
Where to Draw the Line of the Scope of Right to Access to Personal Data? The Constitutional Court Ruled on One's Right to Access Their Own Personal Data

Where to Draw the Line of the Scope of Right to Access to Personal Data? The Constitutional Court Ruled on One's Right to Access Their Own Personal Data

Article by Ertuğrul Can Canbolat, Alper Karafil and Su Başak Satır

On 20.12.2022, The Turkish Constitutional Court's ("Constitutional Court") decision concerning the right to an effective remedy in connection to the right to request protection of the data subject's personal data within the scope of the right to respect for private life was published in the Official Gazette^[1]. In its decision, the Constitutional Court established that the failure to examine the merits of an applicant's lawsuit renders a theoretically available remedy ineffective. In other words, it was determined that a remedy which can be considered effective at the theoretical level loses its capacity to offer a chance of success due to the interpretation of the courts.

In parallel with the foregoing, the Constitutional Court decided that the applicant's right to an effective remedy in connection to the right to request protection of the data subject's personal data has been violated and ruled a retrial by the court of first instance to eliminate the consequences of the violation. Nevertheless, the Constitutional Court rejected the applicant's claim for damages, addressing that a retrial in order for elimination of the violation and its consequences would provide sufficient compensation.

Determinations Made Within the Scope of the Case and General Principles

It was understood by the Constitutional Court that the internet data of the phone line registered in the name of the applicant, log records, IMEI information of the phone, information about the date of using Hot Spot are within the scope of information about a specific natural person. Accordingly, it has been evaluated that accessing this information, requesting their correction or deletion and learning whether they are used for their purposes should be examined in terms of the right to request the protection of personal data within the scope of the right to respect for private life. In addition, it was determined that the information regarding the phone numbers and log records of other subscribers who receive the same, common, single IP number when the applicant uses the internet via his mobile phone was also within the scope of information about a specific natural person in terms of these persons. The inaccessibility of this information was examined within the scope of the right to respect for private life in relation to the allegations of violation of the right to request protection of personal data and the right to an effective remedy.

It has been observed by the Constitutional Court that the court of first instance and court of appeal, with a very narrow interpretation, found the requests in question to be related to material data rather than a right or legal relationship and dismissed the case by not examining the merits of the case due to the lack of an interest requirement. The Constitutional Court stated that this interpretation prevented the applicant from accessing his personal data.

Furthermore, it was understood by the Constitutional Court that no reason was given in accordance with the requirements of the right to request protection of personal data in the rejection of the applicant's request to access his personal data, and no relevant and sufficient rationale that could justify such a practice was set forth. In addition, it was determined that the court of first instance and court of appeal had never discussed and clarified the obligations of the company in terms of providing access to this data, taking into account both the provisions of the Law No. 6698 on the Protection of Personal Data (“**KVKK**”) and other relevant legislation. Consequently, the failure to examine the merits of the dispute in the case, which could have enabled the applicant to benefit from constitutional guarantees, rendered a theoretically available effective remedy ineffective. In other words, a remedy that could be considered effective at the theoretical level was found to have lost its capacity to offer a chance of success due to the interpretation of the court of first instance and court of appeal.

It was decided that the right to request the protection of data subject's personal data within the scope of the right to respect for private life and the right to an effective remedy in connection with this had been violated due to the interpretation of the court of first instance and court of appeal preventing the examination of the merits of the applicant's request to access his personal data.

Advent of the Series of Disputed Events

The applicant requested from the company of which he was a customer the internet data, log records, IMEI information of his phone, and the dates when he used Hot Spot in respect of the years 2014-2015. The applicant also requested from the company to share with him the IP numbers that he shared with other subscribers when he used the internet on his mobile phone, and the log records of the phones belonging to other subscribers in these shared uses on the dates when he received a single IP number that was the same as his phone number.

