ÇAMURŞEN V. TURKEY: STORAGE OF INTERNET TRAFFIC DATA AND SYSTEMATIC VIOLATIONS OF RIGHTS

Dr Ufuk YEŞİL

JUSTICE SQUARE

ABOUT US

Justice Square is a non-governmental organization established in the Netherlands with the aim of raising awareness about fundamental human rights and ongoing rights violations, and to fight in this field.

www.justicesquare.org

PREFACE

As a result of advancements in information technologies, it has become possible to collect a large amount of data that could not be collected through traditional methods, many data that were previously kept unrelated to each other can be brought together centrally, and the capacity to generate new data from data by analysing the data with advanced technological means such as data matching and data mining has increased, factors such as the ease of access to and transfer of data, the more widespread and significant risks created by private sector elements as a result of personal data becoming a valuable asset, and the increase in the activities of terrorist and criminal organisations to obtain personal data make it necessary to protect personal data at the highest level today.

Although it is obligatory to protect personal data at the highest level for the reasons stated above, this right is not absolute and unlimited, and may be restricted by law under certain conditions in accordance with Articles 13 and 20 of the Constitution, provided that it is not contrary to the requirements of the democratic social order and the principle of proportionality. In accordance with the mandatory provision of the Constitution, many regulations have been made on the subject. Some of these regulations are related to the storage and destruction of internet traffic data and HTS records, which are personal data, and laws and regulations include the storage and destruction procedures and control mechanisms of these data and records.

However, despite all this, the Information and Communication Technologies Authority (ICTA), the regulatory and supervisory authority for the information technology sector, has been requesting and retaining Internet traffic data and HTS records from operators for years, and continues to do so, despite the fact that it has no authority to do so and there are no court rulings on the matter. Upon the request of the courts for the records whose retention period has expired, these records have been sent by the ICTA and people have been penalised with this evidence that has become unlawful.

In this study, the procedure for the retention of internet data and HTS records and the evaluation of Ertan Erçıktı (3) judgement of the Constitutional Court and Çamurşen v. Turkey judgement of the ECtHR with reference to this judgement are included.

We hope that this study prepared by **Stichting Justice Square** will be useful.

19 December 2024 / Amsterdam

ÇAMURŞEN V. TURKEY: STORAGE OF INTERNET TRAFFIC DATA AND SYSTEMATIC VIOLATIONS OF RIGHTS

In General

Determination of the person, place and time information related to the internet connection is very important in the elucidation of offences committed in the electronic environment. In order to make this determination, the IP address allocated to individuals, the start and end time of the service provided over the internet, the type of service utilised, the amount of data transferred and subscriber information, in other words, internet *"traffic information"* is needed. Traffic information is a type of data that contains critical information that may disclose many details about an internet user's private life, personal preferences, political tendencies, health information and trade secrets. Therefore, it is possible to easily detect almost every detail about a person's life with traffic information and this traffic information also includes personal data. The concept of personal data includes all information relating to a person, provided that it is specific or identifiable. The right to protection of personal data aims to protect the rights and freedoms of the individual during the processing of personal data as a special form of the protection of human dignity and the right to freely develop one's personality. However, this right is not unlimited. The right to protection of personal data does not enable the data subject to have absolute and unlimited data control.

1. Legislation on the Storage and Destruction of Internet Traffic Information and HTS Records

Regulations on the subject are generally regulated by the Constitution of the Republic of Turkey, Electronic Communications Law No. 5809, Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through Such Publications, Law No. 6698 on the Protection of Personal Data, Turkish Criminal Code (TCK) No. 5237, Criminal Procedure Code (CPC No. 5271 and the regulations issued based on these laws.

a) Constitution of the Republic of Turkey

The Constitution guarantees the right to privacy and everyone has the right to demand respect for his/her private and family life. The privacy of private and family life shall be inviolable (Article 20/1 of the Constitution). In addition to this; it is also guaranteed by a separate provision for personal data. Accordingly, everyone has the right to demand the protection of personal data concerning him/her. This right 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. Personal data may only be processed in cases stipulated by law or with the explicit consent of the person (Constitution Art. 20/3).

The Constitution also provides a guarantee for evidence. According to this regulation, evidence obtained in violation of the law cannot be accepted as evidence (Article 38/6 of the Constitution).

When the above-mentioned two regulations are evaluated together; personal data can only be processed in cases stipulated by law or with the explicit consent of the person, and personal data processed unlawfully cannot be accepted as evidence.

b) Law No. 6698 on the Protection of Personal Data

The purpose of the Law is to protect the fundamental rights and freedoms of individuals, especially the right to privacy, in the processing of personal data and to regulate the obligations of natural and legal persons who process personal data and the procedures and principles to be followed (Art. 1 of the Law), and the scope of the Law is natural persons whose personal data are processed and natural and legal persons who process such data in whole or in part by automatic or non-automatic means (Art. 2 of the Law).

Personal data is defined as "*any information relating to an identified or identifiable natural person*" (Art. 3/1-d of the Law), special categories of personal data are defined as "*data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, and biometric and genetic data*" (Art. 6/1 of the Law), and processing of personal data is defined as "the collection, recording, storage, preservation, alteration, retention, retrieval and processing of personal data in whole or in part by automatic

or non-automatic means provided that it is part of any data recording system" (Art. 6/1 of the Law). 6/1), and processing of personal data is defined as "*any operation performed on personal data such as obtaining, recording, storing, preserving, modifying, reorganising, disclosing, transferring, taking over, making available, classifying or preventing the use of personal data by fully or partially automatic or non-automatic means provided that it is part of any data recording system*" (Art. 3/1-e of the Law).

When the purpose and scope of the Law and the definitions of personal data and processing of personal data in the Law are evaluated together, there is no hesitation that traffic information, which contains critical information such as with whom, how often, how much a person talks, which websites he/she visits and how often, and in this context, which may disclose many details about the user's private life, personal preferences, political tendencies, health information, trade secrets, is personal data.

Personal data cannot be processed without the explicit consent of the data subject (Art. 5/1 of the Law). As can be understood from the definition in the Law, recording, storing, preserving and transferring are also within the scope of "*processing*". Personal data may be processed as long as they fulfil the conditions specified in the law. These conditions are regulated in the law as follows (Art. 5/2 of the Law);

"a) Explicitly stipulated in the laws.

b) It is necessary for the protection of the life or physical integrity of the person who is unable to disclose his/her consent due to actual impossibility or whose consent is not legally valid.

c) Provided that it is directly related to the conclusion or performance of a contract, it is necessary to process personal data of the parties to the contract.

ç) It is mandatory for the data controller to fulfil its legal obligation.

d) It has been publicised by the person concerned.

e) Data processing is mandatory for the establishment, exercise or protection of a right.

f) Data processing is mandatory for the legitimate interests of the data controller, provided that it does not harm the fundamental rights and freedoms of the data subject

The expression "*explicitly*" in the condition of "*explicitly stipulated in the laws*" in the above-mentioned regulation is of great importance. As a matter of fact, it is not possible to process personal data on the basis of a law text that is not clearly stated.

The processed personal data is protected by a regulation in the law as follows; *"Although it has been processed in accordance with the provisions of this Law and other relevant laws,*

personal data shall be deleted, destroyed or anonymised by the data controller ex officio or upon the request of the data subject, in the event that the reasons requiring its processing disappear." (Art. 7/1 of the Law). According to this regulation, regardless of the law under which it was processed, the processed personal data must be deleted, destroyed or anonymised if the reasons requiring its processing disappear. The term "*anonymisation*" in the regulation is regulated in the law as "*making personal data impossible to be associated with an identified or identifiable natural person under any circumstances, even by matching with other data*" (Art. 3/1-b of the Law).

With the Regulation on Deletion, Destruction or Anonymisation of Personal Data[1] (*Deletion Regulation*) issued to determine the implementation principles of the Law, destruction is defined as "*deletion, destruction or anonymisation of personal data*" (Article 4/1-c of the Deletion Regulation) and periodic destruction is defined as "*the process of deletion, destruction or anonymisation to be carried out ex officio at recurring intervals specified in the personal data retention and destruction policy in the event that all of the conditions for processing personal data specified in the law disappear*" (Article 4/1-ğ of the Deletion Regulation).

According to the Deletion Regulation; deletion of personal data is the process of making personal data inaccessible and non-reusable in any way for the relevant users (Art. 10/1 of the Deletion Regulation). The data controller, who has prepared a personal data storage and destruction policy, deletes, destroys or anonymises personal data in the first periodic destruction process following the date on which the obligation to delete, destroy or anonymise personal data arises. This period cannot exceed 6 months in any case. The data controller, who is not obliged to prepare a personal data retention and destruction policy, shall delete, destroy or anonymise personal data within three months following the date on which the obligation to delete, destroy or anonymise personal data arises (Art. 11 of the Deletion Regulation). Those who violate this obligation shall be punished according to Article 138 of the Law No. 5237 (Art. 17/2 of the Law)

As a result; HTS records and internet traffic information, which are personal data, can only be recorded, stored, maintained and transferred for the reasons listed in the Law. Pursuant to the reason "*expressly stipulated in the law*", which is one of the reasons stated in the

1 Official Gazette dated 29/10/2017 and numbered 30224

said law, in order to record these personal data, it must be "expressly" stipulated in the law, as emphasised in the wording of the law. In this context, vague and non-specific expressions such as "such information", "any kind of information" in the laws do not fulfil the condition of "expressly stipulated. Therefore, it is not legally possible to process information in the nature of personal data within the scope of vague and indefinite expressions in the laws. Even personal data processed by explicitly stipulated in the law must be deleted by the data controller upon request or ex officio in any case, in the event that the reasons stipulated in the law disappear (such as the expiration of the retention period). In case of breach of this obligation, the person who commits the breach shall be punished according to Article 138 of the Law No. 5237.

c) Law No. 5809 on Electronic Communications and Regulations Issued Based on this Law

The purpose of the Law is to establish effective competition in the electronic communication sector through regulation and supervision, to protect consumer rights, to expand services throughout the country, to use resources effectively and efficiently, to encourage technological development and new investments in the field of communication infrastructure, networks and services, and to determine the procedures and principles regarding these. Therefore, Law No. 5809 protects the consumer first against the state and then against third parties in terms of ensuring that electronic communication systems comply with international norms, observing information security and communication confidentiality, protecting personal data and confidentiality, providing technical facilities for legal interception and intervention by national institutions authorised by law, and ensuring network security against unauthorised access.

The Law regulates the provision, protection and continuity of the communication service in accordance with the contract between the operator providing communication service and the user receiving the service.

Law No. 5809 on Electronic Communications (Art. 3/1-h), the Regulation on Authorisation of the Electronic Communications Sector[2] *(Authorisation Regulation*) and the

2 Official Gazette dated 28/5/2009 and numbered 27241.

Regulation on the Processing of Personal Data and Protection of Privacy in the Electronic Communications Sector[3] *(Protection of Privacy Regulation),* the term of electronic communication is defined as; "*transmission, sending and receiving of all kinds of signs, symbols, sounds, images and data that can be converted into electrical signals by means of cable, radio, optical, electrical, magnetic, electromagnetic, electrochemical, electromechanical and other transmission systems"* (Art. 4/1-g of the Authorisation Regulation). 4/1-g), GSM companies that provide electronic communication services to their users or provide an electronic communication network and operate its infrastructure, and companies so authorised *are referred to as "operators"* (Art. 3/1-z of the Law, Art. 4/1-o of the Authorisation Regulation, Art. 4/1-d) and real and legal persons who benefit from electronic communication services regardless of whether they have a subscription or not are defined as *"users"* (Art. 3/1-cc of the Law, Art. 4/1-s of the Authorisation Regulation, Art. 4/1-i of the Regulation on Protection of Privacy).

d) In terms of Retention Period and Deletion Obligation

The Law stipulates that the data shall be kept for a period to be determined by regulation, not less than one year and not more than two years from the date of communication with the data categories (Art. 51/10-c of the Law)

The definition of the term *'data categories'*, as mentioned in the law, is neither present in the law itself nor in the regulations issued under the aforementioned law. Data categories are regulated by the Regulation on the Processing of Personal Data and Protection of Privacy in the Electronic Communications Sector[4] , which has been repealed by the Regulation on the Protection of Privacy , and the definitions of issues such as the point of termination of the communication,[5] the type of communication[6] and the date, time and duration of the

---

3 Official Gazette dated 4/12/2020 and numbered 31324.

4 Official Gazette dated 24/7/2012 and numbered 28363

5 *1) In relation to fixed and mobile telephone services; the number or numbers where the communication is/will be terminated, the number or numbers to which the call is directed in case of additional services such as call forwarding and call transfer, the name and address of the subscribers.*
2) With regard to electronic mail and internet telephony, the user ID of the recipients of electronic mail, the user ID or telephone number of the recipients called by internet telephony, the name and address of the recipients of internet telephony or electronic mail.

6 *1) In relation to fixed and mobile telephone services; the electronic communication service used. 2) With regard to electronic mail and internet telephony; internet service used.*

communication[7] and the tracking and source of the communication[8] are included (Repealed Regulation on the Protection of Privacy Art. 13/1).

In the repealed Regulation on the Protection of Privacy, it is stated that these defined data categories can be kept for a maximum of one year from the date of the communication and the records of the calls that did not take place can be kept for three months (Art. 14/1 of the Repealed Regulation on the Protection of Privacy). **In the currently effective Privacy Protection Regulation, there is no definition of data categories, nor is there any regulation regarding the retention period.** Instead, in many parts of the regulation, it is sufficient to refer to the relevant articles of the Law No. 6698 on the Protection of Personal Data. In the last case, since the term *"data categories"* mentioned in the law is neither defined in the law nor in the regulations, and the Law No. 6698 is referred to in many places, we are of the opinion that the term *"data categories"* in Article 51/10-c of the Law No. 5809 should be understood as the distinction between personal data and special categories of personal data made in the Law No. 6698.

It was regulated in the first version of the Authorisation Regulation that *"Preservation of traffic information: The access provider or the operator providing telephone service is obliged to keep the traffic information regarding the number of users, identification information and call durations and the calls made over its infrastructure for a period of one year."*. After the amendment made on **11/6/2016**, however, it was regulated that *"Preservation of traffic information: The operator, who is an access provider or provides telephone service,* is *obliged to keep the IP address, port range, start and end time of the service provided, type of service used, amount of data transferred, number of users and subscriber identification information and traffic information of the calls made over its infrastructure for two years; user information is obliged to be kept for the statute of limitations specified in the relevant legislation."* (Art. 19/1-f of the Authorisation Regulation). As can be seen, the period stipulating the

---

7 *1) Regarding fixed and mobile telephone services; the start and end date and time of the communication.*
2) In relation to internet access, electronic mail and internet telephony; the date and time of logging in and logging out of internet access, the allocated dynamic or static internet protocol address, the port information in addition to the internet protocol address in networks using NAT, the subscriber/user ID, the date and time of logging in and logging out of electronic mail or internet telephony.

8 *1) In relation to fixed and mobile telephone services; the telephone number of the line on which the communication was initiated, including unrealised calls, the name and address of the subscriber, the date and date of allocation of the line to which subscriber.*
2) In relation to internet access, electronic mail and internet telephony; allocated user ID and/or telephone number, internet protocol address at the time of communication, name and address of the subscriber/user".

retention of traffic information for two years was one year prior to the amendment made on 11/06/2016, and until the amendment, access providers and operators were only obliged to retain "*the number of users, identity information, call durations and traffic information of the calls made through their infrastructure*". In other words, "*IP address, port range, start and end time of the service provided, type of service utilised and the amount of data transferred*" cannot be stored by access providers and operators providing telephone services.

