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

FIFTH SECTION

DECISION

Application no. 3599/10
Hannes TRETTER and Others
against Austria

The European Court of Human Rights (Fifth Section), sitting on 29 September 2020 as a Committee composed of:

Latif Hüseynov, *President,*
Gabriele Kucsko-Stadlmayer,
Lado Chanturia, *judges,*

and Anne-Marie Dougin, *Acting Deputy Section Registrar,*

Having regard to the above application lodged on 15 January 2010,

Having regard to the observations submitted by the respondent Government and the observations in reply submitted by the applicants,

Having regard to the comments submitted by Privacy International, which had been given leave to intervene in the written procedure (Article 36 § 2 of the Convention and Rule 44 § 3 of the Rules of Court),

Having deliberated, decides as follows:

INTRODUCTION

1. This case concerns the alleged failure to put in place a system of effective remedies to protect the applicants' rights with regard to certain powers for the police authorities to use personal data for fulfilling their tasks under the Security Police Act.

THE FACTS

2. The applicants, Mr Hannes Tretter and twenty-two others, are represented before the Court by Mr E. Scheucher, a lawyer practising in Vienna. They are Austrian nationals and one company with its seat in Austria, respectively. A list of the applicants is set out in the appendix.

3. The Austrian Government ("the Government") were represented by their Agent, Ambassador H. Tichy, Head of the International Law Department at the Federal Ministry for Europe, Integration and Foreign Affairs.

A. The circumstances of the case

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

5. On 1 January 2008 Federal Law no. 114/2007 containing an amendment to the Security Police Act (*Sicherheitspolizeigesetz*; hereinafter: "the SPA") entered into force. It extended, in particular, the powers of the police authorities to use personal data of suspects and certain other categories of persons for the purposes of operative or strategic analysis and to request personal data of telephone, mobile phone and internet users from telecommunications providers.

6. The applicants, who were university professors of law, lawyers, judges, doctors, accountants, employees, businessmen, a journalist and a company, lodged a complaint under Article 140 of the Federal Constitution (*Bundesverfassungsgesetz*) with the Constitutional Court requesting it to review the constitutionality of section 53(1), (3a), (3b) and (4), of section 53a(1) and (2), of section 54(2 no. 3), (3), (4) and (4b) of the Security Police Act and of section 24 of the Data Protection Act 2000 (*Datenschutzgesetz 2000*).

7. The applicants did not allege that any of these measures had in fact been ordered or implemented against them, nor that they had been affected by measures directed against other persons. However, they contended that - like all other people in Austria - they might be subjected to such measures at any point in time without prior or subsequent notification and without having any effective remedy at their disposal. They submitted in particular that they all resided in Austria and each of them had a mobile and/or landline phone and internet access with an IP-address. In any event, in their respective professions they also communicated via telephone and internet with persons who were of interest to the security authorities. There was therefore some probability that they would be subjected to the impugned measures under the Security Police Act.

8. On 1 July 2009 the Constitutional Court rejected the applicants' complaint as being inadmissible (decision of 1 July 2009, G 147, 148/08-14). It noted that only persons with whose rights a law interfered directly, without being applied through a decision of a court or an administrative authority, had the right to lodge a complaint under Article 140 of the Federal Constitution. The applicants had not submitted that the police authorities had requested any information about them or taken any measures against them under the contested provisions. They had

merely asserted that they were likely to be affected by these provisions as they were mobile phone and internet users and exercised certain professions. In the Constitutional Court's view this was not enough to show that they were directly affected by the said provisions.

9. Referring to the case-law of the European Court of Human Rights (*Klass and Others v. Germany*, 6 September 1978, Series A no. 28, and *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-XI), the Constitutional Court observed that section 53(3a) and (3b) of the SPA did not regulate secret surveillance of communications but merely empowered the police authorities to obtain specific information about telephone or internet users from providers of telecommunication services. Since the circumstances at issue were therefore distinct from those in the Court's case-law, the applicants' complaint in respect of these provisions was inadmissible on that ground alone.

10. If the applicants had reason to believe that their data had been requested or processed by the police authorities on the basis of the contested provisions, they had remedies under the Data Protection Act 2000 at their disposal, in particular the right to obtain information under section 26, the right to request the destruction of data under section 27 and the right to lodge a complaint or an application with the Data Protection Commission under sections 30 and 31 of that said Act.

