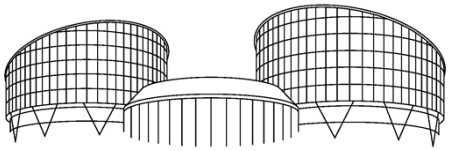

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIFTH SECTION

CASE OF ROOK v. GERMANY

(Application no. 1586/15)

JUDGMENT

STRASBOURG

25 July 2019

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Rook v. Germany,

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

Yonko Grozev, *President,*
Angelika Nußberger,
André Potocki,
Mārtiņš Mits,
Gabriele Kucsko-Stadlmayer,
Lətif Hüseynov,
Lado Chanturia, *judges,*
and Claudia Westerdiek, *Section Registrar,*

Having deliberated in private on 2 July 2019,

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

PROCEDURE

1. The case originated in an application (no. 1586/15) against the Federal Republic of Germany lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a German national, Mr Michael Rook ("the applicant"), on 2 January 2015.

2. The applicant was represented by Mr T. Junker, a lawyer practising in Augsburg. The German Government ("the Government") were represented by their Agents, Mr H.-J. Behrens and Ms K. Behr of the Federal Ministry of Justice and Consumer Protection.

3. The applicant alleged that, during the criminal proceedings against him, he and his counsel had not been provided with sufficient and adequate access to audio files, text messages and electronic files (specifically emails and other text documents) which the investigating authorities had seized throughout the investigation. He relied on Article 6 § 1 and 3 (b) of the Convention.

4. On 16 September 2016 notice of the application was given to the Government.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

5. The applicant was born in 1964 and lives in Quickborn. He was a senior manager and, most recently, managing director of a major retailer for consumer electronics in Germany and other European countries.

A. Criminal investigation

6. On 7 February 2011, the Augsburg public prosecutor's office opened a criminal investigation against the applicant and eight other co-accused for taking bribes in commercial practice, following a criminal charge brought by the applicant's employer. On 9 November 2011 the applicant was taken into detention on remand. He was initially detained in a prison in Munich and later transferred to Augsburg Prison. The applicant chose three lawyers to conduct his defence. One had his office in Augsburg (subsequently referred to as "the applicant's lawyer"), whilst the other two were based in Karlsruhe and Neuwied (subsequently referred to as "the other two lawyers").

1. Telecommunication surveillance

7. During the investigation wide-ranging telecommunication surveillance was carried out. A total of around 44,970 telephone calls and about 34,000 other data sets were stored as part of this. The latter included text and multimedia messages, system files or network providers' report files resulting from technical communication between a device and the provider. The data sets for the individual exchanges over telecommunications media were entered into a special criminal-police database at the Bavarian Office of Criminal Investigation in Munich. They were analysed by the police. Eventually, transcripts of twenty-eight telephone conversations which had been considered relevant were prepared, printed and subsequently included in the (paper) investigation file.

2. Electronic files

8. During searches of the applicant's home and of other premises between 13 July 2011 and 1 February 2012, some 14 million electronic files (for example emails and other text documents), stored on a range of data devices, for example hard discs, were seized. The files of each device were copied as a single "image file", the devices were returned to the rightful holders, including the applicant, afterwards. Each image file was a full digital clone of each data device, readable with a program available free of charge online. However, the image files were subsequently entered into a

special forensic-data-analysis program, after which their content could be retrieved only using that special program, available for 4,031.72 euros (EUR). After the data had been entered into that program, in order to be able to read the data with a program available free of charge online, the data had to be exported from the special forensic-data-analysis program and converted back into an image format. The above-described processing of the data, in particular feeding them into the special forensic-data-analysis program, was finished by the end of February 2012; they were stored at the Bavarian Office of Criminal Investigation in Munich.

9. The data were analysed by the police; around 1,100 of these electronic files were considered as relevant to the case and were printed and subsequently included in the paper files.

3. Access during the investigation

10. On 10 November 2011 the applicant's lawyer was provided access to the (paper) investigation file – the other two lawyers never requested it. The file contained the information that telecommunication surveillance had taken place. Updates of that paper file, such as the inclusion of transcripts of covertly recorded telephone calls (see paragraph 7 above) and prints of the seized electronic files (see paragraph 9 above), were from then on regularly sent to the applicant's lawyer. The information that electronic files – apart from his own – had been retrieved had been noted in the paper file, transmitted in the above described manner, in February 2012 at the latest.

11. On 30 November 2011, after the applicant's lawyer had become aware that there had been much more telecommunication surveillance than what had been prepared as transcripts and put into the paper file (see paragraph 7 and 10 above), he asked to examine "the audio files obtained from telephone tapping" and copies of the audio files on CD or DVD. On 2 December 2011 the public prosecutor's office decided to grant access. It informed the applicant's lawyer by telephone that he could examine the data on the premises of the criminal police during regular opening hours (from Monday to Friday, from 9.00 to 11.00 and from 14.00 to 16.00) and under the supervision of a police officer. At the same time, it dismissed the request for copies of the audio files.

