



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

SECOND SECTION

CASE OF ADOMAITIS v. LITHUANIA

(Application no. 14833/18)

JUDGMENT

Art 6 § 1 (civil) • Art 8 • Fair hearing • Private life • Interception of telephone communications during criminal intelligence investigation against prison director and use of that information in disciplinary proceedings leading to his dismissal • Effective access to court • Due examination of complaints by domestic courts • Decision-making procedure in compliance with requirements of adversarial proceedings and equality of arms • Adequate safeguards • Interference necessary and proportionate

STRASBOURG

18 January 2022

FINAL

18/04/2022

This judgment has become final under Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Adomaitis v. Lithuania,

The European Court of Human Rights (Second Section), sitting as a Chamber composed of:

Jon Fridrik Kjølbro, *President*,

Aleš Pejchal,

Valeriu Grițco,

Egidijus Kūris,

Branko Lubarda,

Pauliine Koskelo,

Marko Bošnjak, *judges*,

and Stanley Naismith, *Section Registrar*,

Having regard to:

the application (no. 14833/18) against the Republic of Lithuania, lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) by a Lithuanian national, Mr Virginijus Adomaitis (“the applicant”), on 23 March 2018;

the decision to give notice to the Lithuanian Government (“the Government”) of the complaints concerning whether the applicant had effective access to a court and whether his right to privacy was respected;

the parties’ observations;

Having deliberated in private on 23 November 2021,

Delivers the following judgment, which was adopted on that date:

INTRODUCTION

1. The case concerns the applicant’s complaints, under Article 6 § 1 and Article 13 of the Convention, that he did not have a fair hearing and was not able to challenge effectively the lawfulness of the interception of his telephone communications and the subsequent use of those materials, and his complaint, under Article 8 of the Convention, of a breach of his right to privacy.

THE FACTS

2. The applicant was born in 1968 and lives in the village of Pilviškiai, in the Vilkaviškis region. He was represented by Mr A. Kručauskas, a lawyer practising in Vilnius.

3. The Government were represented by their Agent, Ms K. Bubnytė-Širmenė.

4. The facts of the case, as submitted by the parties, may be summarised as follows.

I. BACKGROUND TO THE CASE

5. The applicant was the director of Kybartai prison.

6. On 22 June 2015 the Internal Affairs Division at the Department of Prisons (*Kalėjimų departamento Imuniteto skyrius*) opened a criminal intelligence investigation in respect of the applicant, on suspicion of abuse of office (Article 228 § 1 of the Criminal Code).

7. On 26 June 2015 a prosecutor of the Prosecutor General's Office, acting on the basis of the criminal intelligence information received that month from the Department of Prisons, asked the Vilnius Regional Court to authorise the interception of the applicant's electronic communications. The prosecutor based the request on the above-mentioned information which showed that the applicant might have abused his office: it was suspected that he had provided, for pay, better conditions for inmates while they were serving their sentences, and that he had also awarded them incentives (*paskatinimus*). The prosecutor noted that, before asking for authorisation for the interception, other investigative measures had been taken, but that, given in addition the specific features of applicant's post, they had been insufficient to investigate possible criminal activity. In support of his request, the prosecutor referred to two reports by the Department of Prisons, both of 22 June 2015.

8. By ruling of 30 June 2015 the Vilnius Regional Court granted the prosecutor's request on the basis of the Law on Criminal Intelligence (see paragraph 47 below) and allowed, for an initial period of three months, the interception of the applicant's telephone and other communications, in order to investigate his possible abuse of office. The court noted that the material in the file – criminal intelligence reports – confirmed the applicant's possible involvement in criminal activity of medium severity, and that other criminal intelligence measures had already been used, which justified authorising the interception. The authorisation was extended by further orders of the Vilnius Regional Court of 29 September and 22 December 2015, and 29 March 2016. Each time the court based the extension on specific information provided to it – transcripts of concrete and numerous newly intercepted telephone conversations of the applicant, where, among other elements, payment for the applicant's specific actions was mentioned. Those transcripts had been produced by the Department of Prisons in its motions to the prosecutor, who, in turn, referred to that information when asking the court that the authorisation for interception be extended.

9. Between June 2015 and June 2016 the Internal Affairs Division of the Department of Prisons placed covert listening devices in the applicant's office in the prison. During that period, his telephone communications were monitored and intercepted.

10. On 23 June 2016 the criminal intelligence investigation was discontinued for lack of incriminating evidence to charge the applicant under Article 228 § 1 of the Criminal Code.

That notwithstanding, the prosecutor permitted the use of the collected information in disciplinary proceedings, which ultimately led to the applicant's dismissal (see paragraphs 25-45 below).

11. In the meantime, the applicant sought to obtain the information gathered against him during the secret surveillance. He also contested the lawfulness of the relevant measure.

II. THE PROCEEDINGS REGARDING ACCESS TO INFORMATION IN THE CRIMINAL INTELLIGENCE FILE AND REGARDING THE LAWFULNESS OF THE CRIMINAL INTELLIGENCE MEASURES

A. As to access to information

12. By a ruling of 16 March 2017, the Vilnius Regional Court, in a public hearing in which the applicant's lawyer and a representative from the Ministry of Justice (which oversees the Department of Prisons) took part, granted the applicant's request and ordered the Department of Prisons to provide the applicant with the information about him that had been gathered during the criminal intelligence investigation. The court observed that information could be disclosed only inasmuch as the law allowed, and in compliance with restrictions set out in Article 19 § 7 of the Law on Criminal Intelligence (see paragraph 47 below).

13. In compliance with that court decision, on 27 March 2017 the Department of Prisons provided the applicant with two declassified reports (*pažymos*) from the criminal investigation file. The Department noted that it had received a prosecutor's permission to use that information for investigation of the applicant's disciplinary offences (see paragraph 25 below). The first report consisted of eleven pages and included analysis of the applicant's actions in organising the prison's internal competitions, entering into mobile telephone contracts and using the prison car for personal purposes, as well as other offences. The second report contained fifty-four pages of transcripts of the applicant's intercepted telephone conversations.

The Department of Prisons noted that other information, such as that linked to measures, methods or tactics of criminal intelligence, and individuals who had performed those actions, could not be revealed, under Article 19 § 7 of the Law on Criminal Intelligence (see paragraph 47 below).

14. On the basis of its earlier ruling (see paragraph 12 above), on 29 November 2017 the Vilnius Regional Court issued a writ of execution, ordering the Department of Prisons to "disclose" to the applicant the information gathered about him during the criminal intelligence investigation.

15. By a letter of 21 December 2017, the Department of Prisons informed the applicant that it had “repeatedly” sent him and his lawyer two reports (see paragraph 13 above), the Vilnius Regional Court’s rulings authorising the interception of the applicant’s telephone communications (see paragraph 8 above), and certain other documents regarding the declassification of those materials, in total eighty-four pages of documents. The Department wrote that, following the court order for disclosure, it was providing the applicant with “all” the criminal intelligence investigation information gathered about him, except for the information which could not be disclosed pursuant to Article 19 § 7 of the Law on Criminal Intelligence, which point had been emphasised by the Vilnius Regional Court (see paragraph 12 above).

16. According to the Government, in January 2018 the applicant requested, through a bailiff, that the Department of Prisons be ordered to provide certain other documents, such as those relating to a secret entering of the applicant’s office and the placement of covert listening devices, those documents having been mentioned in the documents that had already been made available to the applicant. In February 2018 the Department refused to release that information, referring to Article 19 § 7 of the Law on Criminal Intelligence, on the ground that those documents contained specific information about listening devices, their installation and dismantlement, and information about the identities of secret participants in the criminal intelligence investigation. The Department also informed the bailiff about that refusal.

17. According to the Government, neither the applicant nor his lawyer submitted any further requests to the bailiff regarding the execution of the Vilnius Regional Court’s ruling of 16 March 2017, and on 24 April 2018 the bailiff confirmed that the execution of that court decision had been fully completed. Neither the applicant nor his lawyer complained about the bailiff’s actions.