11. Furthermore, the Constitutional Court observed that a system of safeguards was in place: pursuant to section 91c of the Security Police Act the police authorities had to inform the independent Legal Protection Commissioner (*Rechtsschutzbeauftragter*), *inter alia*, of the reasons for any measures of covert investigation and surveillance through covert audio and video recordings under section 54(3) and (4) of the Security Police Act. In the context of observation of certain dangerous groupings (*erweiterte Gefahrenerforschung*), they had to obtain prior authorisation from the Legal Protection Commissioner for the use of such measures.

12. They also had to notify him of requests for information about telephone or internet users under section 53(3a) and (3b) and about measures recognising registration plates under section 54(4b) of the said Act.

13. The Minister for the Interior had to be notified without delay of measures under section 53a(2) of the Security Police Act, that is of the processing of personal data for operational or strategic analysis. In turn, the Minister had to inform the Legal Protection Commissioner, who could comment within three days.

14. In cases in which the Legal Protection Commissioner considered that an individual's right had been violated by the use of personal data he was entitled to inform the person concerned or, where that was not possible pursuant to section 26(2) of the Data Protection Act 2000, he was entitled to lodge a complaint with the Data Protection Commission.

15. Finally, the Constitutional Court also rejected the applicants' complaint under section 24 of the Data Protection Act because the applicants had not elaborated whether and how this provision had interfered with their rights. With regard to their general complaint about the lack of notification and an effective remedy, it referred to the reasons set out in respect of the contested provisions of the Security Police Act.

B. Relevant domestic law

(a) The Security Police Act ("SPA")

16. A comprehensive summary of the general tasks and the structure of the police authorities under the SPA is contained in the Court's decision in the case of *Ringler v. Austria* (dec.) [Committee], no. 2309/10, §§ 14-17, 12 May 2020.

(b) Powers to collect, process and transmit personal data

17. Sections 51 to 54 of the SPA regulate the use of personal data (*personenbezogene Daten*) in the context of security police tasks.

(i) General authorisation to use personal data under section 53(1) and (2):

18. Section 53(1) of the SPA sets out a list of tasks for which the police authorities may generally collect and process personal data, unless covered by other, more specific provisions. Dragnet investigations (*Rasterfahndung*) are not allowed, pursuant to section 53(2). Those tasks are

a) providing assistance in case of immediate threat to life, health, security or property of persons;
b) averting criminal organisations;
c) observation of groupings from which severe criminal threats to public security must be expected (*erweiterte Gefahrenerforschung*; hereinafter: extended observation of dangerous groupings);
d) averting intentional criminal offences;
e) prevention of criminal offences against life, health, morals, liberty, property, environment or repeat offences;
f) searches for wanted persons;
g) preservation of public order at specific events.

19. Since a law amendment in 2016, the extended observation of dangerous groupings is no longer the task of the security police.

(ii) Communications data from telecommunications providers under section 53(3a) and (3b)

20. A comprehensive summary of the police authorities' powers to request personal data of telephone/mobile phone and internet users from

telecommunications providers under section 53(3a) and (3b) of the SPA is contained in the case of *Ringler* (cited above, §§ 20-23).

(iii) Other sources of personal data under section 53(4)

21. Section 53(4) allows the police authorities to collect and process personal data for the purposes listed in section 53(1) from all other available sources than the one listed in section 53(2)-(3b), in particular, by accessing data available to the general public.

(iv) Compilation of person or object-related files under section 53a(1)

22. Section 53a(1) regulates the compilation of person or object-related files for certain police operations, such as searches for wanted persons, preservation of public order at specific events, protection of persons or buildings and assistance in case of immediate threat to life, health, security or property of persons.

23. Depending on the category of the person or object (for example, applicant, wanted person, person or object at risk, witness) the police authorities may process certain personal data making it possible to contact and/or to identify the person. For wanted persons they may, for example, also process their photo.

(v) Operative and strategic analysis under section 53a(2)

24. Section 53a(2) regulates operative and strategic analysis to avert criminal organisations or intentional criminal offences and to prevent criminal offences if a repeat offence is likely.

25. Depending on the category of the person (victim, threatened person, witness, informant, suspect or contact person if the contact with the suspect is not only by coincidence and if there are reasons to believe that information on the suspect may be obtained through that person) the police authorities may process a broad range of personal data and link it to case-related data in order to, for example, identify serial offenders or criminal organisations.

(vi) Observations, covert investigations, covert audio and video recordings under section 54(2)-(4)

26. Section 54(2)-(4) empowers the police authorities to collect personal data by means of observations, covert investigations and covert audio and video recordings.

27. Observations under section 54(2) are only allowed for the purpose of

a) extended observation of dangerous groupings;
b) prevention of criminal offences against life, health, morals, liberty, property or environment planned by a specific person;

c) averting a criminal organisation or intentional criminal offences if it would otherwise be jeopardised or made considerably more difficult.

