ECtHR JURISPRUDENCE ON THE MATTER
COLLECTION OF PERSONAL DATA

Alexandru ȚĂRNĂ, PhD student, Moldova State University

Summary
The protection and storage of personal data are clearly related to the right to respect for privacy, as guaranteed by art. 8 of the European Convention on Human Rights. The latter provision protects a whole range of rights, namely the right to respect for private and family life, home and correspondence. The principle is that art. 8 protects personal information in respect of which an individual can legitimately hope that it will not be published or used without his or her consent.

The study aims to break into the jurisprudence of the European Court of Human Rights, the main objective being to identify decisions that have a fundamental impact on the doctrine and practice of personal data collection.

We are aware that multiple regulations in the field of personal data collection can be deduced from the practice of the Court of Justice of the European Union (CJEU). However, given the direct impact of ECtHR decisions on the Republic of Moldova, we found it appropriate to summarize only this aspect. However, in subsequent studies we will address the issue of personal data protection by the Court of Justice of the European Union.

The basic idea, derived from that study, is that the Moldovan authorities should adjust their legislation and practices to the standards set out by the ECtHR and thus avoid possible convictions by the European Court.

Keywords: personal data; European Convention on Human Rights; European Court of Human Rights; Article 8 of the Convention; data collection.

CZU: 341.231.14:342.72

The protection and retention of personal data is clearly part of the right to respect for private life as guaranteed by Article 8 of the European Convention on Human Rights. The latter provision protects a whole range of rights, namely the right to respect for private and family life, home and correspondence.

The principle is that Article 8 protects personal information which an individual can legitimately expect not to be published or used without his or her consent.

It follows from the content of Article 8 ECHR that „Everyone has the right to respect for his private and family life, his home and his correspondence [26]”.

At the same time, interference by a public authority with the exercise of this right is not permitted unless such interference is provided for by law and constitutes a measure which, in a democratic society, is necessary for national security, public safety, the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others [26, art. 8, paragraph 2].

Although Article 8 is primarily concerned with the protection of the individual against arbitrary interference by public authorities, positive obligations inherent in effective respect for private or family life can be added to it.
These obligations may involve the adoption by the State of measures designed to ensure respect for privacy even in the sphere of relations between individuals, e.g. an Internet user and persons providing access to a particular website. In other words, the state has a positive obligation to take measures to effectively prevent acts that seriously harm data relating to an individual, sometimes through effective criminal law provisions.

With regard to the Internet, state liability can undoubtedly be incurred by third parties storing data of individuals.

The protection of personal data has been widely enshrined in the case law of the European Court of Human Rights. Conventionally, for purely scientific reasons, we could classify the case law of the ECtHR on the protection of personal data into 3 main areas. We have in mind:

1. ECtHR decisions on the collection of personal data;
2. ECtHR decisions on the storage and use of personal data;
3. ECtHR decisions in relation to deletion or destruction of personal data.

In the present study we intend to analyse judicial practice exclusively on the dimension of the collection of personal data. Other aspects such as storage, use, deletion and destruction of personal data will be addressed in the scientific research that follows.

With regard to the ECtHR decisions with reference to the collection of personal data, it should be noted from the outset that the process of collecting personal data has undergone a huge development in recent times. The diversity of data collected is impressive: DNA and fingerprint information; G.P.S. data; medical data; interception of communications, telephone calls and covert surveillance; monitoring of computer use by employees; voice samples; video surveillance.

As is only natural, the ECtHR decisions have covered many of these issues.

With reference to DNA and fingerprint information, the ECtHR has clarified as follows: „The mere recording of data relating to the private life of an individual constitutes interference within the meaning of Art. 8 [of the European Convention on Human Rights, which guarantees the right to respect for private and family life, home and correspondence]... In this respect, it is easy to note that Article 8 of the European Convention on Human Rights expressly states: „Everyone has the right to respect for his private and family life, his home and his correspondenc”... The subsequent use of the stored information has no impact on this finding [...]. However, in determining whether personal information retained by the authorities involves any [aspect] [...] of privacy [...], the Court will take due account of the specific context in which the information in question was recorded and retained, the nature of the records, the way in which those records are used and processed and the results that may be obtained [...] [20, paragraph 67].”

