
Asena Aytuğ Keser


Filiz Toprak Esin

When the Turkish Data Protection Act entered in force back in 2016, it provided a two-year period for data controllers to bring their data protection policies in conformity with the new law. Since the April 7 expiry of this transition period there has been a boom in the area of data protection similar to what has recently happened in Europe with the General Data Protection Regulation's entry into force.

Although it seems for the time being that the focus is mostly on this conformity process, there is also the criminal law aspect of the matter to which one should not turn a blind eye. As a matter of fact, criminal sanctions on data protection breaches date back further than the DPA as illegal recording, distribution, receipt, transfer and non-destruction of personal data were already criminalized under the Criminal Code. Now, with the newborn provisions of the DPA that introduce the rules and principles for processing personal data and also refer to criminal liability in case of breaches of the law, how these two laws will apply together is an issue of concern.

Criminal Code's approach

The provisions that directly concern the protection of personal data take part in Articles 135 – 140 of the Criminal Code. Article 135 sets out a penalty of imprisonment from one to three years for illegal recording of personal data. The second paragraph of the article regards the recording of personal data concerning political,

philosophical and religious opinions, racial origin, moral tendencies, sexual life, health conditions and union connections as the aggravated form of the crime and foresees a half-rate increase in the imprisonment period. Article 136 provides a penalty of imprisonment from two to four years for illegal transfer, distribution and receipt of personal data. Finally, Article 138 criminalizes non-destruction of personal data in spite of the expiry of retention periods foreseen by laws with one to two years imprisonment.

To put it briefly, in a broad sense, the Criminal Code lists the illegal recording, receipt, transfer, distribution and non-destruction of personal data as the acts establishing a crime and provides an additional protection for personal data concerning political, philosophical and religious opinions, racial origin, moral tendencies, sexual life, health conditions and union connections.

The DPA's approach

Within Article 17 the DPA makes reference to Articles 135 – 140 of the Criminal Code in terms of the crimes concerning personal data with very broad wording. Only in paragraph two, it sets out a more specific rule by clearly referring to the application of Article 138 of the Criminal Code in case of failure to erase or anonymize personal data contrary to the provisions of the DPA.

Under Article 18, the DPA clearly identifies breach of disclosure, data security, and registration and notification to data controllers' registry requirements, and also non-compliance with the decisions of the Data Protection Board as misdemeanor acts and keeps such breaches out of the application of the Criminal Code.

With regards to special categories of personal data, the DPA adds to those listed under the Criminal Code the following: personal data concerning racial and ethnical origin, sects or other beliefs, appearance, association or foundation memberships, criminal convictions, and security measures and biometric and genetic data. Contrary to the Criminal Code, individuals' moral orientation is left out of special categories of personal data under the DPA.

Evaluation of two approaches

As one would expect, the DPA applies not only for recording, receipt, transfer, distribution or non-destruction of personal data, but for any kind of operation on personal data — in technical terms, for processing of personal data. As a natural consequence of this, when the DPA refers to the Criminal Code in terms of criminal liability, it aims for the application of the relevant provisions of the Criminal Code for any type of processing of personal data.

On the other hand, the relevant provisions of the Criminal Code do not take acts of processing other than those mentioned above into its scope. Due to the principle of legality, this precludes the application of the Criminal Code where personal data is processed by means of the unlisted acts and such act could not be linked to one of the listed ones. That means some ways of illegal processing of personal data would not lead to any criminal liability. In point of fact, whether imposing criminal sanctions for any data security breach provides the desired way of protection is a separate matter of debate. However, it is obvious that with the different levels of protections they provide, the current provisions of these two laws cause an ambiguity which could give place to contradictory practices.