B. The decisions regarding the lawfulness of the criminal intelligence measures applied to the applicant

18. The applicant lodged a complaint regarding the lawfulness of the criminal intelligence investigation, and the alleged breach of his rights and freedoms. On 4 August 2017 that complaint was dismissed by the Prosecutor General’s Office. The prosecutor noted that he had obtained and examined the materials in the criminal investigation file. As noted by the prosecutor, given that some of the documents, or parts of the documents, in that file had been marked as “restricted use”, in the decision he would refer only to information which was either not classified or which had been declassified. The prosecutor thus referred to a number of particular documents of 2015 and 2016, such as requests for the interception of the applicant’s telephone communications, lodged by the Department of Prisons and the Prosecutor

General's Office, and the authorising decisions by the Vilnius Regional Court. The prosecutor observed that, prior to authorising the interception of the applicant's telephone communications, other methods had been used to try to establish possible criminal acts: information had been collected about the inmates and other persons with whom the applicant maintained contact, and about incentives and other privileges awarded to inmates. On the facts it had been found that, by calling the applicant from unlawfully owned mobile telephones, the inmates would not only solve their own issues, but also act as intermediaries to solve other inmates' problems. The applicant would meet the inmates' relatives in his office at Kybartai prison or in secret locations in town. Although the applicant contended that the criminal intelligence investigation had been opened in connection with his unlawful actions in organising internal competitions, in reality it had been commenced on the basis of information about the applicant awarding incentives to inmates in exchange for remuneration.

19. In the light of the above, the prosecutor held that the criminal intelligence investigation had been opened and performed reasonably and lawfully. Its duration had been determined by the need to verify and assess the information collected. The prosecutor also considered that the information gathered during the criminal intelligence investigation had been (lawfully) used to examine the applicant's disciplinary offences or misconduct in office, in compliance with the requirements of the Law on Criminal Intelligence.

20. By a ruling of 4 September 2017 ordering the Department of Prisons to provide it with the criminal intelligence materials, and, afterwards, by a ruling of 25 September 2017, adopted in written proceedings, notwithstanding the applicant's request that a hearing be held, the Vilnius Regional Court dismissed an appeal by the applicant against the prosecutor's decision. The court pointed out that, under Article 5 § 9 of the Law on Criminal Intelligence, a person had a right to challenge criminal intelligence measures, should he or she consider that those measures had breached his or her rights (see paragraph 47 below). Such complaints were amenable to appeal at two stages – an appeal could be made to the prosecutor and then to the court. The court also observed that the applicant had not explained which particular freedoms or rights had been breached by the criminal intelligence measures. Even so, it appeared from the applicant's arguments that the complaint was linked to his dismissal from work. For the court, in the proceedings at hand it had jurisdiction to examine only questions relating to the duration of the criminal intelligence measures and their proportionality. Any arguments regarding whether information obtained by employing criminal intelligence measures could be used when examining disciplinary offences should be examined in different court proceedings regarding that disciplinary offence.

21. On the merits, the Vilnius Regional Court specified that on 20 May 2015 the Department of Prisons had received information about the applicant

providing better living conditions for inmates in exchange for payment, and also awarding them incentives. That information had contained elements of the crime of abuse of office. It had included details of one particular inmate who had been given better conditions and incentives; that information had already been known about before the opening of the criminal intelligence investigation. Once the investigation had been opened, but before the authorisation of the interception of the applicant's telephone communications, information about disciplinary penalties and incentives in respect of the inmates had been received, and that information supported the suspicions against the applicant. A criminal intelligence measure – the interception of the applicant's electronic communications – had then been authorised by the court. That authorisation had been extended several times by the court, the interception lasting for twelve months altogether, that being the maximum term allowed under the Law on Criminal Intelligence. Accordingly, neither the time-limit for the above-mentioned measure, nor the rules for its authorisation – by a court decision – had been breached. The court noted that “it had acquainted itself with the criminal intelligence investigation file”. The criminal intelligence investigation had been intensive, information had not only been gathered by intercepting the applicant's telephone communications, and the new information obtained was being verified in various ways, and would prove to be true. The Vilnius Regional Court also specifically noted that during the first three-month period when the technical measures had been applied, “another event” (*kitas įvykis*), having the features of the crime of abuse of office, had been established. That “new event” had been referred to in the prosecutor's request to the court to extend the interception measure. Similarly, during the first and the second extensions, the Department of Prisons had referred to “new concrete events”, and that information had likewise been relied on by the prosecutor when asking to extend the authorisation of the interception. There had not been a single extension in respect of which there had been no new information received about the applicant's possible criminal acts (see also paragraph 8 above). It was understandable that at the time when the criminal intelligence investigation started and the interception had been authorised, there had not been much information about the possible unlawful activity; however, with each extension of the interception period, the amount of such information should have become greater, which had been the case.

22. Given the applicant's place of work and his position – he was the director of a prison – the interception of his electronic communications had been a proportionate measure. Specifically, the State and society had an interest in having inmates following the letter of the law. The information which had prompted the criminal investigation showed that the applicant used to award unwarranted incentives to the inmates, thus portraying them positively, without merit. Those actions by the applicant posed a clear and present danger to society, as those inmates could use the incentives in order

to be released from prison early. Furthermore, the applicant's work in an inaccessible and protected incarceration facility had significantly restricted the means for the criminal intelligence investigation, which made recourse to such technical means as interception of the applicant's electronic communications reasonable and proportionate. The applicant's actions had elements of corruption-related criminal acts, and uncovering such crimes was always complicated on account of the perpetrators' conspiratorial tendencies, their interest in not being detected, and, in this particular case, the applicant's specific knowledge of criminal intelligence means and methods, and his knowledge of how to counter them.

23. Lastly, the Vilnius Regional Court noted that in his complaint the applicant did not demonstrate any possible connection between the court orders authorising the interception of his electronic communications and a breach of his right to respect for his private life. There had been no breach of the applicant's right to respect for his private life on account of those court orders.

C. The list of documents provided to the applicant, as specified by the Government

24. As specified by the Government, the applicant was provided with the following documents relating to the criminal intelligence measures.

As early as in 2016 he had been provided with the materials gathered when his telephone communications were intercepted, as part of his disciplinary investigation file. At his request, he had again been given those documents in March and December 2017. During the court proceedings regarding the disciplinary penalties, those documents had again been given to him in November 2016 and in January 2017. In addition, in April 2017 the applicant had been provided with all of the procedural documents, such as partly declassified applications by the Prosecutor General's Office and partly declassified court decisions, which stated the legal and factual grounds for asking for authorisation for the interception of his telephone communications, the scope of the criminal intelligence measures, and their duration. At the applicant's request, the same documents had again been provided to him in March 2020, during the court proceedings concerning the disciplinary penalties. In addition, in January 2018, at the applicant's request, the Department of Prisons had provided him with all of its applications for the interception of his telephone communications; the same documents had again been provided to the applicant in March 2020, during the court proceedings concerning the disciplinary penalties. He had also been provided that month with the entirely declassified letter no. SD-141RN of 22 June 2016, whereby the Prosecutor General's Office had consented to the use of criminal intelligence information in the disciplinary proceedings against the applicant (see paragraph 25 below).

Additionally, at the applicant's request, during the court proceedings concerning the disciplinary penalties, in September 2020 the Department of Prisons and the Prosecutor General's Office partly declassified and made available to the applicant their applications and the decisions regarding secret entry into the applicant's office to place and use covert listening devices therein, and regarding surveillance of the applicant. In October 2020 the applicant was also given partly declassified rulings of the Vilnius Regional Court, of November 2015 and March 2016, authorising secret entry into the applicant's offices, and his surveillance.

III. THE APPLICANT'S DISMISSAL ON DISCIPLINARY GROUNDS AND RELATED COURT PROCEEDINGS

A. The applicant's dismissal

25. On the basis of a request by the Department of Prisons, referring to Article 19 § 3 of the Law on Criminal Intelligence, on 22 June 2016 by decision no. SD-141RN, the Prosecutor General's Office consented that information gathered during the criminal intelligence investigation could be used when investigating the applicant's disciplinary offences or misconduct in office.