The scope of *"traffic information of calls"* in the first version of the Regulation cannot include the matters added after the amendment. This is because neither the Law No. 5809 nor the regulation issued based on this law includes the definition of traffic information, and it is not possible to apply the issues added to the regulation for the period before the amendment to the detriment of the relevant parties.

Pursuant to Law No. 5809, the confidentiality of traffic data is essential, and it is prohibited to record, store, intercept and track such data except for the relevant legislation, judicial decisions and the consent of the data subjects (Art. 51/2). Traffic data are subject to the personal data processing procedure and may only be processed in a limited and measured manner in connection with the prescribed purpose and may be stored for the period required for the purpose for which they are processed, and this period may not exceed the period stipulated in the Regulations (Art. 51/1)

According to Law No. 5809, private information, including contact information, cannot be stored without permission and authorisation (Art. 56/1), and those who violate this obligation shall be punished with a judicial fine from one thousand days to five thousand days (Art. 63/10). Again, in subparagraph 1/a-2 of Article 13 of the Regulation on Administrative Sanctions of the Information and Communication Technologies Authority issued based on the Law No. 5809[9] under the title of *"Violations Regarding the Protection of Personal Data*", it is stipulated that if the operator fails to fulfil its obligation to keep or delete the processed and stored traffic data of its subscribers/users within the period stipulated in the relevant legislation, an administrative fine up to 3% of the net sales in the previous calendar year will be imposed.

9 Official Gazette dated 15/02/2014 and numbered 28914.

As a result; traffic information collected within the scope of this law is valid for 1 year for all data prior to 11/6/2016 (3 months in terms of unrealised calls) and 2 years for all data after this date. The legislation has made it obligatory for the data controller to delete the traffic information, which is in the nature of personal data, ex officio by the data controller, regardless of a request, after these periods have expired. In addition, it is clearly stated that sanctions will be imposed on those who neglect their storage and deletion obligations. Likewise, with the processing of data in excess of the period of time, an intervention in the private life of individuals without a legal basis is carried out by businesses, and the state has a positive obligation to prevent the violation of the rights of individuals in this way.

e) In terms of the Jurisdictions of the Information and Communication Technologies Authority

Although the Information and Communication Technologies Authority (ICTA) has many duties and powers, only HTS and internet traffic information, their storage and deletion, and the supervision obligation will be evaluated under this heading.

Article 6 of Law No. 5809 regulates the duties and powers of the ICTA. One of these is to receive all kinds of information and documents it may need from operators, public institutions and organisations, real persons and legal entities in relation to electronic communications, to keep the necessary records, and to transmit to the Ministry, upon request, those needed by the Ministry in determining the strategies and policies for the electronic communications sector (Art. 6/1-i of the Law).

Although the wording of the Law states *"to receive all kinds of information and documents it may need from public institutions and organisations and real and legal persons and to keep the necessary records"*, this is not what should be understood from the Law. As a matter of fact, in the preamble of this article; "*This law clarifies the authority of the Institution to examine complaints related to the electronic communications sector, and grants the authority to collect information and documents from relevant parties in order to properly carry out its functions of evaluating complaints and conducting inspections.*"[10] . As can be understood from the preamble, the Legislature has authorised the ICTA to collect information and documents and keep the necessary records,

10 https://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d23/c026/tbmm23026138ss0255.pdf

limited to "*the proper performance of its functions of evaluating complaints and supervision*". **The ICTA, in this respect, is not authorised to receive, request and record all kinds of information and documents in an unlimited manner.** The authority defined by this article is limited to investigating complaints and inspecting businesses, and it **does not have the duty and authority to record, store, store, archive and share traffic information, which is personal data.**

Another related jurisdiction is regulated with the 12th paragraph added to Article 60 of the Law on 15/8/2016 as follows; "*The Authority may receive and evaluate information, documents, data and records from the relevant places within the scope of its duties; may benefit from archives, electronic data processing centres and communication infrastructure, may contact with them and may take or have taken other necessary measures within this scope. The Authority shall work in cooperation with ministries, institutions and organisations in the performance of the duties specified in this paragraph. In this context, any request for information and documents requested by the Authority shall be fulfilled without delay by the relevant ministries, institutions and organisations. The procedures and principles regarding the request for information and documents according to this paragraph and the fulfilment of these requests and other issues shall be determined by the Presidency*."

The Constitutional Court, which examined the regulation in question;[11] stated that the above-mentioned rules should be taken into consideration as a whole in determining the meaning and scope of the rules, and that **after the duty of ensuring cyber security is given to the Authority in the aforementioned article,** the paragraph following the said provision states that the ICTA *"...within the scope of its duty..."* to obtain information, documents, data and records from the relevant places, to evaluate them, to make use of archives, electronic data processing centres and communication infrastructure, to establish contact with them and to take or have taken other necessary measures within this scope; these powers and opportunities granted to the ICTA **are limited to** the ICTA's **duty of ensuring cyber security, on** the other hand, in the continuation of the same article, it is stated that it is obligatory to fulfil the requests of the ICTA regarding its duties in the article *"...related to their duties under this Article..."* and

11 Constitutional Court's decision no. 24/7/2019 T., 2017/16 E., 2019/64 K.; https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2019/64?EsasNo=2017%2F16

the reference to the provision on the duty to ensure cyber security confirms the above-mentioned meaning and scope of the impugned rules (§ § 38-39).

As stated in the decision, the authority and duty of the ICTA is limited to the duty of ensuring cyber security. Within the scope of this article, the ICTA does not have the duty and authority to record, request from the relevant institutions or organisations, store and archive traffic information, which is personal data.

On the other hand, considering that traffic information, which is personal data, is protected by Law No. 6698 and that the processing of personal data according to this law **must be "*explicitly*" stipulated in the law, it is not possible to apply expressions such as "*all kinds of information and documents*" and "*such information and documents*" in the laws in the case of personal data.** Since Article 20 of the Constitution (examined above) guarantees that personal data can only be processed if stipulated by law, the ICTA cannot be given the authority and duty to collect personal data by regulation or any other regulatory act. For these reasons, the ICTA does not have the duty and authority to record, store, store, archive and transfer traffic information, which is personal data.

Although the ICTA does not have the duty and authorisation to record, store, store, archive and transfer traffic information in the nature of personal data, it has the duty and obligation to check whether personal data is properly stored, whether there are data breaches, and whether the personal data in question has been deleted in a timely manner in accordance with many legislative provisions.

According to Law No. 5809, ICTA has the duty and obligation to make necessary regulations and inspections regarding the rights of subscribers, users, consumers and end-users and the processing of personal information and the protection of confidentiality (Art. 6/1-c), to inspect and/or have inspections carried out by those operating in the electronic communication sector to comply with the legislation, to determine the procedures and principles related to the subject, to take the actions stipulated by the legislation in case of non-compliance and to impose sanctions (Art. 6/1-s). Article 14 of the Regulation on Protection of Confidentiality stipulates that the provisions of the Regulation on Administrative Sanctions of the Information and Communication Technologies Authority shall be applied in case of failure to fulfil the obligations set out in this regulation.

According to Law No. 5809, private information, including contact information, cannot be stored without permission and without authorisation (Art. 56/1) and those who violate this obligation shall be punished with a judicial fine from one thousand days to five thousand days (Art. 63/10). Again, in the Regulation on Administrative Sanctions of the Information and Communication Technologies Authority issued on the basis of Law No. 5809[12] **, it is stipulated that an administrative fine will be imposed if** the operator **fails to fulfil its obligation to retain or delete** the processed and stored traffic data of its subscribers/users **within the period stipulated** in the relevant legislation (**Art. 13/1-a-2).**

The duty and authority of the ICTA to supervise whether the traffic information, which is personal data, is properly stored and whether this data is deleted in a timely manner is not limited to the above-mentioned regulations. Similar audit duties and responsibilities are imposed on the ICTA in many legislative provisions.

f) Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through These Publications and Regulations Issued Based on This Law

The purpose of the Law is to regulate the obligations and responsibilities of content providers, hosting providers, access providers and collective use providers, and the principles and procedures for combating certain offences committed on the internet through content, hosting and access providers. In parallel with the developments in the world, this Law aims to enact a special law that will enable an effective and correct structuring in the fight against crimes committed by abusing the opportunities provided by electronic communication tools, including the internet, which are rapidly becoming widespread in our country[13] . Therefore, this Law is only for publications made on the internet and has the nature of a special law. For the procedures and principles regarding the implementation of the Law, the Regulation on the Procedures and Principles Regarding the Regulation of Publications on the Internet[14] (*Implementing Regulation*) has been issued.

12 Official Gazette dated 15/02/2014 and numbered 28914.
13 http://www5.tbmm.gov.tr/tutanaklar/TUTANAK/TBMM/d22/c156/tbmm22156099ss1397.pdf
14 Official Gazette dated 30.11.2007 and numbered 26716

While the concept of **access** is regulated in the Law as "*connecting to an internet environment and gaining the opportunity to use it*" (Art. 2/1-d of the Law), it is regulated in the Implementing Regulation as "*connecting to the internet environment through any means and gaining the opportunity to use it*" (Art. 3/1-e of the Implementing Regulation). The concept of **access provider** is regulated as "*any real or legal person who provides access to the internet environment to its users*" (Art. 2/1-e of the Law, 3/1-f of the Implementing Regulation). Pursuant to the aforementioned regulation, any real or legal person that provides access to the internet, such as GSM operators, is an access provider.

The concept of **traffic information** is defined in the Law and has been amended twice. When the Implementing Regulation is analysed, it is observed that there is no general definition of *"traffic information"*; instead, it is defined in three different categories as *"access provider traffic information"*, *"hosting provider traffic information"* and *"proxy server traffic information"*. It is seen that the definition made by the law has been expanded by the regulation and the issues that are not included in the definition have been included in this way.

In the first version of the Law, while the **traffic information was defined as;** "*values such as parties, time, duration, type of service used, amount of data transferred and connection points regarding all kinds of access on the internet environment*", Law 6527 published on 01/03/2014 defines the article related to[15] as *"IP address related to the parties, the start and end time of the service provided, the type of service used, the amount of data transferred and, if any, subscriber identification information*," and with the Law No. 7253[16] published on 31/7/2020, the phrase "*port information*," was added to come after the phrase "*IP address*," in the same article.

IP information and port information were deliberately not included in the concept of traffic information in the first version of the Law, but with two amendments made in 2014 and 2020, first IP information and then port information were included in the scope of traffic information. As a result, the concept of traffic information does not include IP address and port information before 01/3/2014 and port information between 01/3/2014 and 31/7/2020. The definition of traffic information regulated under the Law has been expanded by the Implementing Regulation by using another name and defined the **access provider traffic**

15 Official Gazette dated 26.12.2024 and numbered 28928
16 Official Gazette dated 31.7.2020 and numbered 31202

information as follows; "*Information such as the source IP address and port number making the request for the proxy server service used by the access provider in the Internet environment, the destination IP address and port number to which access is requested, protocol type, URL address, connection date and time, and disconnection date and time*" (Art. 3/1-g of the Implementing Regulation). The phrase *"such information"* in the said regulation was cancelled by the decision of the Council of State[17].

The Law imposes certain obligations on access providers, one of which is the obligation to store traffic information. According to the Law, the access provider is obliged to "*keep the traffic information specified in the regulation regarding the services it provides for a period of not less than six months and not more than two years, and to ensure the accuracy, integrity and confidentiality of this information*" (Art. 6/1-b of the Law). While this period was set as one year in the first version of the cited regulation (Art. 8/1-b of the Implementing Regulation), the entire relevant paragraph was cancelled by the Council of State Decision. **Currently, there is no regulation in the Implementing Regulation regarding the period of time for which the access provider will store traffic information.**

In the Law (Art. 6/3), the sanctions to be imposed in case the access provider fails to fulfil its retention obligations are regulated as follows: "*The President shall impose an administrative fine from ten thousand New Turkish Liras to fifty thousand New Turkish Liras on the access provider who fails to fulfil one of the obligations set forth in subparagraphs (b), (c), (ç) (...) of the first paragraph*." There is a similar provision in the Implementing Regulation (Art. 9/2). There is no doubt that this sanction will also be applied to the failure to store traffic data for longer than the retention period. As a matter of fact, while determining the retention period, the maximum period for which traffic data may be retained is also determined.

g) Turkish Penal Code No. 5237

Unlawful seizure of personal data, recording of personal data and failure to delete data that should be deleted are sanctioned under the Turkish Penal Code No. 5237. Article 135 of the Law titled *''Recording of personal data''* stipulates that anyone who unlawfully records

17 Decision of the Thirteenth Chamber of the Council of State dated 12/12/2019 and numbered E.:2013/239; K.:2019/4266

personal data shall be sentenced to imprisonment from one year to three years and the penalty to be imposed shall be increased by half if the personal data is related to the political, philosophical or religious views, racial origin, moral tendencies, sexual life, health status or trade union affiliations of the persons.

In Article 136 of the Law, titled *"Unlawful transfer or seizure of data"*, the person who unlawfully transfers, disseminates or seizes personal data to another person shall be sentenced to imprisonment from two years to four years, and in Article 138, titled *"Failure to destroy data"*. Article 138 entitled "Failure to destroy the data" stipulates that those who are obliged to destroy the data within the system despite the expiry of the periods determined by the law shall be sentenced to imprisonment from one year to two years if they fail to fulfil their duties, and that the penalty to be imposed shall be increased by one times if the subject of the offence is data that must be eliminated or destroyed according to the provisions of the Code of Criminal Procedure. As can be understood from the regulations in the TPC and especially Article 138, special arrangements have been made and the failure to destroy the data despite the expiration of the periods stipulated in the legislation has been sanctioned.

h) Law No. 5271 on Criminal Procedure and the Regulations issued based on this Law

Article 135 of the Code of Criminal Procedure No. 5271 regulates the detection, interception and recording of communications within the scope of an investigation and prosecution. The concept of "*interception of communication*" mentioned in this article is not defined in the law. This concept is defined in the Regulation on the Procedures and Principles Regarding the Detection, Interception, Evaluation and Recording of Communication via Telecommunication and the Establishment, Duties and Authorities of the Presidency of Telecommunication Communication[18] *(Communication Detection Regulation*) as *"the procedures for determining the search, call, location and identity information regarding the communication established by the communication tools with other communication tools without interfering with the content of the communication*" (Art. 3/1-i of the Communication Detection Regulation). According to this definition; HTS and internet traffic information are also within this scope.

18 Official Gazette dated 10/11/1005 and numbered 25989

Paragraph 6 of Article 135 of the Code of Criminal Procedure stipulates that "*the detection of telecommunication communications of the suspect and the defendant shall be made upon the decision of the judge at the investigation stage or the public prosecutor in cases where delay is inconvenient, and upon the decision of the court at the prosecution stage. The decision shall specify the type of offence charged, the identity of the person against whom the measure is to be applied, the type of means of communication, the telephone number or code enabling the determination of the communication connection and the duration of the measure. (Additional sentences: 24/11/2016-6763/26 Art.) The public prosecutor shall submit the decision to the judge for approval within twenty-four hours and the judge shall render his decision within twenty-four hours at the latest. In case the time limit expires or the judge decides otherwise, the records shall be destroyed immediately*."