The applicant's request was rejected by the company's customer services on the grounds that this information was kept in the company's records for five years and would only be shared upon a court's request. Subsequently, the applicant filed a lawsuit at the Istanbul Anatolian 1st Consumer Court. In his petition, the applicant stated that the information he requested was related to his private life and it should be shared with him, averting that he was victimized due to the company's stance. Thereby, he demanded that the aforementioned information be provided to him, and non-pecuniary damages be granted.

The court of first instance dismissed the lawsuit on 18.04.2017. In the reasoning of the decision, it was stated that the applicant had filed a lawsuit with the request to determine whether the phone

number registered to him in August and September 2014 had common IP information and whether a Hot Spot operation was performed, and if a common IP was provided, to determine the relevant phone numbers. In the decision, it was emphasized that the issues requested to be determined in the lawsuit were related to material data rather than a right or legal relationship. It was stated that the aforementioned data did not constitute the subject of the declaratory action, and therefore, the existence of an interest could not be proved, and the conditions for non-pecuniary damages were not met since no damage had occurred.

The applicant appealed against the decision. The 3rd Civil Chamber of the Istanbul Regional Court of Appeals rejected the applicant's appeal on 10.11.2017. In the decision, it was stated that the information requested by the applicant was outside the scope of information required to be shared pursuant to the legislation. It was emphasized that the information in question could be provided to judicial authorities with a judge's decision in order to reach the perpetrators of the crimes. On the other hand, it was stated that the applicant's request did not meet the conditions for a declaratory action, since the applicant could not claim and prove that he had a current benefit worthy of legal protection before the consumer court. Further, the applicant's request was not for the determination of the existence of a legal relationship, but for material data. However, this issue could be put forward as a request for the determination of evidence. In addition, it was evaluated that the claims and reasons put forward in the petition did not meet the requirement of violation of personal rights for non-pecuniary damages.

Finally, the applicant applied to the Constitutional Court on the grounds that as a result of the rejection of the lawsuit he filed at the Consumer Court, he could not use his right to access his personal data, to learn whether this data was correct or not, and to correct any errors in this information. In doing so, he claimed that his right to protection of personal data, right to respect for private life, freedom to seek rights and right to property were violated.

The main claim of the applicant was that he had not been provided with an effective, serious and result-oriented solution to the lawsuit he filed with the request that his personal data be given to him, and compensation be awarded. In this context, it has been concluded that the applicant's claims should be evaluated within the scope of the right to effective remedy guaranteed under Article 40 of the Turkish Constitution (“**Constitution**”) in conjunction with the right to protection of personal data regulated under Article 20 of the Constitution.

General principles adopted by the Constitutional Court

The third paragraph of Article 20 of the Constitution states that the right to request the protection of personal data includes the right to be informed about personal data concerning oneself, to access such data, to request their correction or deletion and to learn whether they are used for their intended purposes.

The right to be informed about and have access to personal data concerning oneself is deemed to be an extension of the principle of transparency or openness of data processing by the Constitutional

Court. It is evaluated that the fact that individuals know which data about them are processed, by whom, when and for what reason, makes it possible for them to exercise their rights to rectify, erase and restrict such data and is complementary to the realization of these constitutional guarantees.

Moreover, it is established that the processing of personal data should be carried out in a transparent manner, and as a requirement of this, data subjects should be given the opportunity to access their personal data and necessary measures should be taken to ensure that this opportunity is easily used.

In terms of the right to request the protection of personal data within the scope of the protection of private life, it was emphasized that the state has a positive obligation to protect all individuals under its jurisdiction against risks that may arise from the actions of public authorities and other individuals, as well as the person himself.

Positive obligations should ensure the protection of the material and moral well-being of individuals and the cessation of ongoing interference. They should also enable individuals to effectively challenge the acts, actions or omissions that are the source of the interference and to seek redress for any harm caused. This is deemed to be only possible if an effective remedy is available.

The right to an effective remedy can be defined as providing everyone whose constitutional right has been violated with the opportunity to apply to administrative and judicial remedies that are reasonable, accessible, and capable of preventing the occurrence or continuation of the violation or eliminating its consequences (providing adequate remedy) in accordance with the nature of the right[2].

