THE Fine PRINT

Gökçe

November 2022

108

CRITICAL DECISION FROM THE CONSTITUTIONAL COURT: INSPECTION OF EMPLOYEE'S TELEPHONE CORRESPONDENCE BY THE EMPLOYER

Digital Services Act Entered into Force

TRABIS Decisions for Domain Name Disputes

Latest Legal News

BRSA's Draft Identity Verification Circular has been Published

Striking Results: Digital Banking Statistics are Published

NFT Recognition in Trademark Law

THE Fine PRINT
Gökçe
November 2022
108

Critical Decision from the Constitutional Court: Inspection of Employee's Telephone Correspondence by the Employer

A crucial decision of the Constitutional Court **(AYM)** was published in the Official Gazette dated 15 November 2022. The incident in the decision is about the applicant employee's correspondence with a colleague using the mobile phone provided by the employer and the termination of the employee's employment contract as a result of these correspondences.

In the aforementioned incident, it was determined that the content of the messages on the mobile phone which was returned by an employee who quit the job, contained some humiliating statements about the company employees, and the employee's employment contract was terminated due to the contents of these messages.

The applicant claimed that the employment contract was terminated unjustly, the correspondences that constituted the basis for the termination were not included in the termination notice and that these correspondences did not take place. The applicant alternatively claimed that if the contrary was accepted, the relevant messages were in any case obtained unlawfully.

Consistent with its previous precedent, AYM has listed the following criteria which courts shall consider within the scope of the positive obligations of the state in disputes regarding the inspection of communication devices by the employer:

1. The employer must have a just and legitimate justification for inspecting the employee's communication flow and communication content. However, a distinction shall be made between the examination of ‘’the flow of the communication’’ and “the content of the communication’’, and more serious justifications shall be required for the inspection of the content of the communication.

2. The employer shall inform its employees in advance of suitable methods of the interventions and restrictions foreseen, in the inspection of communication, and such data processing must be carried out in a transparent manner.

3. The intervention regarding the personal data of the employee must be appropriate, proportionate and related to fulfillment of the employer's legitimate purpose.

4. The intervention must be mandatory, in other words, it shall not be possible to achieve the same purpose with a method that interferes less with personal data.

5. A balance must be ensured in terms of the benefit that the intervention brings to the employer and the burden it brings to the employee, and the balance of conflicting interests and rights must be observed in all circumstances.

For further information please contact us at info@gokce.av.tr

Within the context of these principles, AYM stated that it is necessary to examine whether the employer's document titled "Communication Tools Policy" contains sufficient and transparent regulations regarding the criteria. AYM also stated that, employees must be informed about the issues regarding personal data; and emphasized that in this way the employees must be made aware of the data processing to take place.

In light of this information, AYM concluded that the employer's seizure of the message contents that constituted the basis for the termination did not constitute an investigation limited to and compatible with the stated purpose. Additionally, considering that "messaging programs can also be used personally," the seizure of the relevant messages was contrary to the applicant's reasonable expectation of privacy of private life and communication, and it was decided that the right to respect for private life and freedom of communication right were violated.
In accordance with its previous precedent, AYM highlighted the issues that need to be taken into account while assessing the proportionality of the intervention by employers in disputes brought before AYM within the scope of communication tool inspection. In this context, and in line with its previous precedent, AYM reemphasized the obligation to inform the employee and the need to evaluate the proportionality of the intervention with the legitimate purpose.

Considering its previous decisions, AYM has been making parallel decisions for a long time regarding the employer's authority to inspect the corporate e-mail account assigned to the employee. In this context, one of the fundamental conditions pursued by AYM is fully and clearly informing employees beforehand about the conditions of use and inspection of communication tools. Moreover, as touched upon in the relevant decision, AYM emphasizes that even if the e-mail account is a corporate account, the inspection must be with regard to the legitimate interest of the employer.

