NORTON ROSE FULBRIGHT

Biometrics in Turkey

Content

Introduction

This article was written by Olgu Kama, Partner at İnal Kama Attorney Partnership, affiliate firm of Norton Rose Fulbright in Turkey, and Lale Tüzmen, Foreign Legal Advisor at Norton Rose Fulbright

The use of biometrics, the measurement of unique human physiological and behavioral characteristics, has been incorporated into a multitude of technologies that are used on a daily basis to facilitate the identification or authentication of individuals. According to the EU General Data Protection Regulation (GDPR), "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data" means biometric data. Physiological characteristics include those identified from the fingers and hands, veins, face, eyes, ears, odor, and DNA. In contrast to physiological traits, behavioral characteristics (or a combination of both physiological and behavioral traits) also are increasingly utilized by biometric systems. Behavioral characteristics are generally dynamic and can be affected by various factors, including age, illness, or emotional state.

Global trends in use of biometrics

Fingerprints and retinal scans may be two of the most common types of biometric data, but organizations are increasingly experimenting with technologies that make use of biometrics. For example, Visa is working on a system to help banks incorporate biometrics into eCommerce, which follows on from Mastercard's continued interest in 'selfie pay' technology. Meanwhile, certain security companies are working on using facial recognition software in casinos and high-end retailers to alert employees when a VIP customer walks in. Gait and gesture recognition continue to be developed to enhance current authorization systems, such as authentication of signature through the hand motions. Smart watches collecting heart pulse data, online games collecting the reaction time of players and online platforms collecting typing speed are other examples of processing biometric data.

Use of biometrics in Turkey

Turkey has been following global trends in the adaptation of biometrics in technology, particularly in identification and security technologies. As of 2018, Turkey has a population of 82.4m1[1]. 96 percent of the population owns a mobile phone[2], 41.9m of which are smartphone users3. In other words, Turkey is producing a lot of personal data that is likely to be processed. In big cities like Istanbul and Ankara, security systems such as hand geometry recognition, iris or fingerprint scans are widely used to enter office buildings, new residential complexes and even luxury gyms. Mobile service providers, banks and insurance companies use voice recognition to authorize their customer's access to their accounts. Another example of voice recognition is voice command technologies used in recently released cars that Turkey imports from other countries.

However, despite using biometrics in different contexts from touchID of smartphones to voice recognition to pay internet bills, collection, storage, processing and destruction of biometric data was not regulated by privacy laws in Turkey until 2016. The law that entered into force in 2016 originated from the European Union Directive 95/46/EC; however, certain areas still remain untested or are yet to be clarified by lawmakers.

Biometrics and data protection regulations

In Turkey, the main regulation governing the protection of personally identifiable information is the Law No. 6698 on the Protection of Personal Data (the "Data Protection Law") that came into effect on April 7, 2016. Before, it was not clear how biometric data would be treated under Turkish law. The Council of State ruled on several occasions that since privacy is a constitutional right, and storing and using biometric data is a limitation to that right, such a waiver can only be granted by a duly enacted law. In fact, the Council of State declared face recognition and fingerprint recognition practices in public buildings unconstitutional due to the violation of privacy[28]. Therefore, the entry into force of the Data Protection Law was a milestone in the regulation of biometrics in Turkey as it introduced the long-awaited regulatory framework for protection of biometric data. The Data Protection Agency ("DPA") board members were sworn in and their mandate started on January 12, 2017. The Regulation on Personal Health Data entered into effect on June 21, 2019 after its predecessor regulation was twice deemed unconstitutional by the Council of State.[29]

Under the Turkish data protection regime, personal data may not be processed without the data subject's explicit consent. Biometrics are treated as sensitive data under the Data Protection Law and are subject to the rules applicable to protection of sensitive personal data.

Biometric data may only be processed without the data subject's explicit consent if it is for the purposes of the protection of public health, the provision of preventive medicine, medical diagnosis, treatment and care services, or the financial planning and management of healthcare services. Data that falls within one of these exceptions may only be processed by persons or authorized institutions bound by the duty of confidentiality.