26. On 10 August 2016 the Department of Prisons provided the Ministry of Justice with the materials gathered during the criminal intelligence investigation for the purpose of the examination of applicant's disciplinary liability. Those materials have been declassified by the Department of Prisons, the Prosecutor General's Office and the Vilnius Regional Court (each institution having declassified its own documents).

27. On 26 September 2016, by a decision of the Minister of Justice, the applicant received a disciplinary penalty – a strict reprimand. It was established that in 2015 he had organised competitions for several posts at Kybartai prison and had given unlawful orders to his subordinates so that individuals close to him would win those competitions. Among other things, the applicant had demanded that some other individuals should not take part in those competitions and had set up certain requirements so that a person close to him would qualify. Those actions by the applicant were characterised as unethical, and as constituting a gross disciplinary offence (*šiurkštus tarnybinis nusižengimas*) and abuse of office.

28. Additionally, on 3 November 2016, by a decision of the Minister of Justice, the applicant received another disciplinary penalty – dismissal from service. It was established that in 2014 he had, in his capacity as the director of Kybartai prison, without public procurement signed a contract with a telecommunications company and obtained four mobile telephone numbers which he had then given to individuals close to him for their use. In addition, he had used the prison car for personal purposes, and had given the driver of

the prison car unlawful orders. All this constituted a gross breach of numerous legal regulations concerning ethics and the adjustment of private and public interests in public service, and amounted to an abuse of office.

29. The applicant contested both decisions in court.

B. Administrative court proceedings regarding the lawfulness of the use of criminal intelligence information and the lawfulness and proportionality of the applicant's dismissal

1. The Vilnius Regional Administrative Court

30. On 3 November 2016 the Vilnius Regional Administrative Court accepted the applicant's lawsuit for examination. The court ordered the Ministry of Justice to provide a response to the applicant's lawsuit and to provide "all materials they possessed" on which the Ministry's findings regarding the applicant's disciplinary offence had been based. The Ministry of Justice complied, providing the court with a number of documents, such as three criminal intelligence reports from August 2016 by the Department of Prisons (twenty-three, fourteen and nineteen pages), the Department of Prisons report from July 2016 (sixty-five pages), statements of witnesses who had worked at Kybartai prison, and other documents.

On 28 November 2016 the Vilnius Regional Court forwarded the Ministry's reply, as well as the above-mentioned supporting documents to the applicant, for information.

31. The administrative court proceedings were subsequently suspended until 20 December 2018, until another linked complaint by the applicant, regarding a disciplinary penalty – a reprimand received previously for releasing certain prisoners without valid court orders or while the court orders were not yet in force – was over. Those proceedings ended with a final ruling of the Supreme Administrative Court of 14 November 2018, in which the reprimand was upheld.

32. At the applicant's request, on 9 April 2019 the Vilnius Regional Court again suspended the proceedings until the Constitutional Court had given a ruling in a case which concerned an analogous legal measure (see paragraph 50 below). The administrative court proceedings resumed on 2 May 2019, after the Constitutional Court had delivered its ruling of 18 April 2019.

33. As it transpires from the documents submitted by the parties, by a decision of 3 March 2020 the Vilnius Regional Administrative Court, on the basis of the applicant's lawyer's request of 25 February 2020, ordered the Department of Prisons to provide the following documents: 1. the letters of the Department to the Prosecutor General's Office, asking for the authorisation and the extension of the criminal intelligence measures; 2. the prosecutor's corresponding applications to the court; 3. the court's decisions authorising and extending the interception of the applicant's

communications; 4. the Department's request for the prosecutor's consent to use the collected information in the disciplinary proceedings; 5. the prosecutor's consent; 6. the decisions to declassify the materials listed in points 1-3 above. Complying with the court order, the Department provided that court with those documents (thirty-eight pages).

As submitted by the Government, during the court proceedings concerning the disciplinary penalties, both the applicant's lawyer and the applicant had become familiar with the above-mentioned documents (they were in possession of all that information contained in the above-mentioned documents in 2016-2018).

34. On 18 March 2020 the Prosecutor General's Office also provided the Vilnius Regional Administrative Court with a copy of its letter of 22 June 2016, whereby it had consented to information gathered during the criminal intelligence investigation being used in the disciplinary proceedings.

35. On 30 October 2020 the Vilnius Regional Administrative Court wrote to the Ministry of Justice and the applicant, asking whether, in the light of the extreme health situation in the country, they would not object if the case was heard by means of written proceedings. Both parties agreed.

36. By a ruling of 22 December 2020, in written proceedings, the Vilnius Regional Administrative Court dismissed the applicant's complaint. The court referred to the ruling of the Constitutional Court of 18 April 2019 (see paragraph 50 below), and observed that, when deciding a case wherein the unlawfulness of an official's actions was proved by information obtained during a criminal intelligence investigation, the court should examine each time whether the information had been obtained without breaching the law and whether it had been reasonable to use it when investigating disciplinary offences.

37. On the facts, the court established that on 15 June 2016, on the basis of Article 19 § 3 of the Law on Criminal Intelligence, the Department of Prisons had requested the Prosecutor General's Office to allow the use of the information obtained through criminal intelligence measures when investigating the applicant's disciplinary offences; that request had been granted. Between June and August 2016, those criminal intelligence investigation materials had therefore been declassified and transferred to the Ministry of Justice, which oversees the Department.

38. As to the applicant's arguments concerning the lawfulness and proportionality of the criminal intelligence measures, those had already been examined by a court in another set of proceedings, where no breach of the law had been found (see paragraphs 18-23 above). For the administrative court, there was no information in the file that required it to hold that the criminal intelligence institutions' actions, when gathering information which had been used to examine the disciplinary offences, would not have complied with the law. It was also of relevance that the measures had been taken after a corruption-related crime had been suspected. The fact that no criminal

investigation had been opened in respect of the applicant did not, in and of itself, make the use of the criminal intelligence materials unlawful, given that those materials could be used to investigate corruption-related disciplinary offences. In that context, Article 2 § 13 of the Law on State Service was pertinent (see paragraph 48 below). It followed that the materials gathered had been declassified and used in the disciplinary proceedings in compliance with the requirements of Article 19 § 3 of the Law on Criminal Intelligence.

39. On the facts, the administrative court held that both disciplinary offences had been established correctly. Regarding the first disciplinary offence, it had been established on the basis of nine witnesses' testimony, and the content of the applicant's intercepted telephone conversations, which he had not denied. Regarding the second disciplinary offence, that was proven by documents, namely contracts with the telecommunications company, the applicant's entries in the car travel records, and his telephone conversations. The disciplinary penalty of dismissal from work had been imposed on the applicant appropriately, as he had committed two gross disciplinary offences, for which Article 29 § 4 of the Law on State Service provided for dismissal from service (see paragraph 48 below). In the court's view, as the director of Kybartai prison, the applicant had been its [senior] manager, and higher requirements to observe the law applied to him. He had to lead by example, within and outside the service. The disciplinary offences had been committed by the applicant intentionally. His actions discredited the system of the execution of sentences, reduced society's respect for State institutions and officials, and gave the impression that State officials could breach the law and use State property for personal gain.

40. Lastly, the administrative court held that there was no basis on which to rule that the criminal investigation measures had been disproportionate, as no information had been provided to show that any serious restrictions of the applicant's personal rights and freedoms had taken place.

2. The Supreme Administrative Court

41. By a final ruling of 29 April 2021, in written proceedings, the Supreme Administrative Court dismissed an appeal by the applicant. The court noted that both the Ministry of Justice, and the first instance court, when examining the disciplinary offences committed by the applicant, had relied on declassified information obtained through the criminal intelligence measures. The disciplinary offences committed by the applicant had been established on the basis of the entirety of the evidence, and not only on the basis of information obtained through secret surveillance. The first instance court had in particular precisely examined and assessed the lawfulness, reliability and proportionality of the use of the information gathered during the surveillance as evidence, which had later been declassified and had been provided for the investigation of a disciplinary offence. This was in compliance with paragraphs 86.3 and 86.3.1. of the Constitutional Court's

ruling of 18 April 2019 (see paragraph 50 below). Furthermore, the applicant had had an opportunity to put forward his arguments regarding the lawfulness, reliability and proportionality of the use of that information. As noted by the Constitutional Court, Article 19 § 3 of the Law on Criminal Intelligence permitted the use of information obtained through criminal intelligence to investigate corruption-related disciplinary offences. This had been the situation in the applicant's case, as it stemmed from Article 2 § 13 of the Law on State Service. Both the Ministry of Justice and the first instance court had therefore reasonably relied on declassified criminal intelligence information.