12. The applicant's lawyer subsequently scheduled two appointments to visit the premises of the criminal police before the end of 2011. Prior to the scheduled appointments, the police asked the applicant's lawyer which audio files/text messages he wished to examine. He provided the police with the relevant search parameters of his choosing. The police retrieved the files matching the parameters, copied them to a notebook computer, which the lawyer subsequently accessed during the appointment.

13. On 3 January 2012, the defence asked the Augsburg public prosecutor's office to provide lists indicating the raw data for the various telephone lines; the dates of the calls; the duration of the calls; the

Identnummer ("ID number"); and a "link to each MP3 file with filenames". The public prosecutor's office informed the applicant's lawyer on the same day that his request had been forwarded to the responsible criminal police unit, as the public prosecutor's office was not aware if providing such lists was technically possible. The public prosecutor's office did not itself have at its disposal the requested lists.

B. Indictment and access

14. On 22 February 2012 the Augsburg public prosecutor's office indicted the applicant before the Augsburg Regional Court on ninety-one counts of taking bribes in commercial practice. Eight other persons were indicted along with the applicant.

1. Access to the surveillance data

15. Between 22 February 2012 and 6 June 2012 the applicant's lawyer had four more appointments to examine the surveillance data (see paragraph 11 above). At one appointment in April 2012 he was provided with a printed spreadsheet table listing the data sets copied to the notebook according to the chosen parameters. This list contained the dates and the times the conversations had begun, the dates and times the conversations had ended, the number of the tapped line and the "partner line", an assessment of whether the calls were "relevant" or "not relevant" and a technical identification number which allowed the MP3 file for each conversation to be located and retrieved. The list also showed the stored text messages (or for longer messages, parts thereof).

16. On 12 March 2012 the applicant's lawyer applied to the Augsburg Regional Court for access to the audio files of the surveillance data in the form of a read-only copy on DVD or CD, which would be returned after the completion of the criminal proceedings.

17. On 22 March 2012 the Augsburg Regional Court rejected the application. It essentially referred to the previously filed prosecution's submissions on that matter, holding that the files themselves were evidence which the defence had no right to have in its possession. This was all the more true as the files contained highly personal data; the prosecution was obliged to delete those files – an obligation it could not anymore fully comply with once copies of the data had been passed on to the defence. Overall, sufficient access had been granted.

18. On 3 May 2012 the Regional Court, considering an appeal by the applicant of 23 April 2012, extended the access to the telecommunication surveillance files. It ordered that all data sets were to be copied to a notebook computer kept at the prison where the applicant was detained, that the defence could listen to the audio files in prison, together with the applicant and under the supervision of a police officer, to ensure that no

access to telephone records which touched on the private life of others was granted. In so far as the applicant's appeal exceeded the granted access, in particular in so far as the applicant strived for possession of a copy of the files, the Regional Court dismissed it and referred it to the Munich Court of Appeal.

19. On 9 May 2012, the notebook computer with the copied data was deposited ready for examination during regular visiting hours (from Monday to Friday, from 8.00 to 11.00 and from 13.00 to 16.00) on the premises of the prison the applicant was detained in. The applicant's lawyer however never made use of the possibility to examine the files on the premises of the prison – he rather arranged for their examination on the premises of the criminal police (see paragraphs 11 et seq., 15 above and 28 below).

20. On 25 May 2012 the Munich Court of Appeal dismissed the remaining parts of the applicant's appeal as ill-founded. The court, which referred to prior submissions of the prosecution and the prior decisions of the Regional Court in that matter, held that there was no reason to provide the defence with copies of all the records obtained from telecommunication surveillance in excess of the access already granted. Moreover, while understandable that, from the point of view of the defence, a list showing the details of the respective conversations would enable relevant conversations to be identified and listened to faster, there was no entitlement to such a list being prepared.

2. Access to electronic files

21. On 3 April 2012 the applicant's lawyer applied to be provided a copy of the 14 million electronic files (see paragraphs 8 and 10 above).

22. On 18 April 2012 the public prosecutor's office informed the Augsburg Regional Court that it would not be possible to provide the around 14 million files sought, owing to the way the material had been processed and fed into the system at the Bavarian Criminal Police Office (see paragraph 8 above). Nor could the applicant's lawyer be given remote access to the police data-analysis program. He could, however, approach the police to find a common solution. This information was forwarded to the applicant's lawyer on 23 April 2012.

23. On 30 April 2012 the Regional Court informed the applicant's lawyer that the court had no objection, in principle, to the examination of the 14 million seized files. The court suggested that he should contact the responsible police officer. Given the large volume of data involved, the court was unable to ascertain whether it would be possible to create a copy.

24. On 3 May 2012 the Regional Court informed the applicant's lawyer that, according to the information of the responsible police officer, it would be possible to copy the seized emails to an external data-storage device at

the Bavarian Criminal Police headquarters, and the files would be copied once a suitable storage device had been supplied.

25. On 9 May 2012 the applicant's lawyer provided a hard disc to the police. The same day, he was also informed that a special forensic-data-analysis program was needed to read the data, since they had been entered into such a program and were not available in their original format anymore (see paragraph 8 above); he was furthermore supplied with the contact details of a company which provided such software. On 18 May 2012 the disc holding the files was ready for collection and on 22 May 2012 it was collected by the defence.