28. Covert investigations under section 54(3) and covert audio and video recordings under section 54(4) are only allowed for the purposes listed under 54(2a) and (2c) (see paragraph 27 above). Under lit.a, it is additionally required that the extended observation of dangerous groupings with other means would be without prospects of success, and under lit.c, that - in the context of criminal organisations - offences must be expected that are punishable by more than one year's imprisonment.

29. Furthermore, the police authorities are not empowered to audio record statements which are not made in public and not in the presence of the investigator. They are not empowered either to video record conduct which is outside the public sphere and not within the visual reach of the investigator.

30. The extended observation of dangerous groupings is no longer a task of the security police (see paragraph 19 above).

(vii) Recognition devices for registration plates under section 54(4b)

31. Section 54(4b) allows the police authorities to use recognition devices for registration plates of motor vehicles for the purpose of searches for wanted persons. The use of such devices is limited to one month. The data obtained is to be deleted as soon as it is no longer needed for the purpose of the specific search.

32. This provision - in a later version including more powers - was repealed after a judgment of the Constitutional Court on 11 December 2019.

(c) Legal Protection

33. In the context of the security police tasks, a comprehensive summary of the provisions governing the general principles for the protection of personal data, the role of the independent Legal Protection Commissioner, the tasks of the independent Data Protection Authority (former Data Protection Commission), the rules on notification and information for the data subject, the rules on rectification, restriction or deletion of personal data and the system of domestic remedies is contained in the case of *Ringler* (cited above, §§ 24-45).

34. In addition to the rules on notification summarised in *Ringler* (cited above, § 35), the police authorities must pursuant to section 91c of the SPA:

- notify the Legal Protection Commissioner of the use of recognition devices for registration plates under 54(4b) of the SPA (see paragraph 31 above);
- notify the Legal Protection Commissioner of the collection of personal data through covert investigations under section 54(3) of

the SPA or through covert audio and video recordings under section 54(4) of the SPA and give reasons for the use of these measures (see paragraph 28 above);
- obtain prior authorisation from the Legal Protection Commissioner if they intend to use covert investigations under section 54(3) of the SPA or covert audio and video recordings under section 54(4) of the SPA in the context of the extended observation of dangerous groupings (see paragraph 28 above);
- inform the Federal Minister of the Interior of their intention to carry out an operative and strategic analysis of personal data pursuant to section 53a(2) of the SPA (see paragraph 24 above); The Minister has to give the Legal Protection Commissioner the possibility to comment within three days. The operative or strategic analysis of personal data may not be carried out before the expiry of this time-limit.

COMPLAINTS

35. The applicants complained under Articles 8 and 10 of the Convention that the powers provided to the police authorities under section 53(1), (3a), (3b) and (4), section 53a(1) and (2), section 54(2), (3), (4) and (4b) of the SPA and the lack of notification under section 24 of the Data Protection Act 2000 entailed by their very existence an interference with their right to respect for their private life, correspondence and freedom of expression.

36. The applicants further complained under Article 13 of the Convention that they did not have any effective remedy in respect of the alleged violations of Articles 8 and 10 of the Convention.

THE LAW

A. Complaint under Article 8 of the Convention

37. The applicants relied on 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) The Government

38. The Government were of the view that the applicants had no right to challenge the impugned legislation *in abstracto* and that they had failed to exhaust domestic remedies.

39. The applicants had not alleged that they had been subjected to any measures, but merely pointed out that having a driving licence and being users of telephones/the internet they might be affected at any time by the compilation and surveillance measures.

40. However, the secret investigation measures at issue must be distinguished from cases in which the Court has exceptionally accepted an application to challenge a legislation *in abstracto*, because the impugned provisions did not give powers to collect the content of communication, but only to compile and process communications data.

41. Furthermore, only persons who had registered a motor vehicle could possibly be affected by the recognition devices for registration plates under section 54(4b) of the SPA, but the applicants had not made clear which of them had in fact such a registration. Persons affected by person or object-related files under section 53a(1) of the SPA were obviously aware of the use of their data because they were in contact with the police authorities.

42. Generally, there were no indications that the applicants belonged to a group which had an increased risk of being affected by the measures at issue.

43. Nevertheless, the Austrian legal system provided effective and adequate protection against abuse, but the applicants failed to make use of any remedy. As well as being able to notify the data subject, the police authorities had an obligation to do so if retained data had been used. Furthermore, a data subject had also the right to request information, which could be made on the basis of mere suspicion of a data compilation, and the police authorities were obliged to respond.