Pursuant to the aforementioned regulation, the interception of communication can only be made upon the decision of a judge at the investigation stage, a public prosecutor in cases of delay, and a court decision at the prosecution stage.

The Regulation on the Detection of Communication, which was issued in order to regulate the procedures and principles regarding how the communication detection to be made within the scope of the Criminal Procedure Law will be carried out, has given a number of duties and powers to the Information and Communication Technologies and Communication Authority (ICTA) for the purpose of communication detection. Some of these authorisations are given below (Art. 17/1-a,b,c,d);

"*a) To carry out, from a single centre, the operations and procedures for the detection, interception, evaluation of signal information and recording of communications made through telecommunications pursuant to Article 7 of the Law No. 2559, Article 5 of the Law No. 2803 and Article 6 of the Law No. 2937,*

b) To carry out the works and procedures for the detection, interception, recording and evaluation of signal information of communication to be carried out within the scope of Article 135 of the Law No. 5271 from a single centre,

c) To examine whether the requests under subparagraphs (a) and (b) are in compliance with this Regulation and other relevant legislation and to apply to the competent authorities when necessary,

d) To forward the data and information obtained as a result of the transactions carried out pursuant to subparagraphs (a) and (b) to the Undersecretariat of the National Intelligence Organisation,

the General Directorate of Security and the General Command of the Gendarmerie, and upon request to the courts and public prosecutor's offices"

As can be understood from the texts of the Law and Regulation given above, it **is not possible for the ICTA to keep and store traffic information**, which is under the protection of Article 22 of the Constitution and which **is personal data.** It is noteworthy that the condition of being stipulated by law in Article 22 of the Constitution and the condition that personal data is *"**explicitly**"* stipulated by law in the Personal Data Protection Law No. 6698 are not met. Therefore, even if such an authorisation or duty was given in the regulation, it was not legally possible to implement it. This is because the Law does not grant such an authorisation or duty to the ICTA. Since the ICTA is the regulatory authority in the telecommunications sector, its authority in this matter is to ensure coordination between the above-mentioned authorities and to ensure the transmission of the requested information from a single source. In other words, **ICTA is not *an "executive"* but an *"intermediary"* institution.**

2. The Problem of Who Stores HTS Records and Internet Traffic Information

Although internet traffic information and HTS records can be kept for **1 year** until 11/6/2016 and for **2 years** thereafter in accordance with the Electronic Communications Law No. 5809 and the regulations issued on the basis of this Law, since they are related to electronic communications, it is observed that even after the expiry of this period, they are sent to the judicial authorities in accordance with the communication detection decisions under Article 135 of the Code of Criminal Procedure.

Despite the clear regulation in the Law and Regulations, the issue of who or by whom the traffic data, which are personal data, are stored for longer than the period required to be stored, why the relevant data are not deleted, whether those who violate their obligations are audited, and finally, by whom the personal data are sent to the judicial authorities comes to the fore. These issues are categorised and examined under separate headings below.

a) Evaluation of Who Stores the Data Whose Retention Period Has Expired

Pursuant to the provisions of the legislation, GSM and internet operators, known in various laws as "*operators*", "*access providers*", and "*data controllers*, are obliged to store the traffic information, which is in the nature of personal data, for the period specified in the legislation

and to delete it at the end of the period. This responsibility is imposed only on these data controllers by the legislation.

There is no doubt that the said obligation causes a certain burden for access providers, and that they will not want to keep the relevant personal data for more than the period due to problems such as system maintenance and storage space. As a matter of fact, it is not possible for these businesses to benefit from keeping the personal data for more than the period of time, since they cannot use the relevant data for purposes other than they are obliged in accordance with the legislation and no commercial benefit can be obtained with these data. As a matter of fact, all of the data controllers who have the title of data controller, declare that the personal data whose retention period has expired are deleted according to the disclosure text that they are obliged to publish and publish on their websites[19]

For an example, a related heavy penal court requested the traffic data of nine different numbers for a period exceeding one year directly from the GSM company instead of the Information Technologies Authority (ICTA), and the company, in its reply, reminded the 14/1. Article 14/1 of the Regulation on the Protection of Confidentiality; *"although your letter requested "whether the same IP number has been allocated to other persons, and if so, to send the identities and numbers of these persons for each defendant", since the data subject to your request regarding the detected IPs are stored in our company's systems for the last year, it was* not *possible to examine the dates requested to be queried*"[20] . In other words, **the data in question are stored by access providers during the retention period and deleted at the end of the retention period.**

If the access providers do not store the data in question for more than the time period, it is important to explain by whom these data are stored. This is because there is the fact that traffic information, which is personal data, is stored for more than the time limit and sent to the judicial authorities.

According to the provisions of the legislation, the decisions on the interception of communications issued within the scope of Article 135 of the Code of Criminal Procedure should be sent to the ICTA as an intermediary, and the ICTA should receive the relevant data

19 https://www.turktelekom.com.tr/destek/gizlilik-guvenlik-ve-kvkk/aydinlatma-metinleri

20 Turkcell GSM Company's response to the letter sent to Ankara 15th High Criminal Court (2017/9 esas) on 14/7/2017.

from the data controller as an intermediary and send them to the judicial authorities. In the concrete case, how the ICTA sends the traffic data, which the data controller says that it does not keep, to the judicial authorities is in need of explanation. As a matter of fact, according to the provisions of the legislation, **it is the obligation of the data controller to keep the relevant traffic information and the ICTA has no duty and authority in this regard.**

ICTA does not make any public statement on this matter. However, in the content of the defences made by the ICTA in related or similar cases, there are admissions by the ICTA that it keeps the data in question and that it compiles and shares this data with the judicial authorities when requested by the judicial authorities. In the annulment case filed against a Board Decision taken by the ICTA for the purpose of user profiling, The Council of State asked whether *"data processing" was* carried out on the personal data of the subscribers transferred to the ICTA pursuant to the Board decision subject to the lawsuit, and in the respondent administration's response to the interim decision dated 05/08/2021 and numbered 50218, it was stated that it was processed for the relevant query systems in order to ensure that it is kept ready for questioning in case any legal examination is requested by the competent institutions and organizations.

In another lawsuit filed regarding the storage of traffic information, which is personal data, beyond the time limit;[21] **ICTA claimed that it has the authority to store all kinds of data related to communications made through telecommunications without being limited to the period specified in the legislation and deemed it lawful to store traffic information!** [22]

In the Çamurşen application, the Government made the same point in its observations submitted to the ECtHR and stated the following (§ 170); "As can be understood from the purpose and systematic of the Law no. 5651 and the relevant Regulation as well as from the titles of Articles of the Law no. 565l, the Law no. 565l and the relevant Regulation apply solely to the hosting providers, access providers and content providers acting in accordance with the provisions of private law and governs their rights and obligations. Accordingly, the access providers have been placed under an obligation to retain the internet traffic data for a period

21 The case file is pending in the file numbered 2020/997 of the 13th Chamber of the Council of State.

22 Information and Communication Technologies Authority Legal Consultancy's letter dated 04/3/2020 and numbered 53393206-641.04-16101

of one year. Thus, it is clear that the relevant articles of the Law no. 5651 prescribe a time-limit not as regards the ICTA, which is a public instifution, but as regards access provides established and operating in accordance with the provisions of private law."[23]

As it is clear from these statements, ICTA stores, archives and sends traffic information, which is not clear how it obtained it, to the relevant authorities upon request. As if that is not enough, it claims that the personal data in question can be stored for an unlimited period of time both by businesses and by itself. This claim is evaluated separately below.

b) Evaluation of the Data Retention Authorisation of the ICTA

Since the data whose retention period has expired are not kept by the access provider companies and are somehow sent to the judicial authorities by the ICTA, these personal data are kept by the ICTA. However, when the legislation is examined, **there is no legal regulation stipulating that the ICTA may request traffic information, which is personal data, from access provider companies, store, archive and transfer this data.** As such, it is necessary to explain how these data are obtained by the ICTA. In practice, it is understood that the ICTA, as the regulatory authority, obtains the relevant data through Board Decisions labelled Confidential.

It is known that the ICTA occasionally sends letters to access providers, asking them to profile users, to obtain personal information of users and, more importantly, to continuously transfer the traffic information of users to the ICTA. These letters are labelled "***CONFIDENTIAL***" and are not shared with the public.

One of the letters sent by the ICTA to the relevant businesses is the letter of the Information and Communication Technologies Authority dated 15/12/2020 dated E-58415308-400-78040 and titled *"ISP Traffic Log Pattern*"[24] . In the annex of the relevant letter, there are *"ISP Traffic Pattern (13 pages)*" and *"Distribution List*".[25] When the letter labelled *"CONFIDENTIAL*"

23https://www.drgokhangunes.com/wp-content/uploads/2024/12/42883_19__6_cases_GVTs_OBS_.pdf

24 The relevant letter and its annexes can be accessed by entering "TVPEHQGS" in the document verification code and "78040" in the document number on the page at https://www.turkiye.gov.tr/btk-ebys and completing the security check in the security image. The relevant letter is also available at https://static.bianet.org/system/uploads/1/files/attachments/000/003/655/original/%C4%B0SS_Trafik_Log_Deseni.pdf?1658407569 at the time of publication of this article.

25 https://www.drgokhangunes.com/genel/iss-trafik-logu-ve-teknik-detay-dokumani/

is examined; businesses with more than a certain number of subscribers were requested to supply additional servers for the purpose of sending subscriber and session records, while others were requested to continue to use their installed servers and were also warned to comply with the attached technical document.

The statement in the letter that *"Businesses with less than 20,000 subscribers will continue to use the end servers already installed for the transmission of subscriber and session records for the transmission of traffic data"* is important. **It is understood** from this statement that personal **information was sent to the ICTA before this letter.** The relevant letter does not specify the legal regulation under which the ICTA, as a regulatory authority, requested this information. In the distribution list attached to the relevant letter, there are 281 enterprises.

Although the ICTA requested certain personal data to be sent to it continuously before the relevant letter, it was not possible to access the relevant letters and their contents since this request was made confidentially. However, in a recent article,[26] it is stated in another article dated 24/10/2018 before the above-mentioned letter dated 15/12/2020, which information the ICTA requested from the enterprises and what these letters and requests mean; [27]

"ICTA has taken the Board decision dated 24.10.2018 and numbered 2018/DK-BSD-314 and the Board decisions dated 16.04.2019 and numbered 2019/DK-BSD/109, dated 25.04.2019 and numbered 2019/DK-BSD/117, dated 08.05.2019 and numbered 2019/DK-BSD/131. These Board decisions include the transfer of "subscriber files" containing the details of the personal and commercial data of the subscribers of the operators providing ISP, fixed telephone service, infrastructure service, satellite communication service, mobile satellite service to the ICTA for the purpose of fulfilling the ICTA's preventive intelligence purposes within the scope of Law No. 5397 and judicial communication control duties within the scope of the Criminal Procedure Code. The subscriber technical detail document included in the board decision dated 24.20.2018 and numbered 2018/DK-BSD-314 contains provisions regarding the transfer of "subscriber files" containing subscriber personal and commercial data to the ICTA and subscription processes. For individual subscriptions, data such as name, surname, ID

26 Yorgancıoğlu, E., & Demircan, Y., T., (2023). Evaluation of internet traffic data collected by the Information and Communication Technologies Authority in the context of the right to protection of personal data. Istanbul Commerce University Journal of Social Sciences, 22(48), 1189- 1215. doi: 10.46928/iticusbe.1203350, Retrieved from: https://dergipark.org.tr/tr/pub/iticusbe/issue/81841/1203350

27 Elif Yorgancığlu, the author of the article, is the attorney of the plaintiff operator in the case file numbered 2022/314 E. of Ankara 3rd Administrative Court.

number, detailed address information, mother's maiden name, occupation, place and date of birth, serial number of professional ID are requested; for legal entities, data such as trade name, mersis number, tax identification number, title, ID number, name and surname, telephone number of the corporate authority are requested. Pursuant to the Board decision, some of the data will be transmitted to the ICTA as subscriber movement files, while the latest status of subscriptions will be sent as a monthly report. With this decision, the data of all users with telephone and internet subscriptions in Turkey have been transferred to the ICTA since 2019 without their knowledge, without their explicit consent and without any restrictions."

As can be understood from the article, with the decision taken in 2018, ICTA requests personal data, including traffic data, from businesses without any court decision and without any discrimination. This is particularly concerning in terms of traffic data.

When the 13-page technical document attached to the letter of the ICTA dated 15/12/2020 *on "ISP Traffic Log Pattern*" is examined;[28] the notification made by ICTA on the last page of the document is highly concerning: *"The period of sending traffic logs, which can be maximum 1 hour, should be notified to the Authority in writing*," *"If the data not transmitted in accordance with the pattern structure and restrictions in the above-mentioned areas are detected as a result of the examinations made by the ICTA ..... necessary penal actions will be initiated*." and "*Operators are obliged to send their files regularly and to ensure the accuracy and integrity of the data they send*". As can be understood from these statements, the ICTA **requests the traffic logs of all users from the operators at maximum one-hour intervals, states that it is obligatory to send traffic logs, and warns that penalties will be imposed on the operators who do not send traffic logs.** The data requested by the ICTA is explained in detail in the technical document. Among this information; the user's name-surname, IP number, private bridge (port), real IP, real bridge, real bridge start/end information, traffic start time, traffic duration, target IP address and port, the name of the application if the connection was established for the application, the name of the application if the connection was established for the application, the address of the page if the connection was made to a web page, such as personal data that violate the freedom of communication and privacy of the person's private life.

28 https://www.drgokhangunes.com/genel/iss-trafik-logu-ve-teknik-detay-dokumani/

A lawsuit was filed before the Ankara Administrative Court regarding the ICTA's letter on *"ISP Traffic Log Pattern"*[29] and the ICTA, which made a defence in the lawsuit, did not object to the existence of the transaction subject to the lawsuit. **The ICTA obtains personal data, and in some cases even special categories of personal data, from businesses in periods of one hour at most, under the threat of penal sanctions.** There is no information as to what kind of operations the ICTA performs with such data, whether it corrupts the data, with whom it shares the data, who has access to the data, and how it ensures the accuracy and integrity of the data. As a matter of fact, there is no legal legislation on this subject, nor is there any regulatory act issued by the administration on the subject. As such, the values protected by the Constitution and laws are violated by the practices of the ICTA.

Article 13 of the Constitution stipulates that fundamental rights and freedoms may be restricted without prejudice to their essence only for the reasons set out in the relevant articles of the Constitution and only by law, and that such restrictions may not be contrary to the letter and spirit of the Constitution, the requirements of the democratic social order and the secular Republic and the principle of proportionality. In the first paragraph of Article 20 of the Constitution, it is stated that everyone has the right to demand respect for his/her private life and that the privacy of private and family life shall be inviolable; in the last paragraph, it is guaranteed that everyone has the right to demand the protection of his/her personal data and that personal data shall be processed only in cases stipulated by law or in the presence of explicit consent

The freedom of communication provided for in Article 22 of the Constitution is the right to communicate with others without interruption or censorship. This freedom constitutes an aspect of *"private life"* which covers a much wider area. Therefore, the concept of "*confidentiality of communication"* is included within the concept of confidentiality of private life.

The protection of private life means, first and foremost, the protection of the confidentiality of private life and the prevention of being exposed. The right to have the events in one's private life known only by oneself or by those whom one wishes to know, is one of the individual's fundamental rights. Due to this nature, it has been included in declarations

29 It is pending in the file numbered 2022/314 of Ankara 3rd Administrative Court.

and conventions on human rights and has been protected against the state, society and other persons, with clearly defined exceptions in the legislation of all democratic countries.