With regard to the GPS data, the ECtHR specified that the applicant, suspected of involvement in bomb attacks committed by a left-wing extremist movement, complained in particular that his GPS surveillance and the use of the data thus obtained in the criminal proceedings against him violated his right to privacy. The Court ruled that there had been no violation of Article 8 of the Convention. The GPS surveillance and the processing and use of the data thus obtained did indeed constitute an interference with the applicant’s right to respect for his private life. However, the Court observed, it pursued the legitimate aims of protecting national security, public safety and victims’ rights, and preventing the commission of criminal offences. It was also proportionate: the GPS surveillance was ordered only after less intrusive investigative methods had proved insufficient was conducted over a relatively short period (of about
three months) and affected the applicant only when he was travelling in his accomplice's car. The applicant could not therefore claim that he was subject to total and exhaustive surveillance. Given that the investigation concerned very serious offences, GPS surveillance of the applicant was thus necessary in a democratic society [23].

A similar approach was taken in the case of Mohamed Ben Faiza v. France, brought on 22 May 2012. The applicant in that case complained, in particular, of interference with his privacy following the installation of a GPS tracking device in his vehicle in order to monitor his movements in the course of an investigation into drug trafficking. The Court communicated the application to the French Government and addressed questions to the parties under Article 8 (right to respect for private life) of the Convention [27].

The issue of collection of medical data has been confirmed in the case against Latvia. The applicant claimed, in particular, that the collection of her personal medical data by a state agency - in this case, the Health and Work Capacity Quality Control Inspectorate ("MADEKKI") - without her consent violated her right to respect for her private life. In this judgment, the Court recalled the importance of the protection of medical data in order for a person to enjoy the right to respect for his or her private life. It ruled that Article 8 of the Convention had been violated in the applicant's case, finding that the applicable legislation did not indicate with sufficient clarity the extent of the margin of discretion conferred on the competent authorities and the manner in which it should be exercised. The Court noted, in particular, that Latvian law did not limit in any way the scope of the private data that could be collected by MADEKKI, which resulted in the collection of the applicant's medical data for a period of 7 years without distinction and without any prior assessment of whether such data could possibly be decisive, relevant or important for the fulfillment of any purpose that the research in question would have pursued [12].

With regard to the interception of communications, telephone conversations and secret surveillance, the ECtHR has been prodigiously active and several relevant decisions have been recorded. We mention the most relevant ones:

The case of Klass and others v Germany. In this case, the applicants, five German lawyers, complained in particular about German legislation which allowed the authorities to monitor their correspondence and telephone communications without requiring the authorities to inform them afterwards of the measures taken against them. The Court held that there had been no violation of Article 8 of the Convention, finding that the German legislature was justified in regarding the interference resulting from the contested legislation with the exercise of the right guaranteed by Article 8, paragraph 1 as necessary in a democratic society in the interests of national security and in order to prevent disorder or criminal offences (Article 8, paragraph 2). The Court observed, in particular, that these powers to carry out secret surveillance of citizens, which are characteristic of a police State, are tolerable under the Convention only to the extent strictly necessary to protect democratic institutions. Noting, however, that democratic societies today are threatened by highly sophisticated forms of espionage and terrorism, which requires that the State must be able, in order to counter such threats effectively, to supervise in secret subversive elements operating within its jurisdiction, the Court held that the existence of certain legislation granting the power to supervise in secret correspondence, postal communications and telecommunications is, in exceptional circumstances, necessary in a democratic society in the interests of national security and/or to prevent disorder or criminal offences [8].
Malone v United Kingdom. Charged with a series of offences relating to concealing stolen property, the complainant complained in particular about the interception of his telephone and postal communications by or on behalf of the police and the „counting” of his telephone calls (a process involving the use of a device which records the numbers called from a particular telephone and the time and duration of each call). The Court ruled that there had been a violation of Article 8 of the Convention, both in relation to the interception of communications and the sending of records of the numbers dialled to the police, because they were not required by law [13].

Kruslin v France. This case concerned the wiretapping ordered by the investigating judge in a murder case. The Court ruled that there had been a violation of Article 8 of the Convention, finding that French law did not indicate with sufficient clarity the extent and manner of exercise of the authorities’ discretion in this area. This was all the more evident at the time of the facts, so that the Court held that the applicant did not enjoy the minimum degree of protection afforded to citizens under the rule of law in a democratic society [11].