42. The Supreme Administrative Court also noted that by a final ruling of 25 September 2017, the applicant's arguments regarding the alleged unlawfulness of the criminal intelligence actions had been rejected (see paragraphs 20-23 above). It had to be emphasised that within that (second) set of administrative court proceedings the applicant had not contested the reliability of the information collected during the disciplinary investigations.

43. Given the applicant's duties – he had been the manager of an institution – and the offences which he had committed, the use of declassified information when examining those offences had been necessary in a democratic society, and had pursued a legitimate aim of guaranteeing transparency and openness in public service and prevention of the abuse of State office. The use of such information for the investigation of disciplinary offences had also been proportionate. The law set a higher disciplinary and moral standard for officials compared with other persons, and those officials' behaviour when in service should not give rise to doubts about their meeting both the norms of general ethics and service-related ethics. Actions that contradicted the aims of statutory institutions (*statutinės institucijos*) were not acceptable. Use of information thus obtained was a proportionate measure to guarantee the effectiveness of law enforcement institutions.

44. On the entirety of the evidence, the court concluded that the applicant had committed two gross disciplinary offences. Given his position as the manager of an incarceration institution, he had clearly shown an inappropriate example to his employees, and acted for personal gain. His dismissal had therefore been an appropriate measure.

45. The Supreme Administrative Court lastly found that in his appeal, the applicant had not provided any reasoned legal arguments as to why the forwarding of the criminal investigation materials to the Ministry of Justice, for the investigation of disciplinary offences, had restricted his right to respect for his private life under Article 8 of the Convention.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

46. The Constitution reads:

Article 22

“Private life shall be inviolable.

Personal correspondence, telephone conversations, telegraph messages, and other communications shall be inviolable.

Information concerning the private life of a person may be collected only upon a justified court decision and only according to the law.

The law and the courts shall protect everyone from arbitrary or unlawful interference with his or her private and family life, as well as from encroachment upon his or her honour and dignity.”

Article 25

“... Citizens shall have the right to receive, according to the procedure established by law, any information held about them by State institutions.”

Article 33

“Citizens shall have the right to ... enter on equal terms the State Service of the Republic of Lithuania ...”

47. The Law on Criminal Intelligence (*Kriminalinės žvalgybos įstatymas*), in force as of 1 January 2013, read as follows at the material time:

Article 5. Protection of human rights and freedoms when conducting criminal intelligence

“1. Human rights and freedoms must not be violated during the conduct of criminal intelligence measures. Individual limitations on human rights and freedoms must be temporary and apply only in the manner prescribed by law in order to protect the rights and freedoms, as well as property, of other persons, and public and national security.

...

6. At the request of a person who has been subjected to criminal intelligence measures, but where the information received has not been confirmed and no pre-trial investigation has been opened, but [as a result of criminal intelligence measures], the person has experienced negative legal consequences, the information collected about him or her when conducting criminal intelligence, except the information specified in Article 19 § 7 of this Law, must be provided.

...

9. A person who considers that the actions of criminal intelligence entities have violated his or her rights and freedoms may lodge an appeal against their actions with the head of the principal criminal intelligence institution or the prosecutor ... , [and] may lodge an appeal against decisions of the latter to the president of the regional court or a judge authorised by him or her ...”

Article 8. The grounds for a criminal intelligence investigation

“1. A criminal intelligence investigation shall be performed when:

1) there is information about a very serious or serious crime that is being prepared, is being committed, or has been committed, or about crimes of medium severity referred to in Article ... 228 § 1 ... of the Criminal Code [abuse of office], or about those who are preparing, are committing, or have committed such acts,

...

3. If, during the conduct or completion of a criminal intelligence investigation, the characteristics of a criminal act are detected, a pre-trial investigation shall be initiated immediately ...”

Article 19. The Use of Criminal Intelligence Information

“1. Criminal intelligence information may be used in the following cases:

1) to carry out criminal intelligence tasks;

...

3) in providing information about a person in accordance with the procedure established in the Republic of Lithuania’s Law on the Prevention of Corruption.

...

3. Criminal intelligence information about an act with the characteristics of a corruption criminal act may, with the consent of the prosecutor, be declassified by decision of the head of the principal criminal intelligence institution and be used in an investigation into a disciplinary offence and/or misconduct in office.

...

7. The following information shall not be provided: detailed information about the methods and means of collecting criminal intelligence information, tactics concerning the application of the methods by which criminal intelligence information is collected and the identity of secret participants in criminal intelligence, and detailed information on the quantitative and personal composition of these participants.”

48. The Law on State Service (*Valstybės tarnybos įstatymas*) read as follows at the relevant time:

Article 2. Definitions

“13. “Abuse of office” (*Piktnaudžiavimas tarnyba*) means an act (act or omission) by a civil servant where his or her official position is used not in the interests of the service or in accordance with laws or other legal acts, or is used for self-interest (misappropriation of another’s property, funds, and so on, or unlawful transfer thereof to other persons) or for other personal reasons (revenge, envy, self-advancement, unlawful provision of services and so on), also any actions of the civil servant exceeding the powers conferred on him or her, or any wilful acts.”

Article 29. Disciplinary penalties

“4. Dismissal from office may be imposed as a disciplinary penalty for a gross disciplinary offence and for any other disciplinary offence where the civil servant has received a strict reprimand at least once over the past twelve months.

5. Serious misconduct in office shall mean misconduct which results in a serious breach of the laws or other regulatory provisions governing the civil service and the activities of civil servants, or which adversely affects the duties of a civil servant or the principles of ethics for civil servants' conduct.

6. The following shall be considered as serious official misconduct:

1) the conduct of a civil servant, as related to the performance of official duties, which discredits the civil service, degrades human dignity or other actions which directly violate the constitutional rights of people;

...

3) criminal acts of a corrupt nature, as defined in the Law on Prevention of Corruption, related to the performance of the official's duties, even if the act did not incur criminal or administrative liability for the civil servant concerned;

4) abuse of office and non-compliance with the requirements of the Law on the Coordination of Public and Private Interests in the Civil Service."

49. The Law on Prevention of Corruption (*Korupcijos prevencijos įstatymas*) read as follows at the material time:

Article 2. Main definitions

"2. "Corruption offences" (*Korupcinio pobūdžio nusikalstamos veikos*) means the acceptance of a bribe, influence peddling, other criminal acts committed in the public administration sector or when providing public services with a view to seeking personal gain or gain for other persons: abuse of office or misuse of powers, abuse of authority, forgery of documents and measuring devices, fraud, appropriation or embezzlement, disclosure of an official secret or a commercial secret, incorrect income, profit or assets statements, money or asset laundering, interfering with the activities of a civil servant or a person carrying out public administration functions, and other criminal acts aimed at seeking or soliciting a bribe or subornation, or concealing or disguising the acceptance or giving of a bribe or subornation."

50. By a ruling of 18 April 2019, on the compliance of the provisions of the Law on Criminal Intelligence, the Law on State Service and of the Statute of Internal Service with the Constitution, the Constitutional Court held:

"86.3.1. It has ... been mentioned that, under the Constitution, ... a court (judge), when administering justice and settling a dispute concerning the imposition of an official penalty, must, on a case-by-case basis, fully assess all the material, data, or information used in investigating the misconduct in office, and must decide whether, *inter alia*, information about a person that has been collected secretly in the manner established by law, declassified in accordance with the procedure laid down in legal acts, and transmitted for use for the purposes of the investigation of the misconduct in office by the person in question, can be considered evidence in a concrete case, whether such information complies with requirements for the lawfulness and credibility of evidence, and whether such use is necessary in a democratic society when the State seeks to attain certain legitimate aims, such as to ensure the transparency and openness of State service, as well as to prevent corruption and acts of a corrupt nature in State service; the court (judge) must also assess, in each case, whether the use of the information in question for the purposes of investigating misconduct in office of a corrupt nature is in line with the principle of proportionality, and whether the said legitimate aims could be achieved in a particular case by other less restrictive means.