As a result of advancements in information technologies, it has become possible to collect a large amount of data that could not be collected through traditional methods, many data that were previously kept unrelated to each other can be brought together centrally, and the capacity to generate new data from data by analysing the data with advanced technological means such as data matching and data mining has increased, factors such as the ease of access to and transfer of data, the more widespread and significant risks created by private sector elements as a result of personal data becoming a valuable asset, and the increase in the activities of terrorist and criminal organisations to obtain personal data make it necessary to protect personal data at the highest level today.

The concept of personal data refers to all information relating to a person, provided that it is specific or identifiable. In this context, not only information that reveals the identity of the individual such as name-surname, date of birth and place of birth, but also all data that directly or indirectly make the person identifiable such as telephone number, motor vehicle registration number, social security number, passport number, image and sound recordings, IP address, e-mail address, family information are within the scope of personal data. Accordingly, **there is no doubt that traffic information is personal data.**

The Constitutional Court has made many interpretations on the right of the ICTA to receive traffic information, which is personal data, from the operators and has cancelled the relevant articles of the laws on this subject. In one of these decisions, the Constitutional Court examined subparagraph (ı) of paragraph (1) of Article 6 of Law No. 5809, which stipulates that the Information and Communication Technologies Authority may obtain all kinds of information and documents it may need from operators, public institutions and organisations and real and legal persons in relation to electronic communications,[30] and made the following determination;

" *Considering that the jurisdiction granted to the Authority by the phrase requested to be cancelled to 'receive all kinds of information and documents it may need from operators, public institutions and*

30 Constitutional Court's decision dated 2/6/2011 and numbered 2008/115 and 2011/86

organisations and real and legal persons' can only be used in a limited manner in order for the Authority to properly fulfil its functions of evaluating complaints and auditing the electronic communications sector, which is within the scope of its establishment purpose and field of activity, and that the Authority is also responsible for protecting the confidentiality of personal information of subscribers, users, consumers and end users and the trade secrets of operators, ***it cannot be said that the phrase requested for cancellation of the jurisdiction of the Authority to obtain information and documents that violate the right to privacy or freedom of communication from real or legal persons****. Therefore, the rule requested for cancellation does not limit the right to privacy and freedom of communication*."

As can be seen, the ICTA is authorised to receive all kinds of information and documents it may need from public institutions and organisations, real persons and legal entities in relation to electronic communications, for the limited purpose of evaluating complaints about the electronic communications sector and performing its audit functions properly. The unlimited use of this limited authorisation to cover the personal data of all subscribers is not permitted as it would violate the right to privacy and freedom of communication.

Similarly; Article 3, paragraph 4 of the Law No. 5651 on the Regulation of Broadcasts on the Internet and Combating Crimes Committed through These Broadcasts states that *"Traffic information is obtained from the relevant operators by the Telecommunications Communication Presidency. In cases where a decision is made by a judge, it shall be given to the relevant authorities.*" was declared by the Constitutional Court as follows:[31] *"...The information to be provided under the name of traffic information is directly related to many fundamental rights such as confidentiality of communication, freedom to disseminate thought and expression, freedom of communication, protection of personal data, which are guaranteed by the Constitution, and the fact that this information can be obtained by TİB (now* ICTA*) at any time and in any way without any rules and limitations causes a direct violation of fundamental rights and freedoms. Despite the guarantees in Articles 13 and 20 of the Constitution, the rule subject to the lawsuit leaves individuals unprotected against the administration and other persons who have the authority to collect, store, process and change information, and the*

31 Constitutional Court's decision dated 2/10/2014 and numbered 2014/149 and 2014/151

purpose, justification, scope and limits of data collection are not included in the legal regulation. For the reasons explained, the impugned rule is contrary to Articles 2, 13 and 20 of the Constitution".

Likewise, the Constitutional Court has held that Article 5/5 of the Law No. 5651 Article 5/5 of the Law No. 5651; *"The hosting provider is obliged to deliver the information requested by the Authority to the Authority as requested and to take the measures notified by the Authority"* and the expression in Article 6/1-d stating that access providers are obliged *to "deliver the information requested by the Authority to the Authority as requested and to take the measures notified by the Authority"*; *"...In this framework, there is no certainty in the rules requested to be annulled regarding the conditions and grounds under which the information requested by the TİB (ICTA) will be submitted to the Presidency by content, hosting and access providers, or for how long the information provided will be kept by the TİB, the nature of the information requested, and the measures to be notified to content, hosting and access providers. In these respects, the rules are not specific and foreseeable. Despite the guarantee in the Constitution, they allow all kinds of personal data, information and documents belonging to individuals to be given to TİB unconditionally without being subject to sufficient limitations in terms of subject, purpose and scope, thus rendering individuals unprotected against the administration. Therefore, the rules to be cancelled limit the right to protection of personal data disproportionately and contradict Article 20 of the Constitution, as they are not specific and foreseeable. For the reasons explained, the rules are contrary to Articles 2, 13 and 20 of the Constitution"*.[32]

As it is seen, the legal regulations regarding the obtaining of traffic information of the subscriber by the administration from the operators have been cancelled by the Constitutional Court. Currently, there is no legal provision on this issue. **It is not possible to extend** the authority not granted by law, more precisely, **the general authority granted to the ICTA for the regulation of the sector, through secondary legislation, and to collect traffic information in the nature of personal data within this scope.**

In addition, subparagraph (d) of paragraph (2) of Article 12 of Law No. 5809 assigns the duty of protecting the personal data and confidentiality of subscribers to the operators, and the duty of making regulations and inspections regarding the processing and protection of the confidentiality of subscribers' personal data by the operators to the ICTA. Therefore, operators

32 Constitutional Court's decision no. 08/12/2015 T., 2014/87 E., 2015/112 K.

may request personal information and documents from subscribers and shall keep traffic information for the period stipulated in the law. The legislator has also assigned the duty to protect the personal information and documents of the subscribers to the operators. **There is no legal provision stipulating that operators may share the personal data of their subscribers, which they are obliged to protect, with the ICTA. The ICTA is obliged to impose obligations on the operators and to make regulations in order to take the necessary measures for the processing and protection of the confidentiality of the personal data held by the operators.**

Although the right to private life may be restricted by law under certain conditions and provided that it is not contrary to the requirements of the democratic social order and the principle of proportionality; the fact that the ICTA has unlimited access to the personal data of subscribers about whom there is no judicial process or request, and that **it can store and archive this data for an unlimited period of time without any assurance means interfering with the private lives of individuals, which is what happened in the concrete case.**

Pursuant to paragraph 3 of Article 20 of the Constitution, it is regulated that personal data can only be stored in cases stipulated by law, and pursuant to Article 13 of the Constitution, guaranteeing that fundamental rights and freedoms can only be restricted by law without prejudice to their essence, provided that they are limited to the reasons set out in the relevant articles of the Constitution, and pursuant to paragraphs 5/2-a and 6/3-b of the Personal Data Protection Law No. 6698, **it is not possible to store personal data that is not explicitly provided for in the Law. In this context, when the provisions of the legislation are examined, there is no "*explicit*" authorisation given by the law that personal data in the nature of personal data can be processed by the ICTA.**

As can be understood from the texts of the Law and the Regulation on the powers and responsibilities of the ICTA, **it is not possible for the ICTA to keep and store traffic information, which is under the protection of Article 22 of the Constitution and which is personal data.** This is because the ICTA is not authorised to do so, and **the ICTA's authority in this regard is to ensure coordination between the above-mentioned authorities and to ensure the transmission of the requested information from a single source, since it is the regulatory authority in the telecommunications sector.** In other words, **ICTA is not *an "executive"* but an *"intermediary"* institution.**

As can be understood from the explanations made, there is no provision in the Law and Regulations stipulating that the ICTA can request the information it demands from access providers in an unlimited and unconditional manner. It is not possible for the ICTA, which has no such authority, to directly request traffic information, which can only be accessed by a judge's decision pursuant to Article 22 of the Constitution, from access providers, and to store this information and send it to the relevant authorities after the retention period has expired. Nevertheless, the ICTA dictates that traffic information, which is personal data, be sent to it on a regular basis, arbitrarily stores the traffic information obtained within this scope for an unlimited period of time, filters the incoming data, creates meaningful tables and shares them.

c) Supervision Obligation of the Information and Communication Technologies Authority

Although the ICTA does not have the authority and duty to collect, store, retain and archive personal data, it is observed that the legislature and the executive make regulations on this issue from time to time. However, all of these legal regulations were found unconstitutional by the Constitutional Court, and the regulations made by regulations were cancelled by the Council of State. Although there is currently no provision stipulating that the ICTA can obtain personal data from access providers without a court decision, the ICTA requests personal data from businesses through its own board decisions and forced interpretations, threatens businesses with criminal sanctions in this regard, obtains the data and uses it for an unlimited period of time and without complying with any conditions.

In this regard, the responsibility of the ICTA is to supervise the enterprises in terms of whether they properly protect the personal data of the users, whether they transfer the relevant data to other places without consent, and to take the necessary measures. One of the relevant obligations of the ICTA is regulated in Article 6/3 of the Law No. 5651. In the regulation, reference is made to the article regarding the retention period and it is stated that in case of violation of this article, a penalty will be imposed on the enterprise. Likewise, in Article 6/1-c of the Law No. 5809, the ICTA has been assigned the duty of "*making the necessary regulations and inspections regarding the rights of subscribers, users, consumers and end-users and the protection of the processing and confidentiality of personal information*". Pursuant to the aforementioned regulations, the ICTA is required to inspect the enterprises and impose

sanctions on the enterprises due to the data that are not deleted due to the expiry date. **Nevertheless, the ICTA neglects this supervisory obligation and, worse, stores and processes the data that are not deleted despite the expiry date and shares the processed data with other institutions and organisations.**

In practice, the ICTA, far from fulfilling its supervisory duties and responsibilities, receives personal data from enterprises and processes such data itself, despite the fact that it is clearly contrary to the Constitution and laws, and the Constitutional Court and Council of State decisions clearly state that it has no such authority and duty. In this context, the ICTA, which requests the personal data in question, and the businesses that send the data are responsible for this unlawfulness. Although it is the duty of the ICTA to eliminate the unlawfulness in this matter and to impose sanctions when necessary, no action can be taken on the subject due to the fact that the unlawfulness arises directly from the ICTA itself and that it forces the enterprises to violate the law with the threat of sanctions. In short, the ICTA neglects its duty and obligation to supervise the retention of internet traffic information and HTS records, which are personal data, for more than the required period of time.

3. Evidential Quality of Expired Data

In order for a matter to be accepted as evidence in terms of criminal law, it must be obtained in accordance with the law. As a matter of fact, Article 38, paragraph 6 of the Constitution stipulates that evidence obtained in violation of the law cannot be accepted as evidence, Article 206, paragraph 2 of the Code of Criminal Procedure stipulates that evidence obtained in violation of the law shall be rejected, and Article 217, paragraph 2 of the Code of Criminal Procedure stipulates that the charged offence shall be proved by evidence obtained in accordance with the law.

Pursuant to the legislation, when a decision on the interception of communications is issued in accordance with the law, the relevant decision, together with a cover letter, must be sent by the judicial authorities to the ICTA, which is the intermediary institution, and the ICTA must examine the legality of the relevant letter in terms of form and contact the relevant authorities when necessary. The examination here is only a procedural examination and the ICTA does not have the right and authority to supervise court decisions. The duty of the ICTA is to examine whether the decision is attached to the letter, whether there is anything forgotten

in the content of the decision in terms of form (such as the beginning and end of the detection dates, information on the number and person to be detected), and to contact the relevant authority if it sees a deficiency. If there is no such deficiency, it will receive the data from the relevant enterprise and send it to the judicial authority.

However, in practice, contrary to the legislation, traffic information is collected from businesses before the court decides on the interception of communication. In fact, the process carried out by the ICTA *"detection of communication"*. According to the definition made in subparagraph i of Article 3 of the Regulation on the Procedures and Principles Regarding the Detection, Interception, Evaluation and Recording of Signal Information and the Establishment, Duties and Authorities of the Presidency of Telecommunication Communications, **the detection of communication** *refers to "the procedures for determining the call, being called, location information and identity information regarding the communication established by the communication tools with other communication tools without interfering with the content of the communication*". However, it is the obligation of businesses to record and process traffic data and store it for the legal period, and the ICTA is not authorised to do so by law.

The fact that the ICTA, as an administrative institution, receives the traffic data from the companies that hold the traffic data due to the legal obligation, should be evaluated within the scope of "*the procedures for the determination of search, call, location and identity information regarding the communication with other means of communication*". This is because, once the relevant traffic data is received by the ICTA, the communication is detected in the sense of criminal law. In this case, the traffic data becomes unlawful due to the detection of communication without a court order, and the traffic data obtained in this way cannot be used in judgements.

On the other hand, pursuant to paragraph 3 of Article 20 of the Constitution, personal data may only be processed in cases stipulated by law or with the explicit consent of the person. As explained in detail, there is no legal article stating that the relevant traffic information will be processed by the ICTA. The term *"**processing**"* mentioned herein is defined in the Law No. 6698 as "*any operation performed on personal data, such as the acquisition, recording, storage, retention, alteration, reorganisation, disclosure, transfer, acquisition, making available, classification or prevention of the use of personal data by fully or partially automatic means or by non-automatic means provided that it is part of any data recording system*" (Art. 3/1-e) and since the scope

of processing includes operations such as "*obtaining*", "*storing*", "*keeping*", "*preserving*", "*reorganising*", "*taking over*", there is no doubt that the said operation of the ICTA is also "*processing*". **Although the ICTA does not have the authority and duty to process these data without a court decision, it obtains and stores them from data controller enterprises, transforms them into meaningful tables, processes them, shares them with other institutions, and thus processes them unlawfully. It is not possible to use these unlawful data in the proceedings**

Furthermore, there is no regulation and assurance as to how the ICTA protects the traffic data unlawfully obtained by the ICTA, i.e. how their reliability is ensured. It is not possible for the ICTA, which is not authorised to collect, store and archive the data, to have assurances for the protection of the data. In the lawsuits filed against the ICTA, the ICTA **states that it is not subject to the obligations imposed by the law on the protection of personal data, and that it can store the data in question for as long as it wishes under the conditions it wishes without any limitation.** This eliminates the reliability of the traffic data in question. This is because, in response to the decisions of the judicial authorities regarding the interception of communications, the ICTA states that *"...it has been prepared on the basis of the records sent electronically to our institution by the relevant enterprises within the specified date range and presented in the annex*". From these statements, it is understood that the relevant data were created as a result of the *"preparation"* activity carried out by the ICTA on the records received from the relevant business and therefore are not original data. It is not possible to use data whose data integrity has been disrupted, in other words, data that is not raw, as evidence.

These explanations are only related to the illegalities related to the way the relevant data is obtained. Traffic data that are not deleted even though the retention period has expired are data that should not exist legally and even their existence is subject to criminal and legal sanctions. Such data loses its evidential quality with the expiry of the retention period.