That being the legal interpretation of the current provisions in view of the strict nature of the legality principle, a different practice might be shaped by the Court of Appeals if it applies Articles 135 and 136 in a wider sense considering the spirit of the DPA and the protection it wishes to ensure. However, one must remember that broad interpretation is not allowed from the perspective of criminal law. Thus, an interpretation that would fit in the purpose of the law is a difficult task for a criminal judge. Instead, lawmakers should take action in order to eliminate any discrepancies and misinterpretation.

A parenthesis should be put here. If we happen to face the former scenario where the legality principle is adhered to, there is no wonder that criminal proceedings would remain fruitless. On the other hand, this does not change the fact that there will still be a violation of the DPA as it deems the unlisted acts illegal. This would, by reference of Article 12 of the DPA, trigger application of Article 18 of the DPA which sets out misdemeanor

acts and administrative fines to be imposed thereof. Article 12, in a broad sense, is a provision listing the obligations of data controllers in terms of data security and a failure in that context is deemed as misdemeanor act. The problem here for those who would probably feel relieved thanks to exclusion from criminal liability is that the Data Protection Board implements Article 12 in excessively broad terms by regarding any kind of breach as a data security issue, regardless of that breach being in the scope of Article 12. As a result of this criticized approach of the Board, criminal liability is replaced by serious fines that could reach up to TRY 1 million (approximately EUR 200.000 as of July 2018).

Another distinction between the DPA and Criminal Code results from the mismatching scope of special categories of personal data. As explained above, some personal data defined as a special category in the DPA is not defined as such by the older Criminal Code. The result is that even if these types of personal data (concerning racial and ethnical origin, sects or other beliefs, appearance, association or foundation memberships, criminal convictions and security measures and biometric and genetic data) are of special category under the DPA, they are out of the scope of the additional protection provided by the Criminal Code and subject to the application of the basic form of the crime as under Article 135/1. On the other hand, personal data concerning individuals' moral orientation, which is regarded as special category of personal data under the Criminal Code only, enjoys further protection as being subject to the application of the aggravated form of the crime although it is not listed under the DPA. This additional protection over personal data concerning moral orientation is criticized also because of the unidentifiable and vague character of the meaning and content of moral orientation which may cause misinterpretations. In order to be able to provide the desired protection, such ambiguities should be cleared out and DPA should be regarded as the sole guidebook for that purpose.

One last note before concluding this section should be that the confusion caused by the unlisted acts in the Criminal Code and principle of legality by extension is not a ma er of concern in the context of erasure and anonymization of personal data. To clarify, while Article 138 of the Criminal Code regulates non-destruction of personal data, Article 17/2 covers failure to erase and anonymize. Therefore, one may think that criminalization of anonymization would also violate the principle of legality as the Criminal Code does not cover it. However, the clear wording and reference of Article 17/2 gets ahead of this interpretation by reading that these acts shall be punished in accordance with Article 138 of the Criminal Code.

Conclusion

Needless to say, in the presence of these different and mismatching scope and concepts of the two laws, the best solution to this upcoming potential confusion and contradiction in practice would be to make necessary revisions primarily in the Criminal Code and also in the DPA if need be, and by this way clear out the distinctions completely. However, at least for the time being where the focus is on compliance with the regulatory requirements of the DPA, this is more like a secondary issue and therefore, no such project is on the table.

That is why a key concern of today is the way this will affect the practice and reflect on the precedents of the Court of Appeals. Considering that the DPA is a quite new law, it would not be wrong to say that there has not been any sophisticated debate at the court level so far which could have started forming the practice. Another consequence is that the precedents of the Court of Appeals given to date also remain insufficient to provide proper guidance as they are limited in scope and mostly belong to the period prior to the DPA.

Under these circumstances, one may expect contradicting decisions especially at the first instance stage of trial proceedings until the Court of Appeals start to set some standards in interpretation and implementation of the relevant provisions of the DPA and Criminal Code.

photo credit: szeke Istanbul (h p://www.flickr.com/photos/43355249@N00/34243609056) via photopin (h p://photopin.com) (license) (h ps://creativecommons.org/licenses/by-sa/2.0/)