26. On 22 May 2012, after having realized that the special forensic-data-analysis program cost EUR 4,031.72 (see paragraph 8 above), the applicant's lawyer applied to the Regional Court to have the prosecution authorities ordered to either acquire and provide the licence for the software or to have the state bear the cost of EUR 4,031.72 needed to purchase the software.

C. Hearings

27. From 6 June 2012 until 21 December 2012 the Augsburg Regional Court conducted hearings on twenty-two separate days.

1. Access to the surveillance data

28. Until the end of the proceedings, on 21 December 2012, the applicant's lawyer examined the audio files of the telecommunication surveillance on a further sixteen occasions, none later than 31 October 2012 (see paragraph 11 above).

29. On 26 June 2012, the day of the second hearing, the applicant's lawyer applied for the proceedings to be stayed, arguing, *inter alia,* that only this would allow adequate examination of the data sets obtained by telecommunication surveillance.

30. On 28 July 2012, another hearing day, the presiding judge informed the applicant's lawyer of the possibility to seek the support of judicial employees in order to examine the data.

2. Access to electronic files

31. The application for a stay of proceedings of 26 June 2012 (see paragraph 29 above) was additionally based on the reason of securing an opportunity to examine and evaluate at least selected samples of the around 14 million electronic files in a manner which would allow for reliable conclusions to be drawn.

32. On 16 July 2012 the Regional Court decided, with regard to the application of 22 May 2012 (see paragraph 26 above) that the prosecution

authorities should not acquire a software licence and that the cost of EUR 4,031.72 should not be borne by the state. It held that the program was available on the open market and that it was not the responsibility of the court to provide the applicant's lawyer with the technical equipment to have access to files or examine evidence. That might, where necessary, only be different, under the principles of the right to a fair trial and the principle of equality of arms, if the defence had otherwise incurred disproportionate expenses, the technical equipment had been unobtainable or the defendant could not advance the cost. This was not the case here. The applicant was able to afford three lawyers for his defence team. It could therefore be assumed that the applicant had at his disposal the necessary financial means to buy a software licence.

33. On 19 July 2012 the applicant's lawyer asked to be provided with the data in "unencrypted form". On 23 July 2012 the public prosecutor's office informed the defence that it was indeed possible to export the electronic files from the special forensic-data-analysis program and convert them back into an image format, readable with a software available free of charge online (see paragraph 8 above). If the defence wished to receive the data in this format and were to provide hard discs, it would be provided with it. On 31 July 2012 applicant's lawyer delivered two hard discs to the police, which were sent on to the responsible officer the following day. On 4 September 2012 the two hard discs, containing the data as image files, readable with a software available free of charge online, were given to the applicant's lawyer.

3. Dismissal of the application to stay the proceedings

34. On 14 November 2012, a further day of hearings, the Regional Court dismissed the applicant's application for a stay of proceedings (see paragraphs 29 and 31 above). In respect of the telecommunication surveillance, it referred to its prior decisions concerning the scope of access, which had been granted sufficiently. It also referred to the fact that the defence had made scant use of the possibility to seek support of judicial employees, that only one of the three lawyers had made use of his right of access at all, and that that lawyer had not attended several appointments for examination of evidence and had not arranged for a substitute when on leave. In respect of the 14 million electronic files, it had, after the lawyer had initially requested access to the investigation file (see paragraph 10 above), at all times been possible for him to examine them on the premises of the police – a possibility which he had not made use of. Moreover, the files had been provided to him, on 22 May 2012 in a format readable only with the special forensic-data-analysis program at the expense of the defence (see paragraphs 8, 25, 26 and 32 above), and on 4 September 2012 in a format readable with freely available software (see paragraph 33 above).

D. Judgment

35. On 21 December 2012 the Regional Court rendered its judgment and convicted the applicant and four other accused. The applicant was convicted on sixty-three counts of taking bribes in commercial practice and sentenced to five years and three months' imprisonment. On the remainder of the charges he was acquitted.

E. Appeal proceedings

36. The applicant appealed against the judgment to the Federal Court of Justice. He argued, *inter alia*, that his defence had been harmed by the refusal to grant a stay of the proceedings because he and his lawyer had not had enough time and opportunities to review the files of the telecommunication surveillance and the seized electronic data.

37. On 11 February 2014 the Federal Court of Justice quashed the Regional Court's judgment in respect of three counts of bribery in commercial practice, but dismissed the applicant's further appeal as ill-founded.