4. Approach of the European Court of Human Rights

The European Court of Human Rights (ECtHR) examines applications concerning the retention and destruction of internet traffic data, HTS records or personal data under Article 8 of the European Convention on Human Rights (ECHR), namely the right to respect for private and family life, and has issued a number of judgements in this regard.

a) Rotaru v. Romania Grand Chamber Judgement

In Rotaru v. Romania, the applicant alleged that the Romanian Intelligence Service (RIT) kept and used a file containing personal information about him, some of which was false and defamatory. The ECtHR has stated that the risk of arbitrariness increases in cases where the secret power granted to the administration is used, that the uncontrolled power granted to the administration in relation to the surveillance of communications not being open to inspection is incompatible with the principle of the rule of law and that the scope of the power in question and how it will be used must be clearly demonstrated.[33] However, in the case in question; although national law permits the RIT to collect and record information concerning the applicant's private life and archive it in confidential files, there is no regulation restricting the exercise of this power, the type of information to be recorded, the categories of persons to whom the measure will be applied, the duration of the retention of the information obtained and the conditions under which this measure may be applied, as well as the absence of any safeguards and controls to prevent the arbitrary use of this power, and the lack of clarity regarding the use of the discretionary power , the Court ruled that the measure did not meet the requirement of "*conformity with the law"* and therefore the applicant's rights under Article 8 were violated. Article 8 rights of the applicant had been violated.[34]

b) Big Brother Watch and Others v. the United Kingdom

The ECtHR upheld the authorization granted to the UK's intelligence services by the Law on the Regulation of Intelligence Powers to carry out mass interception for intelligence purposes and to obtain communications data in bulk from internet service providers. This includes the search criteria used to obtain, filter, and extract the data, the lack of independent oversight mechanisms in the search and selection processes, as well as the absence of any real safeguards at the screening stage. This is despite the fact that the communication information to be selected for examination relates to individuals' private lives, and there is a lack of

33 ECtHR Judgment in Malone v. the United Kingdom, B. No: 8691/79, 02/8/1984.

34 ECtHR's Rotaru v. Romania Grand Chamber Judgment, B.No: 23841/95, 04/5/2000, § § 56-63.

foreseeable control by a court or independent administrative authority prior to access to the information, in violation of Article 8 of the ECHR. [35]

c) Benedik v Slovenia Judgement

Another case subject to the ECtHR judgement took place as follows; the Slovenian Constitution stipulates that, as a consequence of the confidentiality of communications, the communication and identity information (internet traffic information) of individuals can only be obtained with a court order, but the criminal procedure law stipulates that, within the scope of a judicial investigation, the police can request the internet traffic information of those concerned from internet service providers without a judge's order. A person whose traffic information was obtained by the police without a judge's order within the scope of an investigation and who was arrested on the basis of this information applied to the ECtHR and stated in his application that his traffic information was obtained without a court order, that he did not waive his right to privacy regarding his communication information and that this information should also be protected within the scope of the concept of private life, that he was not provided with sufficient assurance against the interference to his private life due to the uncertainty in domestic law, that the provisions of the Constitution should be applied in the case subject to his application, since the Constitution regulates that communication information can only be provided with a court order and that his right to private life was violated by not complying with these issues.

In its judgment on the application, the ECtHR stated that the provision of subscriber information on IP addresses is subject to a court order and cannot be obtained by a simple written request of the police, that the basis of the law authorising the police to obtain this information lacks formal clarity, that Article 8 does not provide adequate protection against arbitrary interference and that the interference with the applicant's right to respect for private life resulted in a violation of Article 8 of the Convention[36]

35 ECtHR Judgment in Big Brother Watch and Others v. the United Kingdom, B. No: 58170/13, 62322/14 and 24960/15, 13/9/2018, § § § 465-468.

36 Benedik v. Slovenia Judgment of the ECtHR, B.No: 62357/14, 24/04/2018, § 128 et seq.

d) Ekimdzhiev and Others v. Bulgaria

In Ekimdzhiev and Others v. Bulgaria, the ECtHR found a violation of the applicants' right to protection of private and family life, as Bulgarian law provided inadequate legal safeguards against arbitrariness and abuse in relation to covert surveillance, retention and access to communications data.[37]

According to the ECtHR, although the laws governing the retention of communications data and subsequent access to it by the authorities have been significantly improved since the Constitutional Court reviewed them following the CJEU's 2015 judgment in Digital Rights Ireland and Others, the laws, as applied in practice, still lack the minimum safeguards against arbitrariness and abuse required under Article 8 of the Convention in the following respects

(a) The authorisation procedure does not appear to be sufficient to ensure that communications data held by the competent authorities are only accessed "when necessary in a democratic society".

(b) **No clear time limits are set for the destruction of data accessed by the authorities during criminal proceedings.**

(c) **There are no publicly available rules on the storage, access, review, use, transmission and destruction of** communications **data** accessed by the authorities**.**

(d) The supervisory system, in its current organisation, does not appear to be sufficient to effectively control abuse.

(e) The current notification regulations are too narrow and

(f) There appears to be no effective remedy.

Consequently, these laws do not fully satisfy the requirement of *"the character of a law"* and do not bring the *"interference"* required by the Bulgarian system of retention and access to communications data within the scope of the *"necessary in a democratic society"* criterion. There has therefore been a violation of Article 8 of the Convention in this respect as well" (§§ 420-421).

37 ECtHR Judgment in Ekimdzhiev and Others v. Bulgaria, B. No: 70078/12, 11/04/2022.

e) Škoberne v Slovenia Judgement

In the case at hand, in an investigation into a bribery offence, the national court ordered the service providers to provide the applicant, a former judge, with communication records relating to the telephone used by him. The service providers only sent the court data relating to the **14-month** period for **which they were** legally **obliged to keep** such information, rather than the longer period requested by the court. The applicant was convicted on the basis of this information.[38]

There is no dispute that the retention of the applicant's communications data, which constituted an interference with his private life, had a legal basis in national law and was based on a court order (§ 130). However, the ECtHR stated that the systematic collection and retention of information concerning the private life of individuals by identifying the location, the persons contacted and the pattern of communication constituted a far-reaching and particularly serious interference with fundamental rights (§ 134).

According to the ECtHR, although the relevant law specifies the purposes for which contact details are held, there are no provisions outlining the scope and application of this measure. The absence of provisions or mechanisms to ensure that the measure is limited *to "what is necessary in a democratic society"* is incompatible with Article 8 of the ECHR and the **fact that the period of retention of the information was limited to the considerable period of 14 months does not change this conclusion** (§ 139).

According to the Court, where the retention of communications data is incompatible with Article 8, access to, subsequent processing and storage of such information by the competent authorities is incompatible with that Article (§ 144). The ECtHR held that the relevant provisions of the law, which formed the basis for the retention of the applicant's communications data, did not fulfill the requirement of 'legality' and failed to limit the interference with the applicant's Article 8 rights to what was 'necessary in a democratic society.' The Court also found that the retention, access to, and processing of the communications data violated Article 8. (§ 147).

38 ECtHR Judgment Škoberne v. Slovenia, B. No: 19920/20, 15/5/2024.

f) Borislav Tonchev v Bulgaria

In the case at hand, the data subject applicant started work as a prison guard at the General Directorate of the Penitentiary Institution in Bulgaria in July 2004 and was required to have a clean criminal record. However, the applicant received an administrative penalty for driving under the influence of alcohol between the time he applied for the job and his employment. In 2012, the applicant applied for another position at the Ministry of Justice, but his application was rejected and he was dismissed from his current job due to this penalty on his criminal record.[39]

The applicant filed a lawsuit stating that his dismissal from his profession was unlawful, stating that his criminal record was subject **to a five-year retention period** and should be deleted after the expiry of this period. However, his lawsuit was rejected and the higher court upheld this decision. The applicant then lodged a complaint with the Bulgarian data protection authority (CPDP), stating that the Ministry of Justice had processed his data unlawfully. The CPDP found the applicant to be in the right and imposed a fine for storing criminal record data for more than five years. However, this decision was later cancelled.

Following this decision, the applicant applied to the ECtHR, claiming that his data had been unlawfully processed. The Court found that the data were not sufficiently foreseeable due to the ambiguity of the regulations on data retention and the absence of a regulation on when the data should be deleted, in breach of Article 8(2) ECHR. The Bulgarian Ministry of Justice argued that the data should be kept indefinitely, while the CPDP argued that they should be deleted together with the registration cards. The ECtHR found the ambiguities in the regulations contrary to the principle of foreseeability (§ 130 et seq.)

g) Yalçınkaya v. Turkey

In the case at hand, the applicant complained that the National Intelligence Organisation (MIT) collected and used the data relating to the Bylock communication application, which was the basis for his sentence, without a court decision and in violation of the relevant legal

39 ECtHR Judgment Borislav Tonchev v. Bulgaria, B. No: 40519/15, 16/7/2024.

framework, and that the internet traffic data (CGNAT) was kept by the ICTA outside the legal time limit.[40]

The ECtHR addressed the following questions to the Government; in particular, having regard to the applicant's allegation that the data in question contained information which had been stored beyond the maximum period prescribed by law for their retention, were the data provided by the ICTA concerning the applicant's telephone and internet traffic records stored and disclosed in accordance with the relevant national law? What safeguards are there in the relevant law and practice against arbitrary interference and misuse?

Finding violations under Articles 6, 7 and 11 of the ECHR, the ECtHR stated that the essence of the applicant's complaint was that he was convicted on the basis of allegedly unlawfully obtained Bylock and internet traffic data rather than the interference with his private life due to an unlawful act (§ 371).

According to the ECtHR, the Article 8 aspect of the application was considered by the applicant himself to be a secondary issue. This is evident from the applicant's arguments before the national courts and the ECtHR regarding the fairness of his conviction on the basis of the evidence in question. Again, the private life issues relating to Bylock and internet traffic data were largely raised in relation to the use of this evidence in the criminal proceedings (§ 372).

The ECtHR, noting that the applicant's complaints under Article 8 of the Convention concerning his conviction on the basis of unlawful evidence had been examined under Article 6 § 1 of the Convention and that it had found a violation under that Article, held that it was not necessary to examine these complaints separately on admissibility and merits with regard to Article 8 of the Convention (§ 373).

5. Çamurşen v. Turkey

A recent ECHR judgment in relation to Turkey concerns the application of Çamurşen v. Turkey. The ECtHR found the application inadmissible with reference to the Constitutional Court's judgement in Ertan Erçıktı (3), i.e. **that domestic remedies had not been exhausted**. Due to the emphasis on the Constitutional Court's judgement and the rejection of the

40 ECtHR judgement Yüksel Yalçınkaya v. Turkey, 15669/20, 26/9/2023.

application on the same grounds, it is considered appropriate to first include the evaluations regarding the Constitutional Court's judgement.

a) Ertan Erçıktı (3) Decision of the Constitutional Court

In the case subject to the decision, the applicant filed a criminal complaint against the ICTA and three related companies for keeping internet traffic information for longer than the period specified in the legislation and sending this information to the relevant court. At the end of the investigation, the chief public prosecutor's office decided not to prosecute, stating that the investigation against the applicant started in 2014 and that the information was provided at various times in 2015, that although there is a one-year retention obligation for companies, there is no such time limit for the ICTA, and that there is no obligation or sanction for companies to delete or destroy the information. Upon the finalisation of this decision, the applicant made an individual application to the Constitutional Court and claimed that his rights to respect for private life, to request the protection of personal data and to a fair trial were violated as his complaint was rejected without a diligent investigation considering the importance of the matter and without sufficient justification.[41]

According to the applicant ICTA does not keep internet traffic information within its own organisation, it obtains it from access provider companies upon request during the investigation or prosecution process and sends it to the relevant authority, and according to the legislation, access provider companies can keep this information for a maximum of two years. He stated that the fact that ICTA sent the internet traffic information of the mobile phone number he used for the years 2014-2015 upon the request of the court on 4/7/2017 shows that companies established for commercial purposes continue to keep internet traffic information unlawfully even if the periods specified in the relevant legislation have passed.

The applicant stated that personal data can only be processed in cases stipulated by law or with the explicit consent of the person, that he did not consent to the storage of his personal data and that, according to the legislation, companies are not authorised to store personal data indefinitely. According to the applicant, the real problem is the continued storage of people's personal data by private companies and this application is not aimed at penalising third parties

41 Application No: 2018/14040, 30/6/2021. https://kararlarbilgibankasi.anayasa.gov.tr/BB/2018/14040

but at establishing the situation. Moreover, this serious problem cannot be solved by an action for damages.

The Constitutional Court emphasised that the applicant's aim was the determination of the violation of rights, the redress of personal damages and the punishment of the perpetrators and that the act subject to the complaint arose from the actions of the access provider companies and the ICTA in the nature of corporate activities. Likewise, the Court stated that unless an intentional or negligent act is determined in the criminal proceedings, the individual criminal liability of the employees of the institution and the company cannot be mentioned and that corporate liability cannot be subject to criminal proceedings.

According to the Constitutional Court, the personal damages claimed by the applicant cannot be redressed through criminal proceedings and administrative and civil courts are authorised to examine such claims and to determine unlawfulness or violation of rights. Where an unlawful act is found, moral damages may be awarded to compensate for personal injury. The compensation remedy may be based on both individual and corporate liability and the judge may award additional remedies and injunctions in addition to compensation. From the judgements it cited as examples, the Constitutional Court stated that similar claims were examined on the merits in both civil and administrative courts, that the parties were able to participate effectively in the proceedings and that the decisions of the courts of first instance were subject to judicial review.

The Constitutional Court concluded that the compensation proceedings under Article 58 of the Code of Obligations and Articles 11 and 12 of the Code of Administrative Procedure offer a reasonable chance of success and are more appropriate to the applicant's aim than the criminal proceedings. The Court also stated that the applicant did not have a concrete claim that the compensation remedy was ineffective and decided that the application was inadmissible due to non-exhaustion of remedies.

b) Çamurşen v. Turkey

The applicant, whose application was declared inadmissible by the Constitutional Court, filed a complaint under Article 8 of the ECHR on the grounds that the retention of internet traffic data beyond the prescribed legal period and the transmission of this data to the court of first instance for criminal proceedings through the ICTA violated his right to respect for private

life. The applicant also complained under Article 13 of the ECHR that he had been deprived of an effective domestic remedy[42]

The Court notes that, as interpreted and applied by the Constitutional Court, the most effective remedy for complaints such as the applicant's is the remedy of redress before the administrative and civil courts. The Court **further notes that,** as clarified by the Constitutional Court in Ertan Erçıktı (3), in **cases raising similar issues the administrative and civil courts comprehensively examine the merits of the claims raised by the parties who were able to participate effectively in the proceedings and that the decisions of the courts of first instance are subject to review by the higher courts.** The Court, emphasising the subsidiary nature of its task, considers that there is nothing to indicate that the scrutiny exercised by the national courts in connection with the aforementioned remedies would be in any way limited or manifestly doomed to failure. The Court thus sees no reason to doubt the effectiveness of the above-mentioned remedies or to conclude that they cannot offer the applicant any prospect of success (§ 24).

The Court therefore considers that the applicant cannot be regarded as having done all that could be expected of him in order to exhaust domestic remedies, since he did not avail himself of the remedies for redress before the administrative and civil courts set out in Article 12 of Law no 2577 and Article 58 of Law no 6098 (§ 26). However, the Court left open the option of examining the effectiveness of those remedies for the future (§ 27).

In conclusion, the Court, accepting the Government's objection, dismissed the complaint under Article 8 of the ECHR for non-exhaustion of domestic remedies under Article 35 §§ 1 and 4 of the Convention.

c) Evaluation of the Decision

Çamurşen v. Turkey is a group of applications and there are six other applicants in this group besides Çamurşen.[43] However, the ECtHR rejected Çamurşen's application separately and did not render a judgement on the other applications.