Conclusion

In the relevant case as well as in prior similar decisions, AYM evaluates the employer's control of communication tools and content in light of specific criteria. According to these criteria, which are now considered to be well-established precedents, the employer's inspection of communication, even if it holds the right to manage, will not be recognized as valid unless the criteria regarding the "obligation to inform," "proportionality," and "fitness for purpose" are met. As a result, employers must surely check that these criteria are fully and completely met when monitoring the personal data of their employees and the access channels they use.

You can reach the full text of the decision here *(Only available in Turkish)*.

Digital Services Act Entered into Force

Digital Services Act **(DSA)**, the European Union's **(EU)** new regulation focusing on illegal content, transparent advertising, and disinformation aiming to modernise the E-Commerce Directive, entered into force on the 16 November 2022. DSA will be applicable for all hosting services, marketplaces and online platforms regardless of their place of establishment as long as they offer services in the EU.

DSA, which is regarded as the first regulation of the EU regarding platform governance which prioritizes the fundamental rights of people, imposes new obligations on relevant actors in order to ensure a safe and secure online environment. We present below some of the essential changes brought forth by DSA:

- DSA imposes new mechanisms to counter illegal content online, including illegal goods and services.
- DSA imposes new rules to monitor sellers and products on online marketplaces, including a new obligation imposed on online marketplaces to randomly check against existing databases whether products or services on their sites are compliant.
- DSA imposes effective safeguards for users, including the possibility to challenge platforms' content moderation decisions when their content gets removed or restricted.
- DSA implements transparency measures for online platforms, including providing better information on terms and conditions, as well as transparency on the algorithms used for recommending content or products to users.
- DSA obliges very large online platforms **(VLOP)** and search engines **(VLOSE)** to prevent abuse of their systems by risk-based actions, including independent audits of their risk management measures.
- DSA imposes bans on targeted advertising on online platforms by profiling children or based on special categories of personal data.
- DSA imposes a ban on using ‘dark patterns' on the interface of online platforms.
- DSA grants users new rights, including a right to complain to the platform, seek out-of-court settlements, complain to their national authority in their own language, or seek compensation for breaches of the rules.
- DSA envisions that the European Commission **(Commission)** will be the primary regulator for VLOPs and VLOSEs, while other platforms will be under the supervision of the Member States where they are established.

Online platforms will have until 17 February 2023 to report the number of active end users on their websites. Platforms with more than 45 million monthly active users will be designated by the Commission as a VLOP or a VLOSE. Following such designation, the platform in question will have 4 months to comply with the obligations under the DSA. DSA will be fully applicable for all actors by 17 February 2024.

In summary, DSA brings significant changes regarding consumer protection, tighter regulation of online platforms and a more uniform legal framework across the EU. Time will tell what the sectoral effects of these changes will be in Europe and Turkey.

You can reach the full text of the act here.

For further information please contact us at info@gokce.av.tr

THE Fine PRINT
Gökçe
November 2022
108

TRABIS Decisions for Domain Name Disputes

In accordance with The Internet Domain Names Regulation **(Regulation)**, the Dispute Resolution Service Providers **(DRSPs)**, which were envisaged to be established for the resolution of domain name disputes, have begun to operate with the ".tr Network Information System" **(TRABIS)** coming into operation. To explain how this mechanism in Turkey works, we find it appropriate to provide a brief comparison with the Uniform Domain Name Dispute Resolution Policy **(UDRP)**, which has an international structure.

- Pursuant to Article 25 of Regulation, if the criteria of **(i)** similarity, **(ii)** legal right or connection and **(iii)** bad faith are met, the complainant can request the suspension or transfer of the domain name. These three criteria are the same as the three criteria under the UDRP.

- There are two DRSPs in Turkey approved by ICTA; Information Technologies and Internet Security Association **(BTIDER)** and TOBB UYUM Mediation and Dispute Resolution Center **(TOBBUYUM)**. The UDPR regime also has six different such mechanisms, including the World Intellectual Property Organization **(WIPO)**.