1. Access to the surveillance data

38. In regards to access to the surveillance data the court noted that as of 9 May 2012 the defence had been, in the prison premises, provided with the data on a notebook computer with a list indicating both the date and time the communication took place, as well as the content of text messages (see paragraphs 15 and 19 above). The court also noted that the applicant's lawyer had not arranged any appointments to listen to audio files after 31 October 2012 (see paragraph 28 above). It noted that the lawyer had also been able to listen to all the audio files obtained during the investigation, on the premises of the criminal police. Referring to Article 6 § 1 and 3 (b) of the Convention, the court held that there was thus nothing to indicate that the defence did not have adequate time to listen to the audio files. The Federal Court of Justice emphasised in particular, that the applicant's lawyer had neither been at fault in not using other people's help in examining the evidence, nor could he be reproached for the fact that the applicant's two other lawyers had not made use of their entitlement to examine the evidence. The court specifically stated that the right to examine files in their entirety existed for each lawyer individually. However, the defence had failed to make sufficient use of the provided possibilities to examine the telecommunication-surveillance data.

2. Access to electronic files

39. Regarding examination of the data seized during search operations, the court held that it did not have to decide on whether the applicant had been obliged to acquire special software enabling those files to be made readable at his own expense. It clarified, however, that this might be debatable if, as in this instance, the data obtained by the investigating authorities had been in a form readable using standard software and had subsequently been encrypted in a way that had made them readable using only special software (see paragraph 8 above). In sum, the court concluded that since the data had been available to the defence in a form that had been readable with standard software on 4 September 2012 (see paragraph 33 above), they had had sufficient time to examine the files. At this point, there had been three months left before judgment had been rendered.

F. Constitutional Complaint

40. On 25 June 2014 the Federal Constitutional Court refused to admit a constitutional complaint by the applicant, without providing reasons (2 BvR 726/14).

G. Subsequent events

41. After criminal proceedings were terminated, the applicant's former employer lodged a civil action against him for damages and restitution, based on the applicant having taking bribes. On 31 May 2017, after its own taking of evidence and hearing of several witnesses, the Itzehoe Regional Court dismissed the action as it could not establish with sufficient certainty that the applicant had actually been party to any deals concerning bribery or had accepted bribes himself. The difference between the findings of the Augsburg Regional Court and the Itzehoe Regional Court was in essence based on a different assessment of the reliability of the testimony of the main witness for the prosecution, which the latter court did not consider sufficiently reliable.

42. On 26 February 2019, the Schleswig-Holstein Court of Appeal dismissed an appeal by the employer and confirmed the judgment of Itzehoe Regional Court.

43. Following the judgment of the Itzehoe Regional Court, the applicant applied for the reopening of the criminal proceedings. On 27 March 2018 the Munich Regional Court dismissed the applicant's application. The court held that the different assessment of the evidence by the Itzehoe Regional Court did not require a reopening of the criminal proceedings, as the reopening procedure was not an appeal procedure to review previous decisions, but required new facts or evidence. However, as the evidence

taken in the civil proceedings had also been taken in the criminal proceedings, no new evidence was available. On 11 April 2018 the applicant appealed against that decision. No information on the progress of those proceedings has been provided to the Court.

II. RELEVANT DOMESTIC LAW

44. The defence lawyer's right of access to the case file is governed by section 147 of the Code of Criminal Procedure, which reads:

Section 147 - Examination of files

"(1) Defence counsel shall have authority to examine those files which are available to the court or which will have to be submitted to the court if charges are preferred, as well as to examine officially impounded pieces of evidence.

(2) If investigations have not yet been designated as concluded on the file, defence counsel may be refused permission to examine the files or individual parts of the files, as well as examination of officially impounded pieces of evidence, in so far as this may endanger the purpose of the investigation. If the prerequisites of the first sentence have been fulfilled, and if the accused is in remand detention or if, in the case of arrest, this has been requested, information of relevance for the assessment of the lawfulness of such deprivation of liberty shall be made available to defence counsel in a suitable form; to this extent, as a rule, examination of the files shall be granted.

(3) At no stage of the proceedings may defence counsel be refused access to records concerning the examination of the accused or concerning such judicial acts of investigation to which defence counsel was or should have been given access, nor may he or she be refused access to expert opinions.

(4) Upon application, defence counsel shall be permitted to take the files, with the exception of pieces of evidence, to his or her office or to his or her private premises for examination, unless significant grounds present an obstacle thereto. The decision shall not be contestable.

(5) The public prosecutor's office shall decide whether to grant examination of the files in preparatory proceedings and after the final conclusion of the proceedings; in other cases the presiding judge of the court seized of the case shall be competent to decide. If the public prosecutor's office refuses to allow examination of the files after noting the termination of the investigations in the file, or if it refuses to allow examination under subsection (3), or if the accused is not at liberty, a decision by the court competent under section 162 may be applied for. Sections 297 to 300, 302, 306 to 309, 311a and 473a shall apply, *mutatis mutandis*. These decisions shall be given without reasons if their disclosure might endanger the purpose of the investigation.

(6) If the reason for refusing access to the files has not already ceased to pertain, the public prosecution office shall revoke the order no later than upon conclusion of the investigation. Defence counsel shall be notified as soon as he or she once again has the unrestricted right to examine the files.

(7) Where an accused has no defence counsel, information and copies from the files shall be given to the accused upon his or her application, provided that this is necessary for an adequate defence, cannot endanger the purpose of the investigation, also in another criminal proceeding, and that overriding interests of third persons

meriting protection do not present an obstacle thereto. Subsection (2), first part of the second sentence, subsection (5) and section 477(5) shall apply, *mutatis mutandis*."