42 B. No: 42883/19, 12/11/2024

43 https://hudoc.echr.coe.int/eng?i=001-209418

In the other six cases, which the ECtHR grouped together with the Çamurşen application, the applicants first lodged a criminal complaint with the prosecutor's office and then applied to the Constitutional Court following the decision of non-prosecution (one of the applicants also exhausted administrative remedies). Unlike the Çamurşen application, the Constitutional Court found these six applications inadmissible not on the grounds of "**failure to exhaust domestic remedies**", **but** "**on the merits**", i.e. on **the grounds that there was no right violated**.

d) Regarding the Determination that the Compensation Procedure is Effective

According to the ECtHR, like the Constitutional Court, the applicant did not file a compensation claim before the administrative or civil courts when he should have done so and his application was found inadmissible because he did not exhaust this remedy. This is because, in the court decisions cited as examples in the Constitutional Court's judgment, similar allegations related to the subject matter of the application were examined in detail by both the civil and administrative courts, the parties were allowed to participate effectively in the proceedings with their claims and defences, and it was also observed that the decisions of the courts of first instance were subject to judicial review. In other words, there is an effectively functioning remedy before the civil and administrative courts in respect of the applicant's allegations.

But is this really the case? None of the three administrative court decisions and one civil court decision cited by the Constitutional Court awarded compensation and the cases were dismissed. Moreover, none of these judgements assessed that the internet traffic data, which formed the basis of the plaintiffs' complaint, was stored for longer than the retention period. The grounds for rejection of the lawsuit as a result of the application to the compensation remedy, which is stated to be effective and must be exhausted, are as follows; it is a legal obligation to keep the data of the communication made through telecommunication in order to fulfil these requests by the defendant administration if requested by the public prosecutor's offices and courts in judicial investigations and prosecutions,[44] it cannot be said that there is

44 Ankara 13th Administrative Court's decision numbered 14/2/2020 T., 2018/2355 E., 2020/426 K.

any damage that needs to be compensated in the incident subject to the lawsuit[45] and it is out of the question to hold the defendant responsible since there is no unlawful and defective action of the defendant. Because the defendant ICTA only sent the information requested by the High Criminal Court to the court in confidence.[46]

A noteworthy point in both the Constitutional Court and the ECtHR judgement is the reminder that *"the decisions of the courts of first instance are subject to judicial review*" even if no compensation is awarded in similar cases. In this way, even if a favourable decision is not rendered by the courts of first instance, it is possible that compensation may be awarded at the stage of appeal, and thus, a remedy that does not operate on a contingency basis has been found effective.

As a result of our research, we would like to state that we have not come across a favourable decision on this issue, and we have reached much more unfavourable decisions in the number of decisions cited as precedents by the Constitutional Court. These judgements indicate the idea that *"even if the courts of first instance of the Constitutional Court and the ECtHR do not award compensation, the appeal or appellate authority may award compensation"* is not correct. Namely; one of the judgements cited as a precedent by the Constitutional Court was given by the Ankara 2nd Administrative Court. In this decision, the court stated that *"it is clear that the respondent institution did not have any service defect at the point of fulfilling the inspection activities, and the criminal proceedings carried out by the Tekirdağ 2. In the criminal proceedings conducted by the Assize Court, there was no determination that the CGNAT records were created incorrectly by the operator (GSM operator), on the contrary, considering that the plaintiff was convicted as a result of the determination that the plaintiff entered the ByLock programme, which was used as the intra-organisational encrypted communication system of the FETÖ/PDY terrorist organisation, it cannot be said that there is any damage that needs to be compensated in the incident"*.[47] The 7th Administrative Case Chamber of the Ankara Regional Administrative Court, which examined the appeal of this decision, stated that the decision of the administrative court subject to the appeal

45 Ankara 2nd Administrative Court's decision dated 19/2/2019 T., 2019/1169 E., 2019/2537 K.

46 Decision of Istanbul Anatolian 7th Civil Court of First Instance dated 15/10/2020, numbered 2017/454 E., 2020/212 K.

47 Ankara 2nd Administrative Court's decision dated 19/2/2019 T., 2019/1169 E., 2019/2537 K.

application was in accordance with the procedure and law and that there was no reason for its removal **and** rejected the appeal application[48]

In another case where the Constitutional Court gave an example of the effectiveness of the compensation remedy, the plaintiff filed a lawsuit against the ICTA at the Ankara 12th Administrative Court, claiming that the data such as HTS records, GPRS records, GSM call records belonging to him were submitted to the court where he was on trial and that an unlawful action was taken against the ICTA. Ankara 12th Administrative Court decided to dismiss the case without examining the case on the grounds that *"the records, which are the basis of the compensation request subject to the dispute and which are requested to be deleted, are used as evidence in criminal law and are in the nature of determination, are not in the nature of an administrative action and* ***cannot be subject to an administrative action, and therefore, it is not possible to examine the merits of the compensation request requested accordingly***".[49]

Upon the application for appeal by the plaintiff, Ankara Regional Administrative Court 7th Administrative Litigation Chamber of Ankara Regional Administrative Court decided to lift the decision and send the case file back to the court for a new decision, stating that *"the plaintiff filed the case with the allegations that his personal data were stored out of time in violation of the legal provisions and that the failure to delete them on time constituted a service defect, therefore, there is no obstacle to file a full judicial action due to these transactions within the framework of the relevant provision of the Constitution and Law No. 2577, while the Administrative Court should examine the merits of the case and make a decision, there is no legal merit in the decision given to reject the case without examination*"[50] . Ankara 12th Administrative Court decided to dismiss the case this time.[51] As a result of the appeal filed by the plaintiff, the Ankara Regional Administrative Court decided **definitively** to reject the appeal.[52] In other words, the administrative court and the Court of Appeal have stated that this action cannot even be the subject of an administrative lawsuit and accordingly, it is not possible to examine the merits of the compensation claim,

48 Ankara Regional Administrative Court 7th Administrative Case Chamber's decision numbered 30/12/2020 T., 2020/627 E., 2020/1744 K.

49 Ankara 12th Administrative Court's decision numbered 13/02/2020 T., 2019/1908 E., 2020/238 K.

50 Ankara Regional Administrative Court 7th Administrative Case Chamber's decision numbered 25/6/2020 T., 2020/753 E., 2020/627 K.

51 Ankara 12th Administrative Court's decision numbered 24/12/2020 T., 2020/1651 E., 2020/2229 K.

52 Ankara Regional Administrative Court's decision numbered 18/02/2021 T., 2021/198 E., 2021/222 K.

which the Constitutional Court and the ECtHR consider effective. **It is obvious that the compensation remedy, the merits of which the courts have not even examined, is not effective.**

The Ankara Regional Administrative Court 10th Administrative Case Chamber, which conducted the appeal review of the Ankara 13th Administrative Court decision[53] , which is another of the decisions cited as a precedent by the Constitutional Court, stated that the decision of the administrative court was in accordance with the procedure and law and that there was no reason for its reversal and decided to approve it **definitively.**[54]

In another case filed on the subject, Ankara 16th Administrative Court stated: *"...in the case; although it is clear that the relevant parties can file a full judicial action as well as an action for annulment due to an administrative action that violates their rights in accordance with the above-mentioned legislation; since the HTS records, which are requested to be annulled in the case under consideration, do not qualify as a transaction that can be subject to an administrative action, it is concluded that the compensation requested accordingly cannot be qualified as a compensation request made within the scope of Articles 2 and 12 of the Administrative Procedure Law No. 2577. and 12 of the Administrative Procedure Law No. 2577, it is not possible to examine the merits of this part of the case*[55], stating that the incident subject to the application cannot be subject to a full judicial action as well as an action for cancellation. The Ankara Regional Administrative Court 8th Administrative Case Chamber, which examined the appeal of this file, stated that the decision of the administrative court was in accordance with the procedure and law and that there was no reason for the acceptance of the application for appeal and **conclusively** decided to reject the application for appeal.[56]

In another decision rendered by Ankara 2nd Administrative Court, the plaintiff requested the cancellation of the HTS records containing the data on the communication programme named Bylock, which was used as the basis for his criminal conviction, and the calculation of his financial losses and the payment of 2.000.000.000.000,00 TL compensation.

---

53 Ankara 13th Administrative Court's decision numbered 14/2/2020 T., 2018/2355 E., 2020/426 K.

54 Ankara Regional Administrative Court 10th Administrative Case Chamber's decision numbered 11/11/2020 T., 2020/1787 E., 2020/2310 K.

55 Ankara 16th Administrative Court's decision No. 29/3/2018 T., 2018/612 E., 2018/768 K.

56 Ankara Regional Administrative Court 8th Administrative Case Chamber's decision numbered 08/10/2018 T., 2018/1320 E., 2018/1198 K.

Ankara 2nd Administrative Court dismissed **this case with the same reasoning as in the previous decision (16th Administrative Court)**, namely; *"in the case; although it is clear that in accordance with the above-mentioned legislation, those concerned can file a full judicial action as well as an action for cancellation due to an administrative action that violates their rights; since the HTS records requested to be cancelled in the case under consideration do not qualify as a transaction that can be subject to administrative action, the compensation requested accordingly is a compensation request made within the scope of Articles 2 and 12 of the Administrative Procedure Law No. 2577. and 12 of the Administrative Procedure Law No. 2577, it is not possible to examine the merits of this part of the case".*[57] It is noteworthy that the grounds for the rejection decisions of two different courts on different dates are the same with the dots and commas.

This interesting situation is not unique to these two courts. Because the grounds of rejection of the 3rd[58] 12th[59] and 23rd Administrative[60] Courts of Ankara, which rejected the lawsuits filed on the subject, are exactly the same. The grounds for rejection of all three cases are as follows; "*In order to talk about the legal responsibility of the administration, there must be a damage and this damage must arise from a transaction or action that can be attributed to the administration, in other words, there must be a proper causal link between the damage and the administrative activity, the responsibility of the administration is based on the principles of service defect and strict liability, whether service defect, whether it is based on the principles of perfect liability or not, the existence of a damage, the action or transaction causing the damage being attributable to the administration, and the existence of a causal link between the damage and the action or transaction are mandatory in order for the administration's obligation to compensate, and the absence of one of these conditions will eliminate the responsibility of the administration. In other words, if there is no damage or if the damage is not related to the administrative action or transaction, if the administrative activity does not constitute the real cause or causation of the damage, if there is no causal link between them, or if the action or transaction causing the damage is not attributable to the administration, the responsibility of the administration is eliminated.*

57 Decision of Ankara 2nd Administrative Court No. 12/4/2019 T., 2019/628 E., 2019/782 K.
58 Ankara 3rd Administrative Court's decision dated 27/11/2019 T., 2019/365 E., 2019/2456 K.
59 Ankara 23rd Administrative Court's decision numbered 24/12/2020 T., .2020/1651 E., 2020/2229 K.
60 Ankara 23rd Administrative Court's decision dated 3/10/2019, no. 2018/740 E., 2019/353 K.

In the dispute, from the evaluation of the above-mentioned legislative provisions together with the case in question, it is understood that it is a legal obligation for the respondent administration to store the data of the communication made via telecommunication in order to fulfil these requests if requested by the Chief Public Prosecutor's Offices and Courts in judicial investigations and prosecutions.

In this case, since it is understood that there is no service defect that can be attributed to the defendant administration in the case subject to the case arising from the application of the laws, and that the defendant administration cannot be held responsible in the concrete case, it is concluded and concluded that the plaintiff's claim for non-pecuniary damages should be rejected."

In other words, all of the decisions were given in a template and *"cut-copy-paste"* manner. The fact that three different Ankara administrative courts rejected three different cases with the same reasoning, down to the dots and commas, is important in terms of showing the attitude of the administrative courts regarding these cases and is an indication that compensation lawsuits to these courts are not an effective remedy.

Of these three cases, the 10th Administrative Case Chamber of the Ankara Regional Administrative Court, which examined the appeal of the decision of the Ankara 3rd Administrative Court, upheld the decision of the administrative court subject to the appeal application, stating that it was in accordance with the procedure and law and that there was no reason for its reversal.[61] After the finalisation of the decision, the applicant made an individual application to the Constitutional Court and claimed that his rights to private life and fair trial were violated. The Constitutional Court, on the other hand, found the complaint regarding the right to private life to be manifestly unfounded due to the absence of an interference with the fundamental rights and freedoms stipulated in the Constitution, and the complaint regarding the right to a fair trial to be inadmissible due to lack of jurisdiction in terms of subject matter.[62] Thereupon, the applicant applied to the ECtHR and the case is pending before the ECtHR.

The 7th Administrative Case Chamber of the Ankara Regional Administrative Court, which examined the appeal of the decision of the Ankara 23rd Administrative Court, ruled

---

61 Ankara Regional Administrative Court 10th Administrative Case Chamber's decision numbered 25/6/2020 T., 2020/1272 E., 2020/1004 K.

62 Constitutional Court's decision dated 22/12/2020 and numbered 2020/29100 B.

that the administrative court decision subject to the appeal application was in accordance with the procedure and law and that there was no reason for its annulment.[63]

In another lawsuit filed on the subject, the plaintiff filed a lawsuit for the cancellation of the said report, claiming that in the report of the ICTA dated 26/12/2017, an evaluation was made as a result of the administrative examination that 11,480 people were directed to the server IPs served by the Bylock Application against their will, and that in the said report, the gsm line 0532..... was excluded from the classification of those who were directed to the Bylock server against their will, that their personal rights were violated due to this erroneous administrative action and that they were victimised as a result. The court decided to dismiss the lawsuit without examining the case, stating that the legal consequences of the ICTA's report subject to the lawsuit are only possible with the actions to be taken on this report, that the said report is not **final and executable**, since it does not have the nature of affecting the rights and law of the plaintiff alone at this stage, **and that it is not possible to examine the merits of the pending lawsuit in this respect**.[64] As it can be seen, the Government's defence (§ 111 and 112) submitted to the ECtHR in Çamurşen's application that since all kinds of actions taken by the ICTA are administrative actions, the persons who are damaged by these administrative actions can request compensation for the damages by filing a full remedy action before the administrative courts was not adopted by the Administrative Court and it was decided to dismiss the compensation cases without even examining the merits on the grounds that *"HTS records are not in the nature of an action that can be subject to an administrative action*".

In the case subject to the last decision that we have been able to determine on the subject, the plaintiff filed a lawsuit for pecuniary and non-pecuniary damages against this institution due to the fact that the records requested by the court from the ICTA in the criminal file in which he was tried as a defendant were sent to the court by the ICTA despite the expiration of the 2-year retention period.[65] However, as a result of the examination made through Uyap, the court determined that the plaintiff had also filed a lawsuit against Turkcel İletişim Hizmetleri

63 Ankara Regional Administrative Court 7th Administrative Case Chamber's decision numbered 16/01/2020 T., 2020/19 E., 2020/32 K.