44. In cases where statutory restrictions on notification and information applied - which was in particular applicable to the use of personal data for preventing, avoiding and prosecuting criminal offences - the review by the Legal Protection Commissioner compensated for the data subject's inability to challenge the legality of a measure. The commissioner was also obliged to notify the data subject or to lodge a complaint with the Data Protection Commission.

45. Furthermore, the applicants had the right to lodge a complaint with the independent Data Protection Commission for failure to act or to challenge the reply of the police authorities. Also, anyone who suspected an infringement of his data protection rights had the right to apply directly to that commission. Such an application did not require a specific police authority to be named, but the commission was obliged to investigate whether there had been any data compilation, to review the legality of the

measures, to remedy a possible infringement of data protection rights and to notify the applicant as to how his or her application had been dealt with.

46. Those complaints and applications were effective legal remedies because the police authorities were obliged to implement the commission's decisions, which were further subject to judicial review.

(b) The applicants

47. The applicants argued that they were entitled to claim to be the victim of a violation because they had no effective remedy at their disposal.

48. None of the remedies provided for in the Data Protection Act 2000 were available to them because the police authorities were not obliged to notify the data subject of any measure, even if there was no longer an interest in secrecy. Even though section 24 of the Data Protection Act 2000 stipulated a general notification obligation, it also included broad and blanket exceptions from this obligation, which were foremost applicable to measures under section 53(3a) of the SPA.

49. Furthermore, the control exercised by the Legal Protection Commissioner was not sufficient to compensate the lack of individual remedies. While the police authorities had to inform the commissioner of certain measures taken under the impugned provisions, it was at the commissioner's discretion to inform the person concerned or to bring a case before the Data Protection Commission.

50. The information rights under section 26 of the Data Protection Act 2000 were not effective either because the individual had to make such a request into the dark on the basis of mere suspicion and did not know which unit of the police authorities to address. A complaint with the Data Protection Commission was thus not an effective remedy either. Consequently, a data subject would only learn that a telecommunications provider had transmitted personal data to the police if the measure ultimately resulted in criminal court proceedings.

51. Relying on the Court's case-law (*Klass and Others v. Germany*, 6 September 1978, Series A no. 28; *Malone v. the United Kingdom*, 2 August 1984, Series A no. 82; *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006 XI; and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 6, 28 June 2007), they argued that they had to expect anytime that telecommunications providers would transmit to the police authorities their communications data that was stored for billing or technical reasons. All of them had a permanent place of residence in Austria, a mobile phone and/or a land line and internet access, which they used regularly.

52. In the event of measures against a criminal offender, there would be not only an interference with his/her rights and the rights of persons accompanying him/her, but also with the rights of persons who communicated by chance with the offender via telecommunication devices.

Measures under sections 53(3a) of the SPA were also not limited to certain offences.

53. Finally, they submitted that, even though not all the applicants had registered a motor vehicle, they all had a driving licence. Thus, they could be subjected to the measures under section 54(4b) of the SPA.

(c) The third party

54. Privacy International pointed out that access to non-content data or more specific communications data could also be highly invasive and allowed a comprehensive view into a person's private life. Laws providing for State access to such data as well as requests to telecommunications providers continued to proliferate. A distinction between communications and content data became increasingly insignificant.

(d) The Court's assessment

(i) Preliminary observations

55. The Court observes that the applicants have not alleged that they were subjected to any of the measures foreseen in the SPA, but were affected by the mere existence of the legislation as users of telephones, the internet and as holders of a driving licence.

56. The Court notes therefore that the applicants only brought forward arguments for their *victim status* in regard to requests for communications data from telecommunications providers under section 53(3a) and (3b) of the SPA and in regard to recognition devices for registration plates under section 54(4b) of the SPA.

57. Accordingly, the Court will only examine in detail the complaints about measures under section 53(3a) and (3b) and section 54(4b) of the SPA. Section 24 of the Data Protection Act 2000, which contains the rules on notification, taken alone cannot constitute an interference, but must be examined in connection with each measure.

58. Even though the measures do not concern surveillance of communications content, requesting communications data and recognising registration plates also raise privacy issues capable of engaging the protection of Article 8 of the Convention. In the context of personal data, the Court has found that the term 'private life' must not be interpreted restrictively (*Benedik v. Slovenia*, no. 62357/14, §§ 102-104, 24 April 2018 with further references, and *Ben Faiza v. France*, no. 31446/12, § 66, 8 February 2018 concerning, *inter alia,* the numbers dialled, the date and duration of telephone calls).