THE LAW

ALLEGED VIOLATION OF ARTICLE 6 §§ 1 AND 3 OF THE CONVENTION

45. The applicant complained that, during the criminal proceedings against him, he and his lawyer had not been provided with sufficient and adequate access to 45,000 audio files, 34,000 text messages and 14 million email and document files seized by the investigating authorities. He relied on Article 6 §§ 1 and 3 (b) of the Convention, which read, as far as relevant, as follows:

"1. In the determination of ... any criminal charge against him, everyone is entitled to a fair and public hearing ...

3. Everyone charged with a criminal offence has the following minimum rights:

...

(b) to have adequate time and facilities for the preparation of his defence; ..."

46. The Government contested that argument.

A. Admissibility

47. The Court notes that the application is not manifestly ill-founded within the meaning of Article 35 § 3 (a) 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

48. The applicant claimed that the defence had not had, in view of the overwhelming amount of data, sufficient opportunity to acquaint itself with the entirety of the files by listening to or reading through them, or at least to be able to identify relevant files, in order to prepare the defence. This had been all the more true as a lawyer could not be expected to work on one case each and every day, and since the applicant's case had also required other time-consuming activities, such as participation in court hearings on twenty-two separate days.

49. In addition, there had been substantial problems in accessing the data, in particular the obligation to arrange for appointments with the police on their premises, because the data had been stored there and it had been necessary for an officer to be present during the examination of the covertly recorded calls. This had been all the more difficult, since appointments had been confined to regular opening hours. The possibility to access the data without unnecessary restrictions had been provided in respect of telecommunication surveillance from 9 May 2012 onwards only, and in respect of the electronic files from 4 September 2012 only. As far as the domestic courts and the Government had criticised the lawyer for not having arranged for appointments to visit in order to examine the telecommunication-surveillance data as of October 2012, it had to be taken into account that the defence had at that time been busy with analysing the 14 million electronic files, which had been provided only in September 2012. Moreover, after the data had been provided, the authorities had failed to provide the applicant with a list of the data, allowing for identification of relevant and irrelevant data. The applicant's lawyer's work would have been substantially facilitated had the authorities supplied the applicant, in respect of the electronic files, with access software much earlier. It had been unacceptable that they had requested that he pay roughly EUR 4,000 for it.

50. Overall, the applicant considered, the proceedings had therefore not complied with the principle of equality of arms.

(b) The Government

51. The Government was of the opinion that once access had been requested by the defence it had been granted access to all data at all times. The data considered as relevant to the case had been provided upon arrest and subsequently in PDF format upon inclusion in the paper file. As of 2 December 2011, the applicant's lawyer had been allowed to access all telecommunication-surveillance data on the premises of the police. As of the end of February 2012, the same had been true for the by then processed 14 million electronic files. As of 9 May (telecommunication surveillance) and 4 September (electronic files) 2012 the applicant had also been able to access all data personally. Overall, the awarded time had therefore to be considered sufficient for the preparation of the defence.

52. It had to be taken into account that the police had – despite not having been obliged to do so – prepared several lists in order to facilitate the applicant's lawyer in his comprehensive analysis of the data; that it had been possible to substantially narrow down the search by applying search criteria such as certain dates, certain time periods, certain telephone lines or telephone connections; that the applicant's lawyers had not arranged for more appointments; that he had not made use of the possibility of having judicial employees go through the files for him; that he had applied for access to all of the files only significantly later than he could have done; and

that only one of the three lawyers had made use of the possibility to access the data.

53. It had, moreover, not been necessary to enable the defence to listen to and read each and every file; rather, it had been sufficient to allow for the possibility to identify relevant and irrelevant files on the basis of search parameters, such as the telephone from which a call had been made or a telephone to which a call had been made within a certain frame of time. In this connection, it also had to be taken into account that the applicant, who had been involved in the events being examined at trial, had all the necessary knowledge to identify the telephone conversations with possible relevance to the defence.

54. The Government was furthermore of the opinion that the fact that the telecommunication-surveillance data had not all been copied and handed over to the applicant's lawyer had not violated the Convention. That interference with the applicant's rights had been justified, for it had served the protection of the rights of the third persons concerned. In view of roughly 45,000 covertly recorded telephone conversations, it had been rather probable that private, even intimate conversations without any relation to the events under examination had also been captured. There had been a statutory obligation to not listen to those (parts of the) recorded conversations. During examination of the conversations by the lawyer and/or the applicant this obligation had been enforced by the presence of a supervising police officer, who had also been present in order to support the applicant's lawyer with questions regarding the analysis of the data. Had the data been handed over to the applicant's lawyer, that obligation could not have been fulfilled anymore.

2. The Court's assessment

55. As the requirements of paragraph 3 of Article 6 are to be seen as particular aspects of the right to a fair trial guaranteed by paragraph 1, the Court will examine the complaint under both provisions taken together. In doing so, the Court will examine each of the grounds giving rise to the present complaint, in order to determine whether the proceedings, considered as a whole, were fair (see, with further references, *Huseyn and Others v. Azerbaijan*, nos. 35485/05 and 3 others, § 158, 26 July 2011).