64 Ankara 16th Administrative Court's decision numbered 22/5/2018 T., 2018/1032 E., 2018/1153 K.

65 Decision of Istanbul Anatolian 16th Civil Court of First Instance dated 29/5/2018, numbered 2017/558 E., 2018/209 K.

A.Ş. in the file numbered 2017/454 of the Istanbul Anatolian 7th Civil Court of First Instance and decided to consolidate both lawsuits and to continue the proceedings through the case at the Anatolian 7th Civil Court of First Instance. Anadolu 7th Civil Court of First Instance also dismissed the case by stating that "*in the concrete case, the defendant did not have an unlawful and defective action, and accordingly, it is out of question to be held responsible, and since it is understood that he only sent the information requested by the High Criminal Court to the court confidentially, it has been concluded and concluded that the judgement on the dismissal of the lawsuit as follows".*[66]

In dismissing the Çamurşen application, the ECtHR stated that this result would in no way prejudice the subsequent examination of the effectiveness of the relevant remedies and, in particular, the ability of national courts to develop a uniform and Convention-compatible approach to the retention of personal data, and pointed out that it would not close the question of the effectiveness of these remedies altogether but could re-examine this issue. The ECtHR is expected to abandon its view on the effectiveness of the compensation remedy on the basis of the four judgements cited by the Constitutional Court in which no compensation was awarded.

e) The contradiction of the Constitutional Court; Is the compensation remedy a remedy that must be exhausted?

In six cases other than Çamurşen, the Constitutional Court considered the criminal remedy sufficient for exhaustion of domestic remedies and rejected these applications *"on the merits"*. Later, in the case of Ertan Erçıktı (3), in which only the criminal remedy was exhausted, **the Constitutional Court rejected the application, stating that there was no application for compensation before the administrative or judicial courts and therefore domestic remedies were not exhausted.** The remedies considered effective by the Constitutional Court and the ECtHR are non-pecuniary damages to be filed within 2 years and in any case within 10 years from the date of learning that the internet traffic information has been stored for longer than the legal period in accordance with Articles 58 and 72 of the Code of Obligations, or a full judgement action under Article 12 of the İYUK.

66 Decision of Istanbul Anatolian 7th Civil Court of First Instance dated 15/10/2020, numbered 2017/454 E., 2020/212 K.

However, as mentioned above, there has not been a single judgment to date setting out that the compensation remedy is effective and that these cases have been concluded in favour of the applicants. Moreover, the aim of the applicants in these applications is not to obtain compensation, but to establish that internet traffic data and HTS records have become unlawful evidence and cannot be used in the proceedings due to the fact that they have been stored for longer than the required period of time. Likewise, in the event that compensation is awarded, the interference with the right to private life will not end. Because in this case, even if the person concerned receives the compensation awarded, who will request the deletion of the internet traffic data kept longer than the destruction period with this decision?

As mentioned in the previous section, the ICTA is not authorised to spontaneously request data or to retain the data received. According to the legislation, these data should not be in the possession of the ICTA anyway. This is because the ICTA is an *"intermediary"* organisation, not *an "executive" one*, and is tasked with receiving the requested information from internet service providers and forwarding it to the judicial authorities. In other words, the ICTA does not have the authority and duty to destroy this data and terminate the breach. The authorisation granted to the ICTA is given in order to prevent internet traffic data and HTS records from being stored for longer than their duration. However, the ICTA uses this authorisation not to ensure the destruction of the data and records, but to send them to itself, despite the fact that there is no legal basis for this. In other words, the ICTA is clearly abusing the authorisation granted to it, and the problem that has arisen is that the ICTA is receiving and storing data and records from companies even though it has no authorisation to do so.

If the ICTA requests this data from internet service providers, no internet or access provider will admit that it keeps the data more than it is required to keep, and will say that it sends these data and records to ICTA. This is because storing data more than prescribed is explicitly regulated as an offence in Article 138 of the TPC, and the relevant companies will be punished with administrative fines in accordance with Law No. 5809. Therefore, in the event that compensation is awarded, the problem of who will destroy the violation, i.e. internet traffic data or HTS data, will arise. Because normally, these data should have been destroyed in advance and should not have been used in any way. It is precisely at this point that the source of the problem and the reason for the interference with the right to private life of tens of thousands of people is the fact that the ICTA regularly requests all data and records from

internet service providers and businesses, even though it is not authorised to do so, and that these companies are forced to accept this request due to their fear of the public power exercised by the ICTA, despite the fact that it is against the legislation.

Another problem regarding the effectiveness of the remedy is that the ECtHR, like the Constitutional Court, considers the criminal remedy ineffective. However, Article 138 of the TPC explicitly criminalises *"failure to destroy data"* and stipulates that those who are obliged to destroy the data in the system despite the expiry of the time periods set by law shall be punished with imprisonment from one year to two years if they fail to fulfil their duties. Furthermore, pursuant to Article 139 of the TPC, this offence is not subject to complaint. Similarly, Article 134 of the TPC criminalises *"violating the privacy of private life" and* Article 136 criminalises *"illegally giving or obtaining data"*, and the commission of these offences by a public official and by abusing the authority granted by his/her duty is an aggravating circumstance.

While there is a regulation directly related to the incident subject to the complaint in the Turkish Penal Code and the failure to destroy internet traffic data or HTS records within the period stipulated in the legislation is regulated as a criminal offence, why is the insistence on requesting the exhaustion of the compensation remedy, which is not considered effective and where there is no example of an effective remedy? Moreover, if it is accepted that it is possible to eliminate the violation through the compensation remedy, the same applies to the criminal remedy. This is because a criminal court will first determine whether the data has been stored for longer than stipulated and after this determination, the person(s) who did not delete the data will be penalised. As it will be revealed that the traffic data and records have been kept unlawfully, it will not be possible to use these data as evidence in criminal proceedings. Thanks to this way, both the violation of the applicants' private lives and the situation of accepting as evidence the data and records, which are more important for these persons and which are the grounds for their punishment, will be eliminated.

Although this was the concrete reality, the ECtHR stated that there was an effectively functioning legal remedy before the civil and administrative courts, as if there was a compensation awarded in favour of the plaintiffs in the court decisions cited in the Constitutional Court judgment. When the judgements cited above as examples are examined, it is understood that either they were dismissed without even examining the merits (on the grounds that it was not the subject matter of the administrative judiciary) or the compensation

claims were dismissed on abstract grounds stating that there was no fault of the administration and access providers, without taking into account the provisions of Laws No. 5651 and 5809, which contain mandatory regulations in Turkish law that traffic information can be stored for a maximum period of one year, and the provisions of the Regulation on the implementation of these laws. As can be seen, even the judgements submitted by the Government to the Court in order to represent that the remedies for compensation before the administrative and civil courts are effective remedies indicate that these remedies are not effective remedies that offer a chance of success in practice. In other words, the Government has not been able to prove that the application to the Civil and Administrative Courts is an effective domestic remedy, on the contrary, it has demonstrated that the application to these remedies is not effective.

In the concrete case, in the context of the determination of the violation of the right to request the protection of personal data and the prevention of the use of these unlawfully obtained data as evidence in criminal proceedings, it is understood that the compensation proceedings do not offer a reasonable capacity for success that is more appropriate to the applicant's purpose than the criminal investigation. In other words, considering the applicant's allegations of violation, the compensation remedy before the Civil and Administrative Court is prima facie available and does not have the capacity to offer a chance of success and provide adequate redress in relation to the allegations of violation.

In fact, the same situation also applies to the criminal remedy. This is because, despite the obligation to delete internet traffic data under Laws No. 5809 and 5651 and the criminal offence of not deleting such data under the Turkish Penal Code, all six files merged with Çamurşen's application resulted in a decision of *"not to process"*. In other words, the complaints were never investigated. For example, in a case where a criminal complaint was filed for the deletion of internet traffic data between 2014 and 2016, Ankara Chief Public Prosecutor's Office decided not to process the petition, stating that the complainant's claim was in the nature of a defence in the case in which he was being tried, that this request should be evaluated by the court in which he was being tried, and that there was no criminal act. [67]

67 Ankara Chief Public Prosecutor's Office's decision of 30/10/2018 T., 2018/19086 investigation and 2018/115623 decision number.

The justification for the decision not to process another complaint of the same nature is more interesting. In its decision, the Ankara Chief Public Prosecutor's Office stated that Article 6 of the Law No. 5651 Article 6 of the Law No. 5651 states that internet traffic information can be stored for up to two years, the fact that it is determined as one year in the Regulation will not make the action an offence, in the hierarchy of norms, the provision of the law is valid first, moreover, the purpose of storing traffic information for a certain period of time is due to the fact that this process imposes a large amount of burden on access providers and hosting providers, the court did not even process the complaint, stating that the legislator has made it obligatory to keep these data for up to two years in order to reveal criminal acts, and that the crimes of unlawfully obtaining and disseminating personal data and unlawfully recording personal data must be committed intentionally, and that it is understood that sending information in response to the court request cannot be considered as the transfer and dissemination of personal data to another person and will not constitute a crime.[68]

However, the regulation made in Article 138 of the TPC has been introduced precisely for the purpose of penalising the acts subject to the complaints. In a judicial practice that thinks that the purpose of deleting internet traffic data, which is personal data, is not to impose more burdens on companies, is unaware of the fact that the events subject to the complaint are directly related to the violation of the right to private life, and does not process the applications based on personal opinions instead of the regulations in the legislation, it cannot be said that there is an effective legal remedy on the subject. It is precisely for this reason that neither the courts nor the prosecutor's offices issue any favourable judgements, including the so-called effective remedy of compensation.

The ECtHR is aware that tens of thousands of people have been and are being punished on the basis of internet traffic data and HTS records that have not been destroyed despite the expiry of the retention period, particularly in Bylock trials. Although the applicants raise this issue at every stage of the proceedings, their requests are not accepted in any way and even this issue, which is clearly regulated in the legislation, is not taken into consideration by the courts. As in the case of the Çamurşen application, the ECtHR, to which the applicants applied

68 Ankara Chief Public Prosecutor's Office's decision not to proceed on 28/5/2018 T., 2018/102318 investigation and 2018/63023 decision number.

as a last resort, rejected the application by referring to the justifications of the Constitutional Court, which, as mentioned above, even wrote the article of the law it cancelled under the name of *"relevant law*" in its decision in order to reject the application.

In short, the compensation remedy that the ECtHR requires to be exhausted is certainly not effective and, as can be seen from the judgements cited above, the courts are highly motivated not to award compensation in this regard. Despite all this, the ECtHR, in its Çamurşen judgement, required the exhaustion of the ineffective compensation remedy. The question arises as to whether the ECtHR has reserved the six cases in the Çamurşen group for rejection with reference to this judgement.

f) What will be the ECtHR's attitude towards the file separated from the Çamurşen Application?

The Çamurşen judgment has revealed an interesting situation which deserves criticism. This is because, although the Çamurşen application was rejected on the grounds of non-exhaustion of domestic remedies and the applicants in the other six cases had exhausted only the criminal remedy, the ECtHR ignored the fact that the Constitutional Court had rejected these applications not for the same reason but on the grounds that there was no violation of rights. If only exhaustion of the criminal remedy was not effective, why did the Constitutional Court reject the six applications other than Çamurşen *"on the merits"* instead? Although the ECtHR was aware that the exhaustion of the criminal remedy was deemed sufficient by the Constitutional Court, it deemed it appropriate to separate this case and to decide on it and to keep the other cases pending

The first decision of the ECtHR to be criticised in this respect is undoubtedly Yüksel Yalçınkaya v. Turkey. In this application, the ECtHR, which did not even question the Government on the exhaustion of domestic remedies, did not even feel the need to examine the application made under Article 8, citing the violation of the right to a fair trial. If this issue had been examined in Yalçınkaya's application, a violation of this clearly unlawful matter would have been given and the unlawfulness of this judicial practice, which directly concerns tens of thousands of people, would have been judged. However, the ECtHR took the easy way out and ignored the most important indicator of the unlawfulness of this data, namely the

issues raised under Article 8, as if it had stated that the method of obtaining internet traffic data was unlawful in its examination within the scope of fair trial.

If the ECtHR had made this determination in its assessment of the right to a fair trial, it might have been acceptable not to examine the violation allegations regarding Article 8. However, the ECtHR not only did not say anything concrete and clear in its examination within the scope of the right to a fair trial, and contented itself with stating that there were grounds for suspicion regarding the protection of data integrity in the period before the internet traffic data was delivered to the prosecutor's office, but also avoided the examination that would have meant the determination that the data, which was as important as these grounds for suspicion, had become unlawful due to their further storage.

After the Çamurşen judgement, what is of interest is what the ECtHR's attitude will be and what kind of a decision it will make in the six cases that the Constitutional Court found inadmissible on the grounds that there was no violation of the right to private life. In these cases, the ECtHR is expected to decide on the violation of the right to respect for private life by conducting an examination on the merits like the Constitutional Court. Below, explanations on the element of legality, which is expected to be the most important reason for the ECtHR to find a violation under this right, and why the legislation and practice in domestic law do not meet this element are given.

Freedom of communication, which is one of the elements of the right to respect for private life, is regulated in Article 22 of the Constitution and Article 8 of the ECHR. *The confidentiality of communication is essential"* and the ECHR states *that "everyone has the right to respect for his communications".*

This right guarantees the right of individuals to communicate with others without hindrance or censorship and includes the right to confidentiality of communications. The ECtHR has not limited the scope of the right to certain means of communication, but has interpreted it broadly to include all forms of communication by telephone, letter, fax and internet. The Court considers the telephone numbers dialled, personal information relating to telephone, e-mail and internet use, information stored on a card by the investigating authorities about the applicant's business affairs, information stored by the authorities about his remote publicly available past, and the applicant's interests in protecting his identity in relation to his online activity to be within the concept of *"private life"* and therefore within the scope of Article 8. Furthermore, the court

noted that subscriber information associated with a dynamic IP address allocated for a certain period of time was not publicly available and was therefore not comparable to information contained in a publicly available database, such as a traditional telephone directory or government-registered vehicle registration plates, and that the use of such stored data could in itself constitute an interference with private life.[69]

This right is not one of the absolute rights, that is to say, it is not one of the rights whose exercise cannot be stopped under Article 15 of the ECHR, and the right may be interfered with in the presence of conditions. Article 8(2) of the ECHR states*: "Interference by a public authority with the exercise of this right may only take place to the extent necessary in a democratic society in the interests of national security, public safety, the economic well-being of the country, the protection of law and order, the prevention of crime, the protection of health or morals or the rights and freedoms of others, and provided that such interference is prescribed by law"*. Article 22/2 of the Constitution stipulates that communication may be prevented and its confidentiality may be interfered with if there is a duly issued judge's decision based on one or more of the reasons of national security, public order, prevention of crime, protection of public health and public morals or protection of the rights and freedoms of others.

As can be understood from the texts of the articles, the interference with a right is justified if it is legally prescribed (legality), has a legitimate aim and is necessary in a democratic society. The ECtHR examines the existence of these conditions in order and does not investigate the existence of other conditions if the legality condition is not fulfilled.

The requirement of legality is a common element of Articles 8, 9, 10 and 11 of the Convention and requires that the interference with the exercise of the right must have a basis in domestic law. The respondent State must show the existence of a rule of law authorising it to interfere with the right.[70] The source of this rule may be written law, i.e. the Constitution, laws, decrees, statutes and regulations, or case law. In other words, the ECHR is to interpret the concept of law in its substantive, not formal, sense.[71]

---

69 Benedik v Slovenia Judgment of the ECtHR § § 104-108.

70 ECtHR Judgment in Silver and Others v. the United Kingdom, B.No:5947/72, 25/3/1983, § 86.

71 ECHR's Malone v. the United Kingdom, B.No: 8691/79, 02/8/1984, ECHR's Sunday Times v. the United Kingdom, B.No: 6538/74, 26/4/1979, § 47.