- It is deemed appropriate, by Regulation, to resolve disputes regarding domain names through mechanisms operated by DRSPs. The arbitrators within the scope of the DRSPs have the authority to decide on the cancellation of domain names, their transfer to the complainant, or the rejection of the complainant's request, taking into account the relevant legislation. Decisions that can be taken under the UDPR system are of the same type.
- As a point where the two systems diverge, DRSP arbitrators are obliged to apply the rules stipulated by the law. The rules applied by the arbitrators in the UDRP system are the rules created by the establishment of the UDRP system by the Internet Corporation for Assigned Numbers and Names, a private sector non-profit organization. Also, if the dispute resolution mechanisms directed by the UDRP have their own rules, the arbitrators apply these rules as well.

Lastly, to comment on recent decisions, based on the arguments put forward by the complainant and the respondent parties, in an application made to TOBBUYUM, a decision to transfer the domain name to the complainant was made; because, the criteria of similarity, legal right or connection and bad faith were met. In one of the decisions of BTIDER, although it was concluded that the respondent registered the domain name in bad faith, the complainant's application was rejected due to a lack of similarity and lack of legal right or connection.

The status of the applications and the decisions made are made available on the websites of both DRSPs in a transparent manner. You can find the recent decisions here and here. *(Only available in Turkish)*

For further information please contact us at info@gokce.av.tr

BRSA's Draft Identity Verification Circular has been Published

Draft Circular No. 2022/2 **(Circular)** has been published by the Banking Regulation and Supervision Agency **(BRSA)** regarding additional explanations on the criteria to be met for identity verification and transaction security in electronic banking services and the establishment of contractual relations in the electronic environment. Circular includes clarifications that may help with any uncertainties relating to the implementation of certain provisions of the Regulation on Information Systems and Electronic Banking Services of Banks **(ISEBSB)**, Regulation on Remote Identification Methods for Use by Banks and the Establishment of Contractual Relationships in the Electronic Environment **(RIMBCEE)** and the Regulation on Operational Principles of Digital Banks and Service Model Banking **(DBR)**.

We have summarized the issues in the Circular that are not currently regulated in the law:

1. **Use of customer-specific encryption secret key and transaction signing:** Circular sets forth that according to ISEBSB; the "element known to the customer" that will be used in identity and transaction verification processes and will be used to activate the encryption secret key that will be assigned to the customer by the bank, like PIN, is to be verified online at the bank instead of locally on the device where the mobile application is installed. Additionally, it is emphasized once more that except for the following instances, namely the initial installation, activation, re-activation or unusability of the mobile banking application, no OTP or verification code is to be sent via SMS for login or verification of any transaction after the login, to customers who have activated the mobile banking application by installing it.

2. **Performing the transaction signing/approval according to the information submitted to the customer approval:** Circular emphasizes that measures should be established by banks to prevent the use of the customer's encryption secret key by unauthorized persons and that it should be ensured that the content signed by the customer is actually the content that the customer sees and approves. Within this context, it imposes an obligation upon the banks to create a Software Development Kit **(SDK)** to be used for transaction signing and a Security Server **(SS)** configured to communicate directly with this SDK over a secure separate channel, and it contains technical obligations relating to transaction signing processes to be executed through SDK and SS.

3. **Ensuring that the interface provider's interface complies with verification and transaction security obligations:** It is emphasized that the internet/mobile interface provided by interface providers to service banks pursuant to DBR should comply with the provisions of BSEBY and Circular. It is also stated that, in the mobile application interface, the SDK of the service bank should be embedded and the transaction signing flows should be executed over the abovementioned SS and SDK.

4. **Permit obligation:** Organizations that sell products or provide external services to be used in verification and transaction signing to banks, other institutions under the supervision and control of the BRSA, and interface providers, will be obliged to obtain a permit from the BRSA for these activities in accordance with the Circular.