As a rule, personal data may not be transferred outside of Turkey without the data owner's explicit consent according to the Article 9(1) of the Data Protection Law. However, Article 9(2) provides an exception and accordingly personal data may be transferred abroad without explicit consent of the data subject provided that one of the conditions set forth in the Article 5(2) (one of the conditions applicable to the case is "it is clearly provided for by the laws") and the exceptions stated in the Article 6(3) exist and (a) sufficient protection is provided in the foreign country where the data is to be transferred or (b) the controllers in Turkey and in the related foreign country guarantee a sufficient protection in writing and the Board has authorized such transfer, where sufficient protection is not provided. Therefore, health data that falls within one of the exceptions listed above can be transferred outside of Turkey if the recipient country provides sufficient safeguards. The DPA has still not published the list of countries where sufficient data protection safeguards are provided. Therefore, in this case, Article 9(2)b could apply, which indicates that in order to transfer data outside of Turkey, the data controllers in Turkey and in the recipient country should sign a written undertaking to guarantee sufficient safeguards and obtain the DPA's approval. The DPA's approval will take into consideration the reciprocity of data transfer to Turkey from the country where data is intended to be transferred.

Recent DPA decisions on biometrics

In July 2019, the DPA published two decisions on biometrics, which was the first time the DPA has ruled on biometrics[30]. Both decisions concern gyms that have hand-fingerprint recognition systems for the entry and exit of gym members. Also, the gyms made passport photos of the members and information such as the member's last visit time visible on TV screens that could be seen by everyone in the gym.

In its reasoning, the DPA ruled that a reasonable balance between the data processing activity and the intended purpose, in other words, the principle of proportionality, is not observed in these cases. The DPA underlined that there are alternative and less intrusive ways to reach the gyms' goals of controlling the entrance/exit of the gyms; personal data that is not necessary for the realization of the data processors' goals should not be collected and/or processed.

Explicit consent does not render excessive collection of data legitimate, even if the processing of personal data is carried out with the consent of the person concerned. However, in these cases, the DPA ruled that the conditions of explicit consent are not met as giving permission to hand/fingerprint recognition was mandatory under the gym membership agreement. In addition, the gym had the right to terminate the membership in case the member does not consent to the hand/fingerprint recognition at the entrance to the gyms. Considering that gym members were not able to benefit from the gym without consenting to the processing of their biometric data, it is not possible to say that there is express consent.

Finally, the DPA ordered the gyms to immediately dispose of the biometric data they have collected and stop collecting/processing biometric data. These two cases were brought before the DPA based on consumer complaints and show that the DPA is strictly enforcing the rules on processing biometric data. With these two precedents, the DPA has set the ground for similar uses of biometric data, which we will most likely see in the near future.

Other rules on biometrics

New biometric ID cards

In 2016, the Law No. 5490 on Civil Registration Services was amended[4] to the effect that national ID cards will store biometric data and this data may not be used for purposes other than identification. However, what the biometric data would entail was not defined until 2017 when the same law was amended again. Accordingly, biometric data to be stored on national ID cards was defined as: "Personal data obtained from fingerprint, vein trace and palm taken to ensure the identification and authentication process through electronic systems."[5]

Similarly. Turkey also switched to new drivers' licenses with an electronic chip in 2016, which hold data relating to the holder's fingerprints and blood type. The deadline for changing existing drivers' licenses to a new one with an electronic chip is 2021.

Banking regulations

The Turkish Banking Regulation and Supervision Agency has published rules on information systems security.[6] Accordingly, the ID verification mechanism applied to customers should be composed of at least two different components independent from each other; data points that are "known" by the customer, "owned" by the customer or "which is a biometric characteristic" of the customer. For the element "known" by the customer, components such as password/changeable password may be used; and for the element "owned" by the customer, a changeable password producing device, changeable password procured by SMS service may be used. The components shall be entirely special to the customer and the ID verification shall not be realized and the services shall not be accessed without presenting those components.

This communiqué was amended and the definition of biometric data was added in 2010 as follows: "Biometrics means the unique human physiological and behavioral characteristics that are measurable and attributable to that person." This rule is the legal basis for the voice recognition systems used by banks for their customer service hotlines.

Employment law

Under Labor Law No. 4857, employers are required to keep a file for each employee. This file must include all relevant information and documents required by law, in addition to personal information. The employer must submit the file to the appropriate public authorities for inspection whenever asked. However, the employer is obliged to maintain the files in a lawful manner with utmost good faith and not to disclose any information that the employee might have a legitimate interest in keeping confidential.

The DPA has published specific guidelines for employers on how to protect employees' personal data. Accordingly, employees are required to ensure that their employees receive data protection training. There should be disciplinary sanctions if the employees act against the data protection policies and procedures of the company.[7]

Races/games

Another interesting use of biometrics for security reasons was recently introduced in 2018 with an amendment to the Horse Races Regulation. Accordingly, registering a horse for a derby now requires biometric identification of the horse owner or an authorized representative through face recognition, fingerprint recognition, palm veins recognition, etc.