Such an approach has been consistently maintained by the Court in subsequent decisions. For example, Huvig v France [6]; Halford v UK [5]; Kopp v Slovenia [10]. In the latter case, the wiretapping of the telephone lines of the applicant’s law firm by order of the Federal Public Prosecutor is concerned. The Court held that there had been a violation of Article 8 of the Convention, finding that Swiss law did not indicate with sufficient clarity the extent and manner of exercise of the authorities’ discretion in this area. The Court therefore held that the applicant, in his capacity as a lawyer, did not enjoy the minimum degree of protection required by the rule of law in a democratic society [10].

Amann v. Switzerland. The case concerns the telephone call received by the applicant from the embassy of the former Soviet Union - to order a depilatory device which he was advertising - intercepted by the public prosecutor’s office, which asked the intelligence service to draw up a file on the applicant. The Court held that Article 8 of the Convention had been breached in the present case because the telephone call had been recorded, and that the same Article had been breached because the file had been created and kept, finding that such interference with the applicant’s right to respect for his private life was not provided for by law, since Swiss law was unclear as to the discretionary power of the authorities in this area.

Taylor-Sabori v United Kingdom. This case concerned the interception by the police, as part of a covert surveillance operation, of messages sent to the applicant’s pager. The Court ruled that Article 8 of the Convention had been violated in this case. Noting in particular that, at the time of the facts in question, there was no legal system governing the interception of pager messages transmitted via a private telecommunications system, it found, as the United Kingdom Government conceded, that the interference was not provided for by law [22].

Wisse v France. In this case, two applicants were arrested on suspicion of armed robbery and remanded in custody. Pursuant to an arrest warrant issued by the investigating judge, telephone conversations between them and their relatives to the speaker were recorded. The applicants’ request that the proceedings relating to the recording of their conversations be declared null and void was rejected. They argued that the recording of the conversations at the speaker constituted an interference with their right to respect for private and family life. The Court held that there had been a violation of Article 8 of the Convention in the present case, finding that French law did not indicate with sufficient clarity how and to what extent there was
a possibility of interference by the authorities in the private lives of detainees, nor the extent and manner of exercise of their discretion in the area in question. Consequently, the applicants did not enjoy the minimum degree of protection required by the rule of law in a democratic society. The Court observed, in particular, that the systematic recording of conversations with the speaker for purposes other than prison security deprived the speakers of their sole raison d’être, namely to enable persons deprived of their liberty to preserve to a certain degree their privacy, including the private nature of discussions with their families [25].

Kennedy v United Kingdom. Convicted of murder - in a controversial case because of missing and conflicting evidence - and released from prison in 1996, the claimant, suspecting that the police were intercepting his communications after he started a small business, complained to the Investigatory Powers Tribunal (IPT). He was finally informed in 2005 that no finding had been made in his favour in respect of the complaints made. This meant that his communications had not been intercepted or that the IPT considered any interception to be lawful. The IPT did not provide any further information. The complainant complained about the alleged interception of his communications. The Court held that there had been no violation of Article 8 of the Convention, finding that UK law on the interception of domestic communications, in conjunction with clarifications provided by the publication of a code of conduct, indicated with sufficient clarity the procedures for authorising and processing interception warrants, as well as the processing, communication and destruction of the data collected. In addition, there was no evidence of significant deficiencies in the application and functioning of the surveillance regime. Therefore, and in view of the safeguards against abuse in the proceedings, as well as the more general safeguards afforded by the Commissioner’s control and the IPT’s examination, the surveillance measures complained of, in so far as they could have been applied to the applicant, were justified under Article 8, paragraph 2 of the Convention [7].

Dragojevic v Croatia. This case mainly concerned secret surveillance of telephone conversations of a suspected drug trafficker. The applicant argued, in particular, that the investigating judge did not follow the procedure required by Croatian law to effectively assess whether the use of secret surveillance was necessary and justified in his particular situation. The Court held that Article 8 of the Convention had been breached in the present case. It found, in particular, that Croatian law, as interpreted by the national courts, did not provide reasonable clarity as to the discretionary powers of the authorities to order surveillance measures and did not in practice - as in the applicant’s case - provide sufficient safeguards against possible abuse [3]. A similar approach can be found in two other decisions of Croatian origin: Basic v Croatia [2] and Matanovic v Croatia [14].