For further information please contact us at info@gokce.av.tr

5. Independent Audit: In the Circular, it is emphasized that the compliance of the products developed internally or purchased by the banks, with the Circular, must be handled within the scope of the information systems audit to be carried out in accordance with the Regulation on the Independent Audit of Information Systems and Business Processes.

As it can be seen, Circular, if it comes into force in its current form, will impose important obligations on banks, other institutions under the control of the BRSA, and institutions providing identity verification/transaction services for them. In this context, all the said actors must follow the process and take the necessary actions to ensure compliance following the finalization of the Circular.

You can reach the full text of Circular here *(only available in Turkish)*.

Striking Results: Digital Banking Statistics are Published

Digital, Internet and Mobile Banking Statistics published by the Turkish Banks Association consist of data from banks that provide internet banking and mobile banking services. These statistics reveal the level of digitalization reached within this sector.

According to these data, the number of active digital banking customers in Turkey reached 91 million as of September 2022. Compared to 2021, this number has increased by 17 million 139 thousand people. While 78 million 294 thousand people are made up of customers who only perform mobile banking transactions, the number of customers who only perform internet banking transactions is 2 million 845 people. The number of customers making transactions in both ways is 9 million 440 thousand people. In other words, within the scope of these statistics, the majority of the 91 million active customers who benefit from digital banking services are those who make transactions solely through mobile banking.

Internet banking statistics: Between July 2022 and September 2022, the number of active customers who logged into internet banking individually was 10 million 787 thousand, while the number of active corporate customers registered to the system and logged in at least once was 5 million 720 thousand. Again, for July-September 2022, the total amount of transactions made through internet banking reached 5 trillion TL, while the number of transactions made was 127 million.

Mobile banking statistics: The number of mobile banking customers increased by 17 million 79 thousand people compared to 2021. In the period stated above, the number of financial transactions via mobile banking was 1 billion 609 million, amounting to 8 trillion 410 billion TL in sum.

As it is clear from the statistics above, the banking sector is becoming increasingly digitized. When we look at the number of users and transactions, we see a meaningful transition from traditional channels to digital channels. It should not be forgotten that especially in 2022, our law has been trying to catch up with these developments, that we have encountered many legal regulations in areas such as remote customer acquisition, service banking, open banking, and that we expect regulations regulating the digitalization of banking and finance from different angles in the near future.

You can reach the full text of the report here *(Only available in Turkish).*

NFT Recognition in Trademark Law

The International Classification of Goods and Services for the Purposes of the Registration of Marks **(Nice Classification)** 12th Edition will be published on the first of January 2023. Nice classification is a tool employed by the European Union to classify goods and services for the purpose of trademark applications. Out of 45 classes, classes 1 to 34 are assigned to goods and the rest to services.

There is an exciting development for the technology sector in the new edition.

European Union Intellectual Property Office' stated that the new edition of the Nice Classification, will include the definition of *"downloadable digital files verified by NFTs"*. In this regard, this development will clarify which class and sub-categories can be used in the Nice Classification for trademark registrations to be carried out for NFTs in the upcoming year.

THE Fine PRINT
Gökçe
November 2022
108

Answers. Not theories.

Gokce Attorney Partnership

Editors:

Prof. Dr. Ali Paslı
ali.pasli@gokce.av.tr

Dr. Mehmet Bedii Kaya
bedii.kaya@gokce.av.tr

Elif Aksöz
elif.aksoz@gokce.av.tr

Yağmur Yollu
yagmur.yollu@gokce.av.tr

About our firm

Gokce Attorney Partnership is an Istanbul-based law firm offering legal services across a broad range of practice areas including mergers and acquisitions, joint ventures, private equity and venture capital transactions, banking and finance, capital markets, insurance, technology, media, telecoms and internet, e-commerce, data protection, intellectual property, regulatory, debt recovery, real property, and commercial litigation. Please visit our web site at www.gokce.av.tr for further information on our legal staff and expertise.

Please contact us at
info@gokce.av.tr
0 212 352 88 33