On the other hand, the new electronic card system called "Passolig", which replaced all printed tickets for soccer games, does not use biometric recognition systems that are becoming widely used in other countries' stadiums. There is currently no talk of changing it to a biometric system, but it could be implemented in the future as a further security measure.

Biometrics regulations and vehicles

Since the Data Protection law has been in place only since 2016, there are still some untested areas under the data protection regime in Turkey. The Highway Traffic Law No. 2918 (the "Highway Traffic Law") does not yet include provisions relating to autonomous vehicles. Due to the unanswered questions on protection of sensitive data (for example, the question of to which countries sensitive data can be sent), and the likelihood of additional legislation in the future, Turkish automobile manufacturers as well as importers should be careful to consider privacy requirements to avoid data breach fines.

Consequences of non compliance

Data may not be processed without the explicit consent of the data subject, except as explicitly listed under the legislation. Also, data must be collected for a specific and legitimate purpose, be relevant and not disproportionate to the purpose of processing, and be processed in accordance with the general principles set by the law.

In case of an unauthorized destruction of, disclosure of, or access to personal data, the subject may either follow the specific application and complaint procedures under the Data Protection Law and the Communiqué on the Principles and Procedures regarding Applications to the Data Controller (the "*Communiqué on Subject Access Requests*") or it may resort to other remedies foreseen under Turkish law as explained below.

Turkish Criminal Code provides for criminal sanctions for violations of laws on the use of personal data. Criminal acts regulated under the Turkish Criminal Code directly relating to the use of personal data are as follows:

- Violation of privacy (Article 134)
- Unlawful recording of personal data (Article 135)
- Unlawful access to or disclosure of personal data (Article 136)
- Failure to destroy any data subject to destruction as per relevant laws (Article 138)

Unlawful collection of personal data with respect to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, sexual life or health conditions is an aggravating circumstance.

As per Article 140 of the Turkish Criminal Code in case the abovementioned criminal acts are committed by legal entities, specific security measures will apply, such as revocation of privileges, disgorgement of lost profits, or confiscation of property used for unlawful purposes.

The default jurisdiction rule is that Turkish laws apply to criminal offences committed within the Turkish territory (including its airspace and territorial waters). In addition, under specific circumstances, Turkish law may apply even if the criminal offence has been committed outside of Turkey. Criminal offences committed by a Turkish citizen or a foreigner may be subject to Turkish laws, if they are (i) one of the special category crimes listed under the Turkish Criminal Code (e.g., crimes against the security of the state, constitutional order, national defense, relations with foreign states) or (ii) punishable by imprisonment of at least one year.

Offenders of breach of privacy and unlawful collection of personal data might be subject to one to three years of imprisonment, while unlawful access to or disclosure of personal data is punishable by two to four years of imprisonment. Commission of the said offences (a) by a public official misusing his/her position or (b) by benefiting from convenience offered by a profession or trade, are aggravating circumstances.

Footnotes

[1] Turkish Statistical Institute, 2018 Population Statistics.

[2] "Turkish Heritage." *Technology - Turkish Heritage Organization*, www.turkheritage.org/en/issues/technology.

[3] "Smartphone Users in Turkey 2017-2023 | Statistic." *Statista*, www.statista.com/statistics/467181/forecast-of-smartphone-users-in-turkey/.

[4] Law No. 6611 on Amending the Military Service Law and Certain Other Laws dated January 14, 2016 published in the Official Gazette No. 29606 dated January 27, 2016.

[5] Law No. 5490 on Civil Registration Services dated April 25, 2006, published in the Official Gazette No. 26153 dated April 29, 2006.

[6] Communiqué on Principles to be Considered in Information Systems Management in Banks, published in the Official Gazette No. 26643 dated September 14, 2007.

[7] DPA's Personal Data Security Guidelines (Technical and Administrative Measures). Data Protection Agency. Ankara. January 2018.

[8] DPA decision dated 03/25/2019 and numbered 2019/81 and DPA decision dated 05/31/2019 and numbered 2019/165.

[9] This regulation replaced the Regulation on Processing and Ensuring Privacy of Personal Health Data, published in the Official Gazette on October 20, 2016, which was suspended twice by the Council of State due to being deemed unconstitutional.

[10] DPA decision dated 03/25/2019 and numbered 2019/81 and DPA decision dated 05/31/2019 and numbered 2019/165.

Contact

Ayşe Yüksel Mahfoud

Head of Cross-Border Practices;
Partner-in-Charge, Istanbul

New York | Istanbul

Practice areas:

Corporate, M&A and securities | Banking and finance | Litigation and disputes | Crisis management | Risk advisory | Regulation and investigations | Technology | Employment and labor | Data protection, privacy and cybersecurity