86.7.

...

Thus ... it should be held that a State servant or official about whom information has been collected secretly in accordance with the procedure established by the Law on Criminal Intelligence, after such information has been used in investigating misconduct in office of a corrupt nature committed by him or her, has the right, under Paragraph 9 of Article 5 of the Law on Criminal Intelligence, to apply to the court (judge) referred to in this paragraph and raise questions of the legitimacy, necessity, and proportionality of the use of such declassified information, as well as challenge the admissibility of such information as evidence. As mentioned above, under the Constitution, a person must be afforded effective protection against the possible arbitrariness of public authorities, namely an opportunity to apply to a court and to lodge an appeal against the lawfulness, reasonableness, and proportionality of the collection of the criminal intelligence in question about him or her and of the transmission of that information under Paragraph 3 of Article 19 of the Law on Criminal Intelligence for the purposes of investigating misconduct in office of a corrupt nature.”

51. As summed up by the Constitutional Court, in the above-mentioned ruling it held that the legal measure, consolidated in Article 19 § 3 of the Law on Criminal Intelligence, pursuant to which criminal intelligence information could be declassified and used only for the purposes of the investigation of misconduct in office which had the characteristics of a corruption-related criminal act, for the commission of which a State servant or official faced the risk of the most severe official penalty being imposed – dismissal from the position in State service – was justified by constitutionally important objectives, such as ensuring the proper functioning of State service, its transparency and openness, and preventing corruption and acts of a corrupt nature in State service. This was a necessary and proportionate measure in a democratic society in order to achieve the objective of official liability in accordance with the Constitution, that is, to create preconditions for the proper application of official liability as a public form of control over servants or officials of a democratic State and for their accountability to society, for acts that were incompatible with the requirements, arising from the Constitution, of State service as a system and for State servants or officials. After providing for the possibility of declassifying criminal intelligence information relating to an act which had the characteristics of a corruption-related criminal act and using it for the investigation of misconduct in office of a corrupt nature, the right to the protection of private life, enshrined in Article 22 of the Constitution, and the right to enter State service, enshrined in Paragraph 1 of Article 33 thereof, were not restricted more than was permitted by the Constitution, since the essence of those rights had not been denied.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 6 § 1 OF THE CONVENTION

52. The applicant complained of a lack of access to the materials from the secret surveillance against him, those materials having served as the basis for his dismissal from service. He also maintained that there was a lack of a proper and precise legal framework indicating how information gathered when employing criminal intelligence actions could be used and its lawfulness contested.

53. Although in support of his complaints the applicant relied on both Article 6 § 1 and Article 13 of the Convention, the Court, being the master of the characterisation to be given in law to the facts of the case (see *Radomilja and Others v. Croatia* [GC], nos. 37685/10 and 22768/12, § 126, 20 March 2018), finds that the essence of the applicant's grievance is related to the fairness of the court proceedings concerning the lawfulness of the surveillance against him and those regarding his dismissal from service. The complaint thus falls to be examined under Article 6 § 1 of the Convention alone, which is the special norm *vis-à-vis* Article 13 (see also, *mutatis mutandis*, *Airey v. Ireland*, 9 October 1979, § 35, Series A no. 32), and, in so far as is relevant, reads as follows:

“In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair ... hearing ... by [a] ... tribunal ...”

A. Admissibility

1. The submissions by the parties

54. In their initial observations of 6 November 2020 and 9 February 2021, the Government argued that, having regard to the fact that the domestic judicial proceedings concerning the disciplinary penalties were still pending, it would be premature for the Court to deal with the applicant's complaints under Articles 6 and/or 13 and Article 8 of the Convention.

55. The Government also submitted that the applicant's conduct had been contrary to the purpose of the right of individual application. In support of this suggestion, they firstly appeared to argue that, although in his application of 23 March 2018 the applicant had complained to the Court that he had not received all the criminal intelligence information about the interception of his telephone communications in a timely manner, that information had been provided to him by the Department of Prisons as early as April 2017 (see paragraph 24 above). Secondly, the applicant had not informed the Court about any of the developments in the court proceedings about his disciplinary penalties, or about the fact that during those administrative proceedings he had received all the declassified documents regarding the criminal intelligence actions, even documents regarding secret entering of his office,

which went beyond the scope of the applicant's disciplinary liability (see paragraph 24 *in fine* above). The Government thus contended that the application should be rejected as an abuse of the right of application.

56. Lastly, on 21 May 2021 the Government informed the Court about the Supreme Administrative Court's ruling of 29 April 2021 (see paragraphs 41-45 above), and considered that the applicant had had access to an effective remedy and a fair hearing, as required by Article 6 and/or Article 13 of the Convention.

57. The applicant did not comment.

2. *The Court's assessment*

58. The Court considers that the Government's arguments regarding the timing and the amount of the criminal intelligence information disclosed to the applicant are intrinsically linked to the merits of his complaint that he did not have a fair hearing regarding his complaints of unlawful surveillance and his complaints about his dismissal. Furthermore, given the fact that both the applicant and the Government have been asked to inform the Court about the outcome of the pending litigation regarding the disciplinary penalties in respect of the applicant, the Court is not ready to find that the fact that it was the Government which sent the Court a copy of the Supreme Administrative Court's ruling of 29 April 2021, and not the applicant, in and of itself means the applicant's conduct amounted to an abuse of the right of application. Likewise, even if the Government argued that the applicant had received some or all of those previously classified documents, the fact remains that the court proceedings regarding the disciplinary penalties ended by a final court decision only on 29 April 2021, and it was only in those proceedings that the court examined the applicant's grievances regarding the lawfulness and proportionality of the use of those documents during the disciplinary proceedings. The Court therefore cannot hold that the applicant can be regarded as having abused the right of application.

59. The Court finds that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. *The submissions by the parties*

(a) **The applicant**

60. The applicant complained that he had not been able to see in a timely manner the materials from the secret surveillance against him, although those materials had ultimately led to his dismissal, and notwithstanding the fact that State institutions had had access to that information. The applicant argued

that there was a lack of a precise and proper legal framework indicating how information collected through criminal intelligence actions could be used and how its lawfulness could be contested.

61. The applicant also argued that although under Article 5 § 9 of the Law on Criminal Intelligence it was possible to complain about a breach of rights in connection with criminal intelligence actions, in the applicant's case his complaints had been examined by the prosecutor, and then the Vilnius Regional Court only formally, in written proceedings, without making statements about specific criminal intelligence material. As a result, he had not been able to see the criminal intelligence materials or make statements in court. That process had not been fair and had not effectively protected his rights.

(b) The Government

62. In their initial observations of 6 November 2020 and 9 February 2021, the Government argued that the applicant had had access to an effective remedy and had also had a fair hearing before a court with regard to his complaint about the lawfulness and proportionality of the criminal investigation measures, and the use of the information thus obtained in the subsequent disciplinary proceedings. Firstly, his complaints had been examined by the prosecutor and the Vilnius Regional Court (see paragraphs 18-23 above). Secondly, from the very beginning of the disciplinary proceedings the applicant had been afforded the opportunity to comment, and had commented, on the materials used against him, those materials having been disclosed to him to the necessary extent. Overall, he had been aware of the duration, scope and content of the criminal investigation measures employed. The applicant had received all the relevant materials relating to the criminal intelligence investigation, and the scope of the materials that he had received even exceeded the materials directly used in the disciplinary proceedings against him (see paragraphs 24 and 55 above).

63. As the Vilnius Regional Court had examined the applicant's complaint regarding the lawfulness of the criminal intelligence measures in written proceedings, neither the applicant nor the prosecutor had participated in them physically, and therefore the principles of adversarial proceedings and equality of arms had been respected.