The case of R.E. v. United Kingdom. The applicant, who was arrested and detained in Northern Ireland on three occasions in connection with the murder of a police officer, complained in particular about the regime of secret surveillance of consultations between prisoners and their lawyers and between vulnerable prisoners (mentally disordered persons) and „appropriate adults” (relative, guardian, or person with experience in dealing with mentally disordered persons). This case was examined in the light of the principles developed by the Court in the field of interception of telephone conversations between lawyer and client, which require stringent safeguards. The Court found that these principles must be applied to the secret surveillance of consultations between lawyer and client in a police station. In the present case, the Court ruled that Article 8 of the Convention had been violated with regard to the secret surveillance of legal consultations. It noted, in particular, that the guidelines providing for the safe handling,
storage and destruction of material evidence obtained under secret surveillance had been in place since 22 June 2010. However, at the time of the applicant’s detention in May 2010, those guidelines were not yet in force. The Court was therefore not convinced that the domestic law provisions in force at the time of the facts provided sufficient safeguards to protect the applicant’s consultations with his lawyer obtained under secret surveillance. The Court also held that there had been no breach of Article 8 in relation to the secret surveillance of consultations between persons deprived of their liberty and “appropriate adults”, finding in particular that they were not subject to professional secrecy and therefore a person deprived of liberty could not have the same expectation of privacy as in the case of a legal consultation. In addition, the Court was satisfied that the relevant domestic provisions, insofar as they related to the possible supervision of consultations between detainees and “appropriate adults”, were accompanied by adequate safeguards against abuse[18].

Roman Zakharov v. Russia, a case concerning the secret interception of mobile phone communications in Russia. The complainant, the editor-in-chief of a publishing house, complained in particular that mobile phone network operators in Russia were obliged by law to install equipment enabling law enforcement agencies to carry out operational investigative measures and that, without sufficient safeguards under Russian law, this allowed widespread interception of communications. The Court held that Article 8 of the Convention had been violated in the present case, finding that the Russian legal provisions governing the interception of communications did not provide adequate and effective safeguards against the arbitrariness and risks of abuse inherent in any system of covert surveillance, which was extremely high in a system such as that in Russia, where the secret services and the police had direct access, by technical means, to all mobile phone communications. In particular, the Court found shortcomings in the legal framework in the following areas: the circumstances under which public authorities in Russia are entitled to use secret surveillance measures; the duration of such measures, in particular the circumstances in which they should cease; the procedures for authorising interception, and the storage and destruction of intercepted data; the control of interception. In addition, the effectiveness of the remedies available to challenge the interception of communications was affected by the fact that they were only available to persons who could prove the interception and that obtaining such evidence was impossible in the absence of a system of notification or the possibility of having access to interception information [19].

Szabo and Vissy v Hungary. That case concerned Hungarian legislation on secret anti-terrorist surveillance, introduced in 2011. The applicants complained, in particular, that there was a possibility of being subject to unjustified and disproportionately intrusive measures in the Hungarian legal framework of secret surveillance for national security purposes [i.e. “Article 7/E (3) on surveillance”]. In particular, the applicants argued that this legal framework was prone to abuse, especially in the absence of judicial review. In the present case, the Court held that there had been a violation of Article 8 of the Convention. It accepted that it was a natural consequence of today’s forms of terrorism for governments to resort to state-of-the-art technology, including massive communications monitoring, to anticipate imminent incidents. However, the Court was not convinced that the legislation in question offered sufficient safeguards to prevent abuse. In particular, the scope of the measures could have included virtually anyone in Hungary, given the new technologies that allow the government to intercept large volumes of data even on persons outside the original scope
of the operation. On the other hand, such measures were ordered entirely by the executive, without any assessment of whether the interception of communications was strictly necessary and without any effective corrective measures, even judicial ones, being implemented. The Court further held that there had been no violation of Article 13 (right to an effective remedy) of the Convention in conjunction with Article 8 in the present case, reiterating that Article 13 cannot be interpreted as imposing a remedy against the state of domestic law [21].

Mustafa Sezgin Tanrikulu v. Turkey. The applicant complained about a domestic court's decision in 2005 to allow the interception of communications of any person in Turkey, including his own, for about one and a half months. He claimed, in particular, that the interception measures constituted an abuse of the national law in force at the time. He also stated that he had no effective remedy because the national authorities refused to investigate his complaints about the interception of his communications. The Court ruled that there had been a violation of Article 8 of the Convention, finding that the interception order in this case was not provided for by law. The Court also found a violation of Article 13 (right to an effective remedy) of the Convention [15].