(a) General principles

56. The Court reiterates that the right to an adversarial trial under Article 6 § 1 of the Convention means, in a criminal case, that both prosecution and defence must be given the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party (see *Brandstetter v. Austria*, 28 August 1991, §§ 66-67, Series A no. 211). Article 6 § 3 (b) guarantees the accused "adequate time and facilities for the preparation of his defence" and therefore implies that the

substantive defence activity on his or her behalf may comprise everything which is "necessary" to prepare the main trial. The accused must have the opportunity to organise his or her defence in an appropriate way and without restriction as to the possibility of putting all relevant defence arguments before the trial court and thus of influencing the outcome of the proceedings (see *Can v. Austria,* 30 September 1985, opinion of the Commission, § 53, Series A no. 96; *Connolly v. the United Kingdom*, no. 27245/95, Commission decision of 26 June 1996; and *Mayzit v. Russia*, no. 63378/00, § 78, 20 January 2005).

57. The facilities which everyone charged with a criminal offence should enjoy include the opportunity to acquaint him or herself for the purposes of preparing his or her defence with the results of investigations carried out throughout the proceedings (see *C.G.P. v. the Netherlands* (dec.), no. 29835/96, 15 January 1997, and *Foucher v. France*, 18 March 1997, §§ 31-38, *Reports of Judgments and Decisions* 1997-II). The accused must be given unrestricted access to the case file (*Matanović v. Croatia*, no. 2742/12, § 159, 4 April 2017). The issue of the adequacy of the time and facilities afforded to an accused must be assessed in the light of the circumstances of each particular case (*Khodorkovskiy and Lebedev v. Russia*, nos. 11082/06 and 13772/05, § 579, 25 July 2013).

58. The right to an adversarial trial, quite apart from the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party (compare §§ 56-57 above; compare also *Rowe and Davis v. the United Kingdom* [GC], no. 28901/95, § 60, ECHR 2000-II), also requires, in a criminal case, that the prosecution authorities disclose to the defence all material evidence in their possession for or against the accused (see *Edwards v. the United Kingdom*, 16 December 1992, § 36, Series A no. 247-B, and *Rowe and Davis*, cited above, § 60). The term material evidence cannot be construed narrowly in the sense that it cannot be confined to evidence considered as relevant by the prosecution. Rather, it covers all material in the possession of the authorities with potential relevance, also if not at all considered, or not considered as relevant (compare *Edwards*, cited above, § 36; *Bendenoun v. France*, 24 February 1994, § 52, Series A no. 284; and *Rowe and Davis*, cited above, § 60). Failure to disclose to the defence material evidence, which contains such particulars which could enable the accused to exonerate himself or have his sentence reduced would constitute a refusal of facilities necessary for the preparation of the defence (see *Natunen v. Finland*, no. 21022/04, § 43, 31 March 2009; *Matanović,* cited above, § 157).

59. However, the Convention does not prevent member States from requiring an applicant to give valid reasons for a request that such evidence be disclosed (see *Matanović,* cited above, § 157; *Bendenoun*, cited above, § 52; *C.G.P. v. the Netherlands*, cited above; and *Natunen*, cited above, §§ 43-50). The Court has also held that the entitlement to such disclosure of

material evidence is not an absolute right. In any criminal proceedings there may be competing interests, which must be weighed against the rights of the accused. In some cases it may be necessary to withhold certain evidence from the defence so as to preserve the fundamental rights of another individual or to safeguard an important public interest. However, only such measures restricting the rights of the defence which are strictly necessary are permissible under Article 6 § 1. Moreover, in order to ensure that the accused receives a fair trial, any difficulties caused to the defence by a limitation on its rights must be sufficiently counterbalanced by the procedures followed by the judicial authorities (see *Rowe and Davis*, cited above, § 61, with further references).

(b) Application of these general principles to the present case

60. The Court notes that the applicant complained of his lawyer's not having had sufficient opportunity to acquaint himself, in order to prepare the defence, with the entirety of the telecommunication-surveillance data and the entirety of the electronic files, or at least to be able to identify the relevant data and files, both produced and gathered to an enormous extent in the investigation stage of the proceedings – the compliance of the retrieval as such with the Convention not being in issue here. The Court will deal with this complaint under the separate subsequent headings of access to the case file, disclosure of the telecommunication-surveillance data and disclosure of the electronic case files.

(i) Access to the case file

61. The Court observes that, as of the day of the applicant's detention until the very end of the proceedings, the prosecution and the domestic courts granted the applicant's lawyers access to the paper investigation file (see paragraph 10 above), whose extent has not been submitted to the Court. Upon arrest and later again upon indictment they provided him with a comprehensive overview of the accusations as well as the adduced evidence. They provided him not only with a copy of the investigation file, but also forwarded updates of that file at all times, including copies of the twenty-eight transcripts of telecommunication-surveillance data and around 1,100 printouts of electronic files (see paragraphs 7, 9 and 10 above). The applicant has not claimed, nor is there any other indication, that data, files or documents which formed part of that paper file and/or should have done so because they were the basis for the indictment and conviction were not transmitted to his lawyer early enough in order to allow him to acquaint himself with them before or during the trial and potentially adjust the defence.