Relevant Case Law and Certain Key Remarks

The Personal Data Protection Board's ("**Board**") decision concerning the failure of the data controller to respond to the request of the data subject to provide a copy of their personal data within the scope of their personal file may be deemed relevant to the foregoing decision[3]. In this case, the person requested to access their personal data pursuant to Article 11 of the KVKK. In the defence received from the data controller within the framework of the investigation, it was claimed that the data subject did not intend to use its "right of access to information" regulated under the law, but only intended to obtain evidence for themselves, in order to obtain severance, reputation indemnity and other labour receivables.

In this regard, the Board did not take into account the claims of the data controller. Instead, it is stated that the data subject has the right to access their personal data within the scope of Article 11 of KVKK. Consequently, the Board decided to instruct the data controller to provide the requested documents to the data subject. This determination of the Board is of importance considering that the Board did not make an evaluation regarding the intent of the data subject but instead it broadly interpreted the right to access personal data.

Accordingly, the following question may easily spring to mind: Can the fact that a data subject

requests from the data controller his/her personal data for their own personal means, such as providing evidence, be interpreted to be contrary to the essence of the data protection legislation? Indeed, KVKK aims to prevent the unlimited and indiscriminate collection of personal data, making it accessible to unauthorized persons, disclosure or violation of personal rights as a result of misuse or abuse[4]. Although the ratio legis of KVKK in essence can be deemed as providing protection to individuals rather than limitless access to every personal data which has been processed data controller, both the approach of the Constitutional Court and the Board may be deemed widening this scope to a certain extent.

Moreover, it is possible to see that the approach of the authorities may vary in different jurisdictions. In a decision of a German District Court[5], it was ruled that the data controller had acted lawfully when it did not provide the recordings requested by the data subject. In this case, the surveillance recordings were only kept for forty-eight hours, and subsequently deleted. The data subject claimed that his/her right to access information ensured under Article 15 of the General Data Protection Regulation was violated. In this regard, the German District Court stated that the data subject's interest in acquiring those recordings were very limited and in return it would be considerably difficult for the data controller to provide the recordings. Accordingly, the German District Court made an analysis regarding the intent of the data subject and decided that he/she did not have sufficient benefit in acquiring the recordings.

In a decision of the Federal Labour Court of Germany (“**Federal Labour Court**”)[6] with regards to work related e-mails it was ruled that the request needed to be specific, and it could not comprise all the e-mails which are subject to processing. This approach was adopted by the Federal Labour Court as the system was prone to abuse of the employees quitting work. Accordingly, the intention behind the request of the data subject had played a significant role in the determination of the authority.

Conclusion

The decision of the Constitutional Court illustrates that the courts of first instance and the courts of appeal should ensure that the applicants rights to an effective remedy is provided in the practical sense as well as the theoretical sense. In order to do so, based on the facts of the case the courts should carefully interpret the issues at hand. This necessitates an in depth and expansive analysis of the arguments of the applicant, the respondent and the relevant legislation. By doing so, the applicants' and the respondents' rights and interests can be protected as it is required, and unwanted results can be avoided.

Moreover, it stands out that both the Constitutional Court and the Board adopt a data subject friendly approach when it comes to interpreting the level of access which needs to be granted by the data controller. Considering the rapid developments in this area we believe that the decision of the Constitutional Court can hold some light.

Previously published by Lexology on January 25, 2023

[1] Constitutional Court's decision dated 28.06.2022 and numbered 2018/6161, published in the Official Gazette dated 20.12.2022 and numbered 32049.

[2] Turkish Constitutional Court's Decision dated 30.05.2019 and numbered 2016/22418, para. 47.

[3] The Personal Data Protection Board's Decision dated 28.05.2020 and numbered 2020/435.

[4] Implementation Guidelines on the Personal Data Protection Law, page 36.

[5] AG Pankow, 4 C 199/21, 28.03.2022.

[6] Labour Court of Wiesbaden, 93 C 3382/20, 31.05.2021.