With reference to the monitoring of computer use by employees, the ECtHR has issued two major judgments, one against Romania and one against France. In the case of Bărbulescu v. Romania, a private company's decision to dismiss an employee - the applicant - after monitoring his electronic communications and their content is concerned. The applicant complained that his employer's decision was based on a violation of his privacy and that the national courts had failed to protect his right to respect for his privacy and correspondence. The Grand Chamber of the Court ruled that there had been a violation of Article 8 of the Convention, finding that the Romanian authorities had failed to adequately protect the applicant's right to respect for his private life and correspondence. Consequently, they had failed to strike a fair balance between the interests at stake. In particular, the domestic courts failed to establish whether the applicant had received prior notice from his employer of the possibility that his communications might be monitored; they also failed to take into account the fact that the applicant had not been informed of the nature or extent of the monitoring, or of the extent of the monitoring of his privacy and correspondence. In addition, the national courts failed to establish, first, the specific reasons justifying the introduction of monitoring measures; second, whether the employer could have used fewer measures involving intrusion into the applicant's privacy and correspondence; third, whether those communications could have been accessed without the applicant's knowledge [1].

In the second case - Eric Libert v France - the applicant complains, in particular, of a breach of his right to respect for his private life resulting from the fact that his employer (the French national railway company, SNCF) opened files on the partition of his work computer's hard drive called „D:/personal data” without him being present. He was subsequently dismissed because of the contents of the files in question.

The Court communicated the application to the French Government and addressed questions to the parties under Article 8 (right to respect for private life) of the Convention [4].

With reference to voice samples, the ECtHR issues two important judgments.

First, we consider the case of P. G. and J. H. v. the United Kingdom, which concerns the recording of the applicants’ voices in a police station following their arrest on suspicion of having committed a robbery. The Court held that there had been a breach of Article 8 of the Convention in the present case in relation to the use of secret listening devices in the police
station. Noting in particular that, at the time of the facts, there was no formal system regulating the use of secret listening devices by the police at the police station, the Court found that the interference with the applicants’ right to privacy was not provided for by law. In this case, the Court also found that there had been a violation of Article 8 in view of the use of a secret listening device in an apartment and that there had been no violation of Article 8 in relation to obtaining information about the use of a telephone [17].

And secondly, in Vetter v France, following the discovery of the body of a person with gunshot wounds, the police, suspecting that the applicant had committed the murder, installed listening devices in an apartment he regularly visited. The Court held that there had been a violation of Article 8 of the Convention, finding that French law did not indicate with sufficient clarity the extent and manner of exercise of the authorities’ discretion in relation to the listening devices [24].

With reference to video surveillance, the ECtHR has concerned two cases originating in the UK and Germany. These are the case of Peck v UK [16] and the case of Kopke v Germany [9]. In the latter case, the applicant, a cashier in a supermarket, was dismissed without notice for theft following a covert video surveillance operation carried out by her employer with the assistance of a private detective agency. She unsuccessfully challenged the dismissal before the employment tribunals. Her complaint on constitutionality grounds was also rejected. The Court rejected the applicant’s complaint under Article 8 of the Convention as inadmissible (manifestly ill-founded). It concluded that the domestic authorities had maintained a fair balance between the employee’s right to respect for private life and her employer’s interest in protecting her property rights and the public interest in the proper administration of justice. The Court noted, however, that the competing interests involved might be given different weight in the future, given the extent to which intrusions into privacy have become possible thanks to new and increasingly sophisticated technologies [9].

In conclusion of the above, we come up with the following findings and recommendations for lawmakers and legal practitioners in the Republic of Moldova.

1. The basic idea, drawn from the study, is that the Moldovan authorities should adjust their legislation and practices to the standards set by the ECtHR and thus avoid possible condemnations by the European Court.

2. The study revealed the complexity of the cases handled by the European Court of Human Rights. The issue of personal data protection has been steadily gaining ground in judicial practice, especially in recent years.

3. Access to personal data remains the most vulnerable area for abuse by authorities or third parties. There is therefore a need for legal and institutional intervention to regulate data activity more effectively.

4. From the research carried out, we have concluded that a large part of the violations brought before the ECtHR are due to the defective application of national legislation by law enforcement bodies, especially the police. Therefore, we consider absolutely necessary a re-configuration of the whole architecture of operation with personal data by law enforcement institutions in the Republic of Moldova.

5. With the development of information technologies, the constant shift of social and legal relations from offline to online and the effective entry of the Internet into every home in the Republic of Moldova, there is a pressing need to reconceptualize the doctrine of human rights protection, extending it to the Internet.
Bibliography


**Presented:** 15 November 2021.

**E-mail:** tarna_alex@mail.ru