The review of legality requires that the regulation on which the intervention is based is accessible, that its consequences are foreseeably clear, and it contains safeguards against abuse.[72]

In accordance with the accessibility criterion, the legal regulation forming the basis of the interference must be made available by publication and the persons concerned must have the necessary and sufficient information about the rule of law applicable to a particular case.[73] In accordance with the foreseeability criterion, domestic law must be sufficiently clear as to the circumstances and grounds on which the measure constituting the basis of the interference may be invoked. This clarity may vary according to the nature of the right interfered with and the measure applied, the content of the legal regulation, the field it regulates, the status and number of persons concerned. [74]

Having a legal basis, being accessible and foreseeable is not sufficient for the interference to be recognised as lawful and the existing law must provide safeguards against arbitrary interference

The requirement that the existing law must also provide guarantees against arbitrary interventions, which is one of the elements of legality, is not met in the present and similar cases. This is because the ICTA itself does not comply with the data retention periods introduced for this purpose. The principles laid down by the ECtHR in its recent judgement in **Skoberne v. Slovenia** are also closely related to the files separated from the Çamurşen application. Finding a violation in the aforementioned judgement, the ECtHR stated that the relevant service provider kept the internet traffic data for the fourteen-month legal period stipulated in the Law and handed over to the authorities only the data within this period, and that the interference in question was in accordance with the applicable domestic law and did not see a problem with the interference in terms of legality (130).

According to the ECtHR, the Slovenian Act did not leave any decision in this respect to the discretion of the State or non-State organisation and was not ambiguous as to its application. Any individual or organisation using the services of telecommunications

72 ECtHR Judgment in PG and JH v. the United Kingdom, B.No: 44787/98, 25/9/2001.
73 ECtHR Judgment in Silver and Others v. the United Kingdom, § § 87-88.
74 ECtHR Judgment in Sunday Times v. the United Kingdom, § 49.

providers in Slovenia can assume that telecommunications data is stored as part of comprehensive data collection. However, **the vagueness of the law establishing the general and indiscriminate retention of** telecommunications data **cannot be interpreted as constituting a sufficient guarantee of compliance with the principles of the rule of law and proportionality** (§ 138).

The Court notes that in Slovenia the amended 2004 Act sets out a number of purposes for which telecommunications data should be retained, but contains no provisions limiting the scope and application of the measure in relation to what is necessary to achieve those purposes. In accordance with the Court's case-law, as part of the minimum requirements, national legislation must, as part of the minimum requirements, define the scope of the application of the measure in question in a manner appropriate to the form of review concerned and provide for appropriate procedures for the award of such a measure and/or its review with a view to keeping it within the limits of what is necessary. Given the nature of the interference in the present case, these minimum requirements must also be met in the case of a measure requiring the retention of communications data. The absence of provisions or mechanisms to ensure that the measure is genuinely limited to what is *"necessary in a democratic society"* for the specific purposes enumerated in Law 2004 renders such a regime incompatible with the State's obligations under Article 8. The fact that the retention of the data was limited to a considerable period of only 14 months does not alter this conclusion (§ 139).

In this case, the applicant argued that, due to the unjustified retention of his data, their acquisition and use in domestic proceedings violated Article 8. According to the ECtHR, where the retention of telecommunications data is found to breach Article 8 because it does not comply with the *"quality of law*" requirement and/or the principle of proportionality, access to that data - and its subsequent processing and storage by the authorities - would be contrary to Article 8 for the same reason. Referring to the CJEU's opinion in this context, the ECtHR noted that communications data cannot be held in general and indiscriminate retention for the purpose of combating serious offences, and therefore access to such data cannot be justified for the same purpose (144).

The applicant's complaint relates to the entirety of his data relating to a period of fourteen months, which was obtained by law enforcement agencies and subsequently processed, stored and analysed for the purposes of the criminal proceedings in question. It is

undisputed that so much data could not and was not retained for contractual purposes, but was instead retained as part of a general and retention regime which the Court found above to be in breach of Article 8 of the Convention . (145)

In conclusion, the ECtHR found that the challenged provisions of the Law, which formed the basis for the retention of the applicant's telecommunications data, did not meet the *"quality of law*" requirement and failed to limit *the "interference" with* the applicant's rights under Article 8 to that which was *"necessary in a democratic society*" and that the storage, access and processing of telecommunications data constituted a violation of Article 8 of the Convention. Beyond the 14-month retention period, it is obvious that a practice in which data is stored indefinitely and arbitrarily is not in the nature of a law and violates the right to private life of those concerned.

In the application of Ertan Erçıktı (3), which is the subject of the Constitutional Court's judgement, although there is a legal basis for the interference with the applicant's right to respect for private life, the ICTA itself rendered the 2-year period for the destruction of the data inoperable and caused the violation of the right itself, which is not considered to be a preventive mechanism against the right after the ECtHR's Skoberne v. Slovenia judgement. As mentioned in the previous sections, Article 3, paragraph 4, Article 5, paragraph 5 and subparagraph (d) of paragraph 1 of Article 6 of Law No. 5651, which clearly interferes with the right to private life and authorises the ICTA to request, store and process personal data without a judge's decision, have been cancelled by the Constitutional Court. Pursuant to the legislation, it is not possible for the ICTA to obtain and keep internet traffic information from service providers without a court order. However, the ICTA receives this data on an hourly basis without a court order, the data that should have been destroyed by the service providers after 1 year before 06/11/2016 and after 2 years after 06/11/2016 cannot be destroyed and are kept by the ICTA itself, and people are punished with this data, which is then sent to the courts upon request. In this respect, the procedure envisaged in the legislation is part of a haphazard retention regime, just like in Slovenia, and it is not possible to say that this regulation meets the requirement of legality.

The Constitutional Court, being aware of this situation and knowing that internet traffic data is stored for longer than the periods stipulated in the law, and even not destroyed at all, tried to prove that the ICTA is given wide powers, that the ICTA's data storage authority has a legal basis, and that the period of storage of traffic data is valid for internet access providers

and that there is no time limit for the ICTA, with the regulations related to Laws No. 5809 and No. 5651, which the Ertan Erçıktı (3) decision included under the title of *"relevant legislation"*.

The first point that confirms this is the inclusion in the decision of the provision in Article 6/1-ı of Law No. 5809 stating that "the ICTA *may receive all kinds of information and documents it may need from operators, public institutions and organisations and real and legal persons in relation to electronic communications and keep the necessary records"*. As mentioned before, although the wording of this article initially suggests that the ICTA may receive all kinds of information, documents and data within the scope of its duties, the Law does not authorise the ICTA to do so.

As a matter of fact, the Constitutional Court, which examined the regulation in question;[75] stated that the above-mentioned rules should be taken into consideration as a whole in determining the meaning and scope of the rules, and that after the duty of ensuring cyber security is given to the Authority in the aforementioned article, the paragraph following the said provision states that the ICTA *"...within the scope of its duty..."* to obtain information, documents, data and records from the relevant places, to evaluate them, to make use of archives, electronic data processing centres and communication infrastructure, to establish contact with them and to take or have taken other necessary measures within this scope; These powers and opportunities granted to the ICTA **are limited to** the ICTA's **duty of ensuring cyber security** , on the other hand, in the continuation of the same article, it is stated that it is obligatory to fulfil the requests of the ICTA regarding its duties in the article *"...related to their duties under this article..."* and referring to the provision on the duty to ensure cyber security confirms the above-mentioned meaning and scope of the rules subject to the lawsuit.[76]

In short, **the authority and duty of the ICTA is limited to the task of ensuring cyber security.** Within the scope of this article, the ICTA does not have the duty and authority to record, request from the relevant institutions or organisations, store and archive traffic information, which is personal data. Even though this is the concrete reality, the Constitutional

75 Constitutional Court's decision no. 24/7/2019 T., 2017/16 E., 2019/64 K.; https://normkararlarbilgibankasi.anayasa.gov.tr/ND/2019/64?EsasNo=2017%2F16

76 AYM, E.2017/16, K.2019/64, 24/07/2019, § 38-39

Court has not made an assessment on this issue before, giving the impression that this regulation authorises the ICTA to request all kinds of information and documents.

A more interesting and troublesome situation regarding the decision is that the Constitutional Court included Article 6/1-d of Law No. 5651, which states that access providers are obliged *to "submit the information requested by the Authority to the Authority as requested and take the measures notified by the Authority"*. However, the Constitutional Court cancelled this article on 08/12/2015 with the following reasoning and the article was repealed on 28/01/2017; *"...in this framework, the rules to be cancelled do not provide any certainty regarding the conditions and grounds under which the information requested by the TİB (ICTA) will be delivered to the Presidency by content, hosting and access providers or how long the information provided will be kept at the TİB, the nature of the requested information, the measures to be notified to content, hosting and access providers. In these respects, the rules are not specific and foreseeable. Despite the guarantee in the Constitution, they allow all kinds of personal data, information and documents belonging to individuals to be unconditionally given to TİB without being subject to sufficient limitations in terms of subject, purpose and scope, thus rendering individuals unprotected against the administration. Therefore, since the rules to be cancelled are not specific and foreseeable, they limit the right to protection of personal data disproportionately and contradict Article 20 of the Constitution. For the reasons explained, the rules are contrary to Articles 2, 13 and 20 of the Constitution."*[77] There is no legal explanation for the Constitutional Court's decision to include the article it cancelled as if it is still in force and the documents and information requested by the ICTA based on this article must be sent by the relevant institutions.

In its submissions to the ECtHR in relation to the allegation that the ICTA had retained CGNAT data for longer than provided for by law (Government submission § 71), the Government argued that the provisions of Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed through Such Publications and the Regulation on the Procedures and Principles for the Regulation of Publications on the Internet and the Regulation on the Procedures and Principles for the Regulation of Publications on the Internet implementing this law do not apply to hosting providers established and operating under

77 Constitutional Court's decision no. 08/12/2015 T., 2014/87 E., 2015/112 K.

private law, access providers and content providers, that access providers are only obliged to keep internet traffic information for one year, and that the Law No. 5651 and the Regulation do not impose any obligation on the ICTA, which is a public institution.

As stated in the government's opinion, (in practice) during criminal proceedings, the courts request CGNAT records (traffic information) from the ICTA, and the ICTA sends the court decision to the access providers and requests that these data be sent to it. When the ICTA receives the CGNAT records (traffic information) from the access providers, as in the case of Bylock, the ICTA makes an enquiry as to whether the persons have made a connection to the Bylock server or not, converts the result of the enquiry into a table and sends it to the relevant court. (ICTA does not send the data verbatim, it makes a query as to whether the persons are connected to the Ip addresses of the bylock server, converts the query result into a table and sends the data by processing it in this way). On the other hand, it is contradictory to claim that the legal regulations regarding the retention of internet traffic information for only one year are related to hosting providers, access providers and content providers established and operating under private law provisions, and that the Law No. 5651 and the Regulation do not impose any obligation on the ICTA, which is a public institution. Moreover, with this opinion, the Government has accepted that access providers do not comply with the legal regulations regarding the retention of internet traffic information for only one year.

Based on the definition in Article 1 of Law No. 5651, the Government argued that Article 6/1-b of Law No. 5651 and Article 8/1-b of the Regulation on the Procedures and Principles Regarding the Regulation of Broadcasts on the Internet, issued based on this law, regulate the obligations of access providers. The relevant section states: '...regarding the services it provides, in order for the Presidency to fulfill its duties assigned by the Law and other relevant legislation, the access provider shall retain traffic information for one year.' The Government claimed that the 1-year period in this sentence binds the access providers, meaning that this period does not bind the Information and Communication Technologies Authority (ICTA). However, this provision of the Regulation was cancelled by the Thirteenth Chamber of the Council of State[78] and the cancellation decision became final with the approval of the Council

78 Decision of the 13th Chamber of the Council of State dated 12/12/2019 T., numbered 2013/239 E., 2019/4266 K.

of Administrative Chambers of the Council of State.[79] Therefore, the Government's allegations have no legal basis and equivalent. There is no legal regulation authorising the ICTA to receive, store and destroy internet traffic data. The ICTA, which was established to prevent interferences with the right to private life, clearly violates the right to private life of those concerned by receiving personal data from businesses, keeping them for years and sending them to court, despite the lack of any authorisation granted to it. As of the current situation, the relevant regulations do not contain any guarantee for the protection of personal data and do not fulfil the element of legality in any way.

6. Which Article(s) will the ECtHR examine and decide on?

Another issue of interest is the scope of the right/rights that the ECtHR will examine and decide on in the six applications that it separated from the Çamurşen case. This is because, although the applicants mainly and primarily claimed violation of their right to private life, they also claimed violation of the right to a reasoned judgement, i.e. their right to a fair trial. In this regard, the principles laid down in the ECtHR's **Skoberne v. Slovenia** judgement are of a nature to answer this question.

In the case at hand, the applicant argued that the unjustified retention of his data and their acquisition and use in domestic proceedings violated Article 8. The ECtHR stated that if the retention of communications data was found to violate Article 8 of the Convention on the grounds of *"having the character of a law*" and/or contravening the proportionality requirement, access to such data and the authorities' subsequent processing and retention of such data would also be in breach of Article 8 on the same grounds (§ 144)

The ECtHR notes that, in its view, the violation in the present case occurred irrespective of whether or not the national courts referred to the data held in breach of Article 8 when convicting the applicant. As far as Article 8 is concerned, it is of no significance in the present application that the national courts, when convicting the applicant, referred to a limited portion of the communications data in question (which concerned a period of one month and which could have been retained for contractual reasons). This is because the applicant's complaint concerns the entire data set for a period of fourteen months obtained by the law

79 Decision of the Council of State İDDK numbered 24/2/2022 T., 2020/1851 E., 2022/649 K.

enforcement authorities and subsequently processed, stored and analysed for the relevant criminal proceedings. It is undisputed that such an amount of data cannot and is not retained on contractual grounds; it is rather part of a general and non-discriminatory retention regime which the Court considers contrary to Article 8 (§ 145).

Finally, the Court found a violation of Article 8, stating that the findings on the applicant's complaint under Article 8 did not concern the admissibility of evidence obtained against the applicant, which was a matter to be considered by the national courts in accordance with applicable national law, and that the admission and use in judicial proceedings of evidence obtained in violation of Article 8 did not necessarily lead to a violation of Article 6 (§ 146).

This is precisely the case in the six cases separated from Çamurşen's application, which are expected to be examined by the ECtHR on the merits, and the extent of the violation is even greater in these cases. As explained in detail above, there is no doubt that the keeping of internet traffic data and records in Turkey *"does not have the character of a law"*, violates the proportionality requirement and violates Article 8 of the Convention. Therefore, the ICTA's access to, processing and retention of this data also constitutes a violation of Article 8 on the same grounds.

Similarly, the complaints of the applicants in the six cases relate not to data relating to a period of one year obtained by the courts and subsequently processed, stored and analysed for the purposes of the relevant criminal proceedings, but rather to data kept for more than that period, which should therefore have been destroyed, i.e. should not have existed. It would not be surprising if the ECtHR, which stated that not even all of the data relating to a period of 14 months stipulated in the Slovenian Law could be retained on convention-related grounds and that this was rather contrary to Article 8 and part of a general and non-discriminatory retention regime, would give a stronger violation judgement regarding the data retained in Turkey without a judge's decision, for an unlimited period of time and without any supervision.

Finally, according to the ECtHR, the admission and use of evidence obtained in violation of Article 8 in judicial proceedings does not necessarily result in a violation of Article 6. The main violation claim in these applications is the use of internet traffic data obtained in violation of the right to private life as evidence and the alleged violation of Article 8 of the Convention,

and for the same reason, the ECtHR is expected to find a violation in six applications seperated from Çamurşen .