64. Lastly, referring to the content of the Supreme Administrative Court's ruling of 29 April 2021 (see paragraphs 41-45 above), the Government contended that the lawfulness and proportionality of the intelligence measures, as well as the use of the information thus obtained, had been carefully and properly addressed, also having regard to the principles stemming from the Constitutional Court's ruling of 18 April 2019.

2. *The Court's assessment*

(a) General principles

65. The relevant case-law of the Court has been set out in *Drakšas v. Lithuania* (no. 36662/04, § 67, 31 July 2012); *Pocius v. Lithuania* (no. 35601/04, §§ 51 and 52, 6 July 2010); see also, more recently, *Prebil v. Slovenia* (no. 29278/16, § 42, 19 March 2019, and, *mutatis mutandis*, *López Ribalda and Others v. Spain* [GC], nos. 1874/13 and 8567/13, §§ 150 and 152, 17 October 2019).

(b) Application of the general principles to the instant case

66. The Court finds that the applicant's complaint may be understood as twofold: firstly, he pleaded not having been able to effectively contest the lawfulness of the authorities' actions and decisions concerning the interception of his telephone communications; secondly, he contended that he had not been able to become familiar with and contest the materials obtained during that surveillance, even though those materials had led to his dismissal. The Court will address both issues in turn.

67. The Court finds that this case must be distinguished from the facts in *Drakšas* (cited above, § 68), where the applicant could not contest the lawfulness of the interception of his telephone communications in an effective manner. With regard to this point, the Court refers to Article 5 § 9 of the Law on Criminal Intelligence, which sets out two levels of appeal against such actions (see paragraph 47 above), this fact also having been noted by the domestic court (see paragraph 20 above). Accordingly, in the instant case the applicant put his grievances to the prosecutor, who examined his complaint and gave detailed answers, and afterwards to a court (see paragraphs 18-23 above). As it appears from the documents in the Court's possession, before reaching his decision the prosecutor had obtained the criminal investigation file; even so, the prosecutor would only rely on the materials which were not classified (see paragraph 18 above).

68. The applicant's appeal against the prosecutor's decision was then examined by the Vilnius Regional Court, which gave detailed and specific reasons why it had been lawful and proportionate to use criminal intelligence measures against the applicant. Before reaching its verdict, the Vilnius Regional Court had ordered the Department of Prisons to provide it with the criminal intelligence materials (see paragraph 20 *in limine* above). As the court decision of 25 September 2017 reads, the Vilnius Regional Court entered into the merits of the applicant's complaint concerning the lawfulness and proportionality of the use of the criminal intelligence measures (see, in particular, paragraph 21 above; contrast, *mutatis mutandis*, *Prebil*, cited above, § 44). This aspect was later pointed out by the administrative court, which also held that there had been no basis on which to hold that the authorities' actions would have been in breach of the law (see paragraph 38

above). Given the documents previously made available to the applicant (see paragraphs 12 and 13 above; see also paragraph 24 above), the Court considers that he was able to formulate his claims to the necessary extent (contrast *Pocius*, cited above, §§ 51, 54 and 56). Even assuming that at the stage of the proceedings before the Vilnius Regional Court the applicant had not yet had access to all the criminal intelligence materials – a circumstance which in any case was remedied by the applicant having access to those materials at a later stage (see paragraph 70 below) –, the Court observes that the entitlement to disclosure of relevant evidence is not an absolute right. In any court proceedings there may be competing interests, such as national security or the need to keep secret certain police methods of investigation, which must be weighed against the rights of the defence (see *Pocius*, cited above, §§ 52 and 53), this having clearly been the situation in the case at hand. On the effectiveness of review, the Court has stated that a reviewing authority must be able to verify whether contested measures have been lawfully ordered and executed. In the case of retrospective review of the lawfulness of a surveillance measure, the applicant must, at the very least, be provided with sufficient information regarding the existence of an authorisation and the minimum level of information about the decision authorising secret surveillance (see *Šantare and Labazņikovs v. Latvia*, no. 34148/07, § 55, 31 March 2016, and the case-law cited therein). On the facts of this case, the Court finds that such information was provided to the applicant. The Court also does not lose sight of the legal rule that certain materials, such as those relating to the participants in the criminal investigation measures, may not be disclosed to individuals by law (see paragraph 47 above), this aspect having been underscored both by the Department of Prisons and the court (see paragraphs 12 and 13 above).

69. Last but not least, the Court considers that the fact that the proceedings before the Vilnius Regional Court were conducted in writing (see paragraph 20 above), does not mean, in and of itself, that the examination of the applicant's complaints was in any sense formal, as alleged by him (see paragraph 61 above), or that the applicant was placed at a disadvantage *vis-à-vis* the State authorities – the Department of Prisons and the Prosecutor General's Office – because the representatives of those institutions did not take part in that court hearing either so as to be able to counter the applicant's written submissions to the Vilnius Regional Court (contrast, *mutatis mutandis*, *Prebil*, cited above, § 43). It follows, that each party had thus been given a reasonable opportunity to present its case under conditions that did not place it at a substantial disadvantage *vis-a-vis* its opponent. As the relevant case-law bears out, Article 6 § 1 is intended above all to secure the interests of the parties and those of the proper administration of justice (see *Nideröst-Huber v. Switzerland*, 18 February 1997, § 30, *Reports of Judgments and Decisions* 1997-I), and to ensure that such fundamental principles as the right to adversarial proceedings and the

principle of equality of arms have been respected. Besides, the Court notes that during the subsequent set of proceedings in which the lawfulness of the criminal intelligence measure against the applicant was examined afresh, the applicant consented to no hearing being held (see paragraph 35 above).

70. The Court also finds that the applicant's main grievance lies in the fact that he was dismissed from his post on the basis of the materials gathered during the secret interception of his telephone communications, those materials containing factual allegations about the applicant's behaviour. On this point, and as regards the factual grounds for his dismissal, the Court notes that as early as 2016, within the disciplinary proceedings, the Vilnius Regional Administrative Court obliged the relevant institutions to provide those documents, and, in accordance with the principle of equality of arms, the applicant was provided with numerous documents on which the disciplinary penalty had been based (see paragraph 36 above). It also transpires that relevant documents were provided to him in March and December 2017 (see paragraphs 12-15, and 24 *in limine*, above). Likewise, other declassified documents concerning the basis for the interception measure from the Department of Prisons, the Prosecutor General's Office and the court were disclosed to the applicant in 2020 (see paragraph 33 above; contrast *Pocius*, cited above, § 57).

71. The Court also finds that the proportionality of the use of that information for the purpose of the applicant's disciplinary liability was thoroughly examined and explained, firstly by the Vilnius Regional Administrative Court and then by the Supreme Administrative Court (see paragraphs 36-38, 41 and 42 above), both of which in turn relied on the Constitutional Court's ruling on that issue (see paragraphs 36 and 41 above). As noted by the administrative courts, the applicant had not contested the reliability of that information (see paragraphs 39 and 43 above). The Court also takes into account the fact that, as pointed out by the Government, during the judicial proceedings regarding the disciplinary penalties, the applicant was even provided with the documents proving the lawfulness of the secret entry and surveillance that were not used in the disciplinary proceedings against him (see paragraph 24 *in fine* above). Similarly, the Court also does not lose sight of the fact that the applicant's dismissal was based not only on the materials gathered through the interception of his telephone communications, but also on the entirety of the evidence, which included contracts with the telecommunications company and witness testimony (see paragraphs 39, 41 and 44 above). Thus, in the present case the applicant was apprised of the evidence against him and had the opportunity to respond to it. In addition, the applicant did not object to the hearing before the Vilnius Regional Administrative Court being held in writing, this having been for clearly objective reasons (see paragraph 35 above).

72. That being so, the Court finds that the applicant had effective access to court for his complaints about the interception of his telephone

communications and the use of the thus obtained information, and his complaints were given due examination by the domestic courts of both general and administrative jurisdiction.

73. The foregoing considerations are also sufficient to enable the Court to conclude that the applicant had effective access to court and that the decision-making procedure fully complied with the requirements of adversarial proceedings and equality of arms, and incorporated adequate safeguards to protect the interests of the applicant.

