore the main risk for such users is the breach of their personal privacy and unwanted third-party access to their personal data. This issue has gained serious media attention after photos of Hollywood actresses were obtained from the cloud by hackers and published online in August 2014.

However, the issues raised by cloud service businesses are quite different. Many countries are developing new laws to regulate data privacy and related matters in regard to cloud services, and the likelihood of a unified global standard for cloud computing is low. One of the most serious issues in this regard is data sovereignty. In order to mitigate the risks in this area, businesses should adopt policies resulting from detailed and thorough processes in order to address any risks related to data sovereignty. In addition, these policies should be administered and monitored vigilantly.

The contractual relationship between a business and a cloud service provider is another major way for businesses to mitigate certain risks which may arise from legal lacunae regarding cloud computing services. Thorough negotiation of contractual terms is key in this area. There is a conflict of interests between the cloud service provider and the businesses using the service. Cloud service providers often offer standard form contracts containing boilerplate terms in their own favour, while business users aim to mitigate the risks that may arise from use of the Cloud.

The contractual safeguards in this regard will include provisions on:

- how to store data;
- data breaches;
- governing law and venue;
- employee screening;
- the breach notification regime;
- measures to prevent unwanted access to the dedicated cloud space;
- detailed explanations as to who can have access;
- detailed and accurate *force majeure* clauses;
- data recovery conditions;
- damage and disaster recovery conditions;
- liability of contracting parties for the actions of subcontractors;
- supervision of the cloud service providers' acts regarding data stored in the dedicated cloud

space; and
- insurance policies.

For further information on this topic please contact Gönenç Gürkaynak or İlay Yılmaz at ELIG by telephone (+90 212 327 17 24), fax (+90 212 327 17 25) or email (gonenc.gurkaynak@elig.com orilay.yilmaz@elig.com). The ELIG website can be accessed at www.elig.com.