62. The Court further notes that the initial access to the paper file was granted in November 2011, while the trial started in June 2012 and lasted until December 2012. Within this frame of time, the possibilities to access

the file were essentially unrestricted. Therefore, the Court considers that the applicant's lawyer had the possibility to acquaint himself with the investigation file, regardless of the specific numbers of pages and volumes of that file. This is all the more true as the applicant had two other lawyers, who, according to the submissions of the parties, never requested access to the investigation file. The possibilities of contact between the lawyer and the detained applicant in order to prepare the defence were also not unduly restricted. The Court therefore considers that there were sufficient possibilities for the applicant's lawyer to discuss the investigation file in detail with him, in order to effectively prepare the defence.

63. Moreover, the Court observes that the indeed enormous amount of telecommunication-surveillance data and electronic files produced and collected during the investigation were only to a minor extent included in the paper file. As they were considered irrelevant to the charges by the police and/or the prosecution, they were in fact kept in storage on police computers. In this connection, the Court further observes that the prosecution and the courts were, in acquainting themselves with the case, also essentially confined to the investigation file and the evidence later produced in the hearing. They did make use of neither the entirety nor a single one of those other files and subsequently based neither the applicant's indictment nor his conviction on them. Against this background, the time afforded to allow the defence to acquaint itself with the relatively extensive results of the investigation was sufficient.

64. In view of this, the Court finds that in the circumstances of the case the applicant and his lawyer were granted sufficient access to the file in order to allow for preparation for the applicant's trial.

(ii) Disclosure of the telecommunication-surveillance data

65. The Court observes that the prosecution and the domestic courts, without having required the applicant to provide specific reasons for his application, decided to allow for disclosure of the entirety of the telecommunication-surveillance data only a few days after he had applied for it (see paragraph 11 above). The Court furthermore notes that, subsequently, although the authorities did not provide the applicant's lawyer with a copy of the telecommunication-surveillance data, he was allowed to examine that data initially in the police premises upon appointment during regular opening hours and on the presence of a police officer, and, as of 9 May 2012 additionally upon appointment during regular opening hours on the prison premises together with the applicant, also in the presence of a police officer (see paragraph 19 above). Moreover, even if the Court does not consider it necessary for the applicant to explain his defence strategy, the Court observes that the applicant has, neither in the domestic proceedings nor before the Court, specified in what particular manner the invoked restrictions had interfered with his opportunity to defend himself.

66. The applicant complained in this connection, that a copy of the telecommunication-surveillance data had not been handed over to his lawyer and that the data could not be examined without a police officer present. The Government claimed that these measures had been justified in order to protect the rights of all those whose conversations may have been recorded. There had been a statutory obligation to prevent private and even intimate parts of the recorded conversations being listened to, which had been essential for the legitimisation of telecommunication surveillance as such, and which therefore had had to be enforced by the presence of a police officer. These explanations, which the applicant essentially did not oppose, appear reasonable to the Court.

67. The applicant moreover complained that it had not been possible for his lawyer to listen to and read the entirety of the telecommunication-surveillance data, due to the time constraints and its significant volume. The Government were of the opinion that it had not been necessary to allow for the possibility to listen to each and every recording and read each and every text message. The Court is indeed satisfied that, in view of the complexity of the criminal proceedings at issue (see *Gregačević v. Croatia*, no. 58331/09, § 53, 10 July 2012), it was not necessary to allow for the opportunity that the applicant's lawyer read through and listen to each and every single item of the telecommunication-surveillance data. Rather, it was, in principle, sufficient to allow an effective opportunity for the applicant's lawyer to analyse the recordings and text messages in order to identify and then listen or read those which he considered to be of relevance. In this connection, the Court is mindful of the fact that modern investigation means may indeed produce, as in the present case, enormous amounts of data, the integration of which into the criminal proceedings should not cause unnecessary delays to those proceedings. It therefore considers that the applicant's right to disclosure must not be confused with his right of access to all material already considered as relevant by the authorities, which will generally require for the possibility to comprehend the material in its entirety (see, as an exception, *Khodorkovskiy and Lebedev*, cited above, §§ 581-85).