74. The Court holds that there has been no violation of Article 6 § 1 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

75. The applicant further complained that the secret surveillance against him had been in breach of his right to respect for his private life, as provided in Article 8 of the Convention, which reads as follows:

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or 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.”

A. Admissibility

1. *The parties' submissions*

(a) **The Government**

76. Referring to the Supreme Administrative Court's analysis in the ruling of 29 April 2021, the Government contended that the applicant's complaint regarding the use of information obtained during the criminal intelligence investigation in the criminal proceedings had been unfounded.

(b) **The applicant**

77. The applicant made no comments regarding the admissibility of the complaint.

2. *The Court's assessment*

78. The Court finds that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. *The parties' submissions*

(a) The applicant

79. The applicant submitted that there had been no proper factual or legal basis to intercept his telephone communications. The factual basis for the criminal intelligence investigation had been his alleged abuse of office. That being so, and even though this information had not been confirmed during the first period authorised by the court, in order to obtain further information about any other possible offences committed by the applicant, the criminal intelligence officers had listened to his calls for an entire year. The applicant thus contended that, in the absence of evidence of a crime, the investigation should have finished after the initial period of three months. The applicant also argued that the judge authorising and extending the secret measures had based all the orders on identical and abstract reasons. Given that no pre-trial investigation had eventually been initiated, such measures could not be considered as a proportionate interference with his private life. The applicant was dissatisfied that, although the authorities had not identified any criminal offences in his respect, the information gathered was used to investigate his disciplinary offences. His right to privacy had been disproportionately restricted.

(b) The Government

80. The Government admitted that there had been an interference with the applicant's right to respect for his private life, given the interception of his telephone conversations and their use to investigate the applicant's disciplinary offences. However, the interference with the applicant's right to respect for his private life was in compliance with the requirements of Article 8 § 2 of the Convention, as it was lawful, it pursued a legitimate aim and it was necessary in a democratic society.

2. *The Court's assessment*

81. On the facts of the case the Court cannot but find that the interception of the applicant's telephone conversations, the storage of that information and its disclosure in the disciplinary proceedings, which ultimately led to his dismissal, amounted to an interference with his right to respect for his private life (see, *mutatis mutandis*, *Pocius*, cited above, §§ 41-43, with further references). The Court has emphasised that telephone tapping is a very serious interference with a person's rights and that only very serious reasons based on a reasonable suspicion that the person is involved in serious criminal activity should be taken as a basis for authorising it (see *Iordachi and Others v. Moldova*, no. 25198/02, § 51, 10 February 2009). The existence of the

interference has not been disputed by the Government (see paragraph 80 above).

82. The cardinal issue arising in the present case is whether the interference so found was justified in terms of paragraph 2 of Article 8. This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions (see *Rotaru v. Romania* [GC], no. 28341/95, § 47, ECHR 2000-V, see also *Drakšas*, cited above, § 54).

83. In order for the interference established above not to infringe Article 8, it must first of all have been “in accordance with the law” (see *Drakšas*, cited above, § 55), a condition which has been met in the present case, given that the interference had a basis in the Law on Criminal Intelligence. The Court is also satisfied that the measure was authorised by the court (see paragraph 8 above). Accordingly, the authorisation to start monitoring the applicant’s telephone conversations had a legal basis in domestic law. The same conclusion holds true regarding the use of those materials within the disciplinary proceedings, as authorised by the prosecutor on the basis of Article 19 § 3 of the Law on Criminal Intelligence (see paragraph 25 above), that provision having been in force well before the applicant had committed the disciplinary offences, and the constitutionality of that provision having been confirmed by the Constitutional Court (see paragraphs 47, 50 and 51 above; compare *Karabeyoğlu v. Turkey*, no. 30083/10, §§ 78-84, 7 June 2016, and *Eminağaoğlu v. Turkey*, no. 76521/12, § 161, 9 March 2021). Besides, as to the requirement of foreseeability, it cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see *Drakšas*, cited above, § 67). In the present case the Court also finds that the absence of prior notification of interception was compensated for in the Law on Criminal Intelligence, accessible to the applicant, as that Law laid down strict conditions with regard to the implementation of the surveillance measures.

84. Regarding the legitimate aim, the Court observes that the applicant had been suspected of corruption-related activity – giving better conditions, as well as incentives, to inmates – for personal gain. Such actions, which could have led to inmates being released before they had reformed, demonstrated a danger to society (see paragraphs 21 and 22 above). In this context the Court notes the domestic courts’ finding that such activity, which the applicant was suspected of, and which was not entirely without basis (see paragraph 31 above), could have placed people outside the prison walls in danger (see paragraph 22 above). Furthermore, as pointed out by the Vilnius Regional Administrative Court, the applicant’s actions discredited the system of the execution of sentences, and were damaging to society’s trust in public

service (see paragraph 39 above). Likewise, as emphasised by the Supreme Administrative Court, the use of information gathered during the secret surveillance against the applicant served the purpose of guaranteeing the transparency and openness of public service, and sought to ensure that the aims of statutory institutions were not ignored (see paragraph 43 above). Prevention of acts of a corrupt nature and transparency and openness of State service have also been listed among legitimate aims by the Constitutional Court (see paragraphs 50 and 51 above). Seeing no reason to depart from the domestic courts' findings, the Court therefore holds that the interference pursued a legitimate aim – the prevention of disorder or crime, and the protection of the rights and freedoms of others – in pursuance of Article 8 paragraph 2 of the Convention.

85. The Court lastly turns to the necessity and proportionality of the interference. It observes that on 30 June 2015 the Vilnius Regional Court, acting on a request by the Prosecutor General's Office, and on the basis of the information made available to that court by the Department of Prisons through the prosecutor, authorised the tapping of the applicant's telephone on the basis of information that the applicant had been involved in corruption-related acts that amounted to an abuse of office (see paragraphs 6-8 above). As it appears from the prosecutor's application, and as it was afterwards upheld by a court, by then other investigative measures had already been employed; however, they had been insufficient to investigate possible criminal activity (see paragraphs 7, 8 and 21 above). As later explained by the Vilnius Regional Court, that information included information about a particular inmate who had received better conditions in prison, and also incentives (see paragraph 21 above). Having regard to the facts of the case, the Court is ready to accept that the Vilnius Regional Court had sufficient reasons, based on specific information, to authorise and extend the measure of the telephone tapping (see also paragraph 8 above). Accordingly, the Court cannot find that the authorisation was without grounds or that the surveillance was "general" or "exploratory" (see *Klass and Others v. Germany*, 6 September 1978, § 51, Series A no. 28, see also *Drakšas*, cited above, § 56). Above all, on this last point the Court also reiterates that it is primarily for the national authorities, notably the courts, to interpret and apply domestic law. In principle, therefore, it is not for the Court to express an opinion contrary to that of the Vilnius Regional Court in its ruling of 30 June 2015 on the compatibility of the judicially ordered tapping of the applicant's telephone with Article 10 of the Law on Criminal Intelligence (see *Kopp v. Switzerland*, 25 March 1998, § 59, *Reports* 1998-II, and *Drakšas*, cited above, § 56).

86. Furthermore, although the applicant implied that the interception of his telephone communications had been exploratory (see paragraph 79 above), the Court cannot subscribe to that statement, because, as was clearly explained by the Vilnius Regional Court, during each three-month period that the measure was extended, new events materialised which showed the

applicant's involvement in illegal activities, and information about "new concrete events" proved to be true (see paragraph 21 above). The duration of the interception did not exceed the maximum twelve-month period, as set out in the Law on Criminal Intelligence, which was also pointed out by the domestic court (see paragraph 21 above). Lastly, as noted by the Vilnius Regional Court, the interception was proportionate in view of the applicant's position – he was the director of a protected incarceration facility – which significantly reduced other means for a criminal investigation (see paragraph 22 above).

87. As regards the proportionality of the use of that information in the disciplinary proceedings, the Court gives weight to the applicant's position as the director of a prison, and the seriousness of the acts which were investigated, and thus does not dispute the Vilnius Regional Administrative Court's finding that the fact that no criminal investigation had been opened in respect of the applicant, in and of itself, did not make the use of the information obtained unlawful in the disciplinary proceedings (see paragraph 38 above). The Court also notes that the use of the materials obtained during the criminal intelligence investigation was not limitless; rather, under Article 19 § 3 of the Law on Criminal Intelligence, it was restricted to acts of a corrupt nature (see paragraph 47 above). The proportionality of such use – in order to guarantee the effectiveness of the law enforcement institutions, and the need for a high disciplinary and moral standard for State officials, including the applicant, who was supposed to lead by example – was explained by the Supreme Administrative Court (see paragraphs 39 and 43 above). That court found that disciplinary offences, as committed by the applicant, had been established on the basis of the entirety of evidence, and the applicant had not contested the reliability of the collected information during the disciplinary investigation (see paragraphs 41 and 42 above). The applicant had also been able to contest the proportionality of the use of that information (see paragraph 41 above), this finding also having been reached by this Court (see paragraph 73 above). In the light of the foregoing, the Court finds that when assessing the necessity and proportionality of the use of such information for the investigation of the applicant's disciplinary offences, the administrative courts followed the Constitutional Court's guidelines and afforded effective protection of his rights (see paragraphs 50 and 51 above). The fact that there had been no disproportionate interference with the applicant's right to privacy has also been noted by the domestic courts (see paragraphs 23 and 40 above).

88. Lastly, as noted by the administrative court, and as already established by this Court, the applicant had an opportunity to take part in court proceedings in an effective manner in order to contest the lawfulness and proportionality of the use of those materials (see paragraphs 41 and 73 above).

89. In the light of the foregoing the Court holds that the interference with the applicant's right to respect for his private life may be regarded necessary and proportionate.

90. There has therefore been no violation of Article 8 of the Convention.

FOR THESE REASONS, THE COURT

1. *Declares*, unanimously, the application admissible;
2. *Holds*, unanimously, that there has been no violation of Article 6 § 1 of the Convention;
3. *Holds*, by six votes to one, that there has been no violation of Article 8 of the Convention.

Done in English, and notified in writing on 18 January 2022, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Stanley Naismith
Registrar

Jon Fridrik Kjølbro
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judge Koskelo is annexed to this judgment.

J.F.K.
S.H.N.

PARTLY DISSENTING OPINION OF JUDGE KOSKELO

1. I have regrettably not been able to agree with the conclusion reached by the majority, to the extent that they have found no violation of Article 8 in the present case. I consider that the use, in the disciplinary proceedings against the applicant, of the records obtained by the previous interception of his telephone communications has not been subjected to the necessary level of scrutiny by the domestic courts, nor by our Court. Given the highly intrusive nature of such interception, and the associated risks of abuse, the approach taken is, in my view, a matter of concern, also in the light of the Court’s existing case-law.

2. To sum up the essential factual circumstances of the case, the applicant was first subjected to a criminal investigation based on suspicions of “corruption-related activity” in his dealings with the inmates of the prison of which he was the director. In connection with that criminal investigation, the interception of his telephone calls was authorised, repeatedly, until the maximum period for such a measure (one year) ran out. Apart from that, it appears that covert listening devices were also placed in the applicant’s office (see paragraph 9 of the judgment). In the end, the criminal investigation was discontinued on the grounds of a lack of incriminating evidence (see paragraph 10 of the judgment). Subsequently, however, the records obtained through the phone-tapping operation were released for further use in the context of an investigation into “the applicant’s disciplinary offences or misconduct in office” (see paragraph 25 of the judgment).

3. Under domestic law, such further use of the materials from the interception was in principle permissible, subject to the important reservation set out by the Constitutional Court in its ruling of 18 April 2019. According to this ruling (cited in paragraph 50 of the judgment), it is necessary to assess, in each case, whether the use of the information in question for the purposes of investigating misconduct in office of a corrupt nature is in line with the principle of proportionality, or whether the aims pursued could be achieved in a particular case by other, less restrictive means. In the present case, however, it is open to doubt whether such an assessment has taken place. In the light of the domestic decisions as cited in the present judgment, it appears that the domestic authorities relied on the fact that recourse to the interception measure in the context of the *criminal* investigation had been considered lawful (see paragraph 38 of the judgment). This, however, cannot be sufficient when it comes to an assessment of the *further* use of such materials outside the criminal investigation for the purposes of which the measure was authorised.

4. The interception of telephone conversations and/or other means of communication, which involves surveillance of the content of such communications, is an extremely intrusive measure of interference with the

rights protected under Article 8 of the Convention. While there is no doubt that such interception measures may be necessary and justified in the context of criminal investigations into serious offences, any further use of the records of such interceptions, outside the context for the purposes of which those measures have been authorised, raises distinct issues from the point of view of the requirements of Article 8.

5. The Court has acknowledged that tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence which must, also in view of the inherent risks of abuse, be based on a “law” that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated (see, for instance, *Amann v. Switzerland* [GC], no. 27798/95, § 56, ECHR 2000-I, and *Uzun v. Germany*, no. 35623/05, § 61, ECHR 2010, with further references). Accordingly, in its case-law on the interception of communications in criminal investigations, the Court long ago developed certain minimum requirements, to be set out in law, in order to avoid abuses of power. They include a definition of the categories of people liable to have their telephones tapped by judicial order, the nature of the offences which may give rise to such an order, a limit on the duration of telephone tapping, the procedure for drawing up the summary reports containing intercepted conversations, the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and by the defence, and the circumstances in which recordings may or must be erased or the tapes destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court (see *Valenzuela Contreras v. Spain*, 30 July 1998, § 46, *Reports of Judgments and Decisions* 1998-V).

6. Against this background, and in the light of contemporary principles relating to the protection of personal data in general, it seems clear that the question of safeguards concerning any further disclosure and use of intercepted information *outside* the context of criminal investigations also requires specific consideration. Indeed, the Court has held on many occasions that domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of Article 8 (see *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 103, ECHR 2008). There can be no doubt, in my view, that this requirement also applies to disclosure of the content of a person’s communications with other individuals. The need for sufficient safeguards against a risk of abuse, inherent in any system of secret surveillance, is also present in the context at issue here (compare *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 93, 28 June 2007).

7. Accordingly, it cannot be sufficient for only the original interception of communications for the purposes of a criminal investigation, and its use in

that context, to take place in compliance with Article 8. Any *further* disclosure and use of such information must also satisfy the requirements of lawfulness, necessity and proportionality.

8. It is easy to see how circumstances similar to the factual background of the present case might provide illustrations of the importance of a sufficiently rigorous approach in this respect. Where the interception of an individual's communications has been authorised on the grounds of a criminal suspicion but no incriminating evidence has emerged, even if the interception has lasted a whole year (maximum duration), the handing-over of the information thus obtained for the purposes of non-criminal proceedings may give rise to legitimate questions about possible circumvention of the statutory constraints. In any event, the use of intercepted materials for purposes which, in themselves, could not have served as a basis for the authorisation of such investigation measures clearly requires specific safeguards to be put in place in law and to be effectively applied in practice.

9. Indeed, as already mentioned above, the Constitutional Court has acknowledged the need for a separate assessment of the necessity and proportionality of such further use of intercepted communications. Based on the reasoning in the domestic decisions, however, I am not convinced that in the present case such an assessment has actually taken place in any proper sense. In particular, whereas the criminal suspicions against the applicant had to do with his alleged dealings with prison inmates, the disciplinary proceedings concerned matters of a different nature, namely irregularities in the internal recruitment or promotion processes, in the acquisition of some mobile phones on behalf of the prison, and in the use of the prison car (see paragraphs 27 and 28 of the judgment). It is difficult to see how an investigation into the latter kinds of misconduct in the prison administration could reasonably have depended on information obtained by the interception of the applicant's telephone communications.

10. In my view, the domestic authorities have not put forward relevant and sufficient reasons, as should be required, to explain and justify the necessity and proportionality of the disclosure and use of the intercepted information for the purposes of the disciplinary investigation. I therefore consider that there has been a violation of Article 8 in this respect.