68. In so far as the applicant complained that his lawyer had not been, given sufficient opportunity to identify relevant recordings and text messages, the Court observes that the responsible police officer supported the applicant's lawyer, who was likely not acquainted with the software to analyse the telecommunication-surveillance data. Initially, the police provided the applicant's lawyer with the data produced in respect of certain search parameters of his choosing (see paragraph 12 above). Subsequently, it provided him with lists containing substantial amounts of information on the retrieved telecommunication data (see paragraph 15 above). In so far as the applicant alleged that the lists had fallen short of what he had requested, he has not substantiated why it would not have been possible to identify

relevant data by substantially reducing the amount to actually listen to on the basis of search parameters and the provided lists. In fact, it appears that it was possible to narrow down the search by looking for specific telephone lines, for connections between specific telephones lines, within a certain frame of time, overall allowing for substantial reduction of the data with potential relevance. Moreover, the applicant's lawyer, who could have been expected to arrange for at least some shift in the emphasis of his work (see *Mattick v. Germany* (dec.), no. 62116/00, ECHR 2005-VII, with further references), even if appointments with the police and in prison were, in particular due to limited opening hours (see paragraphs 11 and 19), difficult to arrange, only managed to examine the data on twenty-two occasions within more than one year, apparently never together with the applicant on the prison premises and not after 31 October 2012. At the same time, he neither made use of the possibility to have a judicial employee replace him, as the court had suggested, nor can it be taken from the applicant's submissions that his two other lawyers engaged substantially in the analysing, listening and reading exercise. It also has to be taken into account that the applicant, who had been the one subjected to the surveillance measures, would have known best what specific telecommunication-surveillance data to look for. The Court therefore cannot see that the authorities provided the defence only with an ineffective opportunity to identify the relevant files.

69. In view of this, the Court finds that in the circumstances of the case the applicant had sufficient time to acquaint himself with the telecommunication-surveillance data.

(iii) Disclosure of the electronic files

70. The Court observes that the applicant's lawyer could have accessed – but never did – the entirety of the electronic files on the premises of the criminal police as of the end of February 2012, when he must also have been aware of the fact that electronic files – apart from his own – had been retrieved (see paragraphs 8, 10 and 34 above). The Court furthermore observes that, after the applicant had only on 3 April 2012 (see paragraph 21 above) requested disclosure of the entirety of the electronic files, the authorities did not object in principle, but were ready to allow for examination. In this connection, the Court notes that on 22 May 2012 the authorities provided the applicant's lawyer with a copy of the entirety of the electronic files. This copy was, however, readable only with an expensive software which lawyers and private individuals appear to not usually have at their disposal (see paragraphs 8, 25 above). Therefore, the events following the request of 3 April 2012, in particular the dispute concerning the question whether the state should bear the cost for the expensive special forensic-data-analysis program (see paragraphs 26, 32 above), disclose practical difficulties in view of the encryptment of an enormous amount of data. The

Court moreover notes that only in July 2012, the defence asked to be provided with a copy in a format readable with freely available software, a request to which the authorities agreed on short notice (see paragraph 33 above). The applicant's lawyer provided two hard discs at the end of July 2012, and the data was provided on 4 September 2012 (see paragraph 33 above). Moreover, even if the Court does not consider it necessary for the applicant to explain his defence strategy, the Court observes that the applicant has, neither in the domestic proceedings nor before the Court, specified in what particular manner the invoked restrictions had interfered with his opportunity to defend himself.

71. As to the complaint that the applicant's lawyer was not given sufficient opportunities to acquaint himself with the entirety of the files, the Court considers that the access was, for the reasons stated above (see paragraph 67 above), sufficient in principle to allow an effective opportunity for the applicant's lawyer to analyse the electronic files in order to identify those which he considered to be of relevance.

72. As to the complaint that applicant's lawyer had indeed not been given sufficient opportunity to identify the relevant files, the Court observes, that the exact nature of the 14 million electronic files, which stemmed from the seizure of a range of storage media, cannot be taken from the submissions of the parties. Their nature must, however, have allowed for an initial identification of files with potential relevance to the criminal proceedings, allowing already for a substantial reduction of the files to be actually looked at. Moreover, the electronic files must have stemmed from different people – amongst them also the applicant, giving him the best knowledge of their content – and from over a long period of time, allowing for further reduction of the search parameters. The Court therefore considers it to have been sufficient that the applicant's lawyer, who could have been expected to arrange for at least some shift in the emphasis of his work (*Mattick*, cited above, with further references), had at least from 4 September 2012, the day on which he was provided a full copy readable with software available free of charge, to 21 December 2012, the day judgment was rendered, which amounts to three and a half months – that is to say sufficient time – to analyse the electronic files in order to identify those which he considered to be of relevance.

73. Even assuming the applicant's lawyer had only been able to acquaint himself with the files from 4 September 2012, the mere fact that the court proceedings had already begun does not render the preparatory time insufficient. The Court has already held that Article 6 § 3 (b) of the Convention does not require the preparation of a trial lasting over a certain period of time to be completed before the first hearing. The question rather is whether the amount of time actually available before the end of the hearing was sufficient (*Mattick*, cited above).

74. The foregoing considerations are sufficient to enable the Court to conclude that in the circumstances of the case the applicant had sufficient time to acquaint himself with the electronic files.

(c) Conclusion

75. There has accordingly been no violation of Article 6 § 1 of the Convention taken together with Article 6 § 3 (b) of the Convention. The proceedings, considered as a whole, were fair.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the application admissible;

2. *Holds* that there has been no violation of Article 6 § 1 of the Convention taken together with Article 6 § 3 (b) of the Convention.

Done in English, and notified in writing on 25 July 2019, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Claudia Westerdiek
Registrar

Yonko Grozev
President