59. The present case does not concern retained data *(Vorratsdaten)* because the impugned provisions of the SPA, as in force at the time of the Constitutional Court's judgment on 1 July 2009 and as they stand at the time of the present examination, did not introduce a specific obligation for

telecommunications providers to retain data for the purpose of the investigation, detection and prosecution of crime. Thus, the notification obligation under section 53 (3c) of the SPA (see paragraph 43 above) is not relevant for the present examination.

60. The Court does not need to examine whether the applicants complied with the rule of exhaustion of domestic remedies as their application is in any event inadmissible for the reasons set out below.

(ii) Victim status

61. As to the applicants' victim status, the Court has constantly held that its task is not normally to review the relevant law and practice *in abstracto*, but to determine whether the manner in which they were applied to or affected the applicant gave rise to a violation of the Convention (see, *inter alia*, *Klass and Others*, cited above, § 33, and more recently *Szabó and Vissy v. Hungary*, no. 37138/14, § 32, 12 January 2016, *and Kosaité-Cypiené and Others v. Lithuania*, no. 69489/12, § 67, 4 June 2019).

62. However, in recognition of the particular features of secret surveillance measures, the Court has accepted that, under certain circumstances, an individual may claim to be a victim on account of the mere existence of legislation (*Szabó and Vissy*, cited above, § 33). By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if she/he is able to show that, due to her/his personal situation, she/he is potentially at risk of being subjected to such measures (*Roman Zakharov v. Russia* ([GC], no. 47143/06, § 171, ECHR 2015 which concerned covert interception of mobile telephone communications). The Court will also apply those conditions for victim status to the circumstances of the present case, which did not concern content data, but communications data and recognition of registration plates.

63. Turning to the first condition, that is the scope of the legislation, the applicants may possibly be affected by measures foreseen under section 53(3a) and (3b) of the SPA because all users of communication services are potentially affected (*Roman Zakharov*, cited above, § 171).

64. However, they cannot claim to be possibly affected by recognition devices for registration plates. Section 54(4b) of the SPA, as in force at the time of the Constitutional Court's decision of 1 July 2009, allowed the use of such recognition devices only for searches for wanted persons. That means that an individual was either directly affected as a wanted person and could challenge the specific measure, or was not affected at all. The applicants of the present application neither alleged that they were wanted persons nor was it possible that they were unaware of this because then they would have been caught by the police as persons with known work places

and known places of residence in Austria. Consequently, they could only be possibly affected by that measure if a wanted person had used their car. The applicants conceded that not all of them had registered a motor vehicle, but they did not specify which of them had one. The Court is therefore not able to determine which applicant could be possibly affected and will thus limit its further examination to the measures foreseen under 53(3a) and (3b) of the SPA.

65. As to the second condition, the Court has identified the availability of an effective domestic remedy as decisive in determining whether there is greater need for scrutiny by the Court and an exception to the rule denying individuals the right to challenge a law *in abstracto* is justified (*Roman Zakharov*, cited above, § 171). The Court has linked limitations on notification and information with the effectiveness of the remedies (see, for example, *Klass and others*, cited above, §§ 58-59; *Roman Zakharov*, cited above, §§ 286-87, and *Szabó and Vissy*, cited above, § 86). There is, in principle, little scope for recourse to the courts by the individual concerned unless she/he is advised of the measures taken without her/his knowledge and thus able retrospectively to challenge their legality (*Klass and Others*, cited above § 57).

66. In this context, the Court refers to its assessment of the domestic law on notification and information for data subjects and to its analysis of the domestic remedies set out in the case of *Ringler* (cited above, §§ 69-78).

(iii) Conclusion

67. As set out in *Ringler* (cited above, § 79), the Court finds that, although the notification obligations lacked practical significance, a system of effective remedies with access to judicial control existed. The applicants in the present case did not demonstrate that they had tried to seek any information under section 26 of the Data Protection Act 2000 or had lodged a complaint with the Data Protection Commission under sections 30 and 31 of the Data Protection Act 2000. In such a situation, a widespread suspicion of abuse and thus a review of legislation *in abstracto* is more difficult to justify (see, *mutatis mutandis*, *Kennedy v. the United Kingdom*, no. 26839/05, § 124, 18 May 2010).

68. Even though the applicants referred to their place of residence in Austria and their respective professions, they did not demonstrate for each of them why their personal or professional situation was of a kind that might normally attract the application of measures under section 53(3a) and (3b) of the SPA. With regard to the applicant company, it did not even disclose its field of business. Generally, the applicants only asserted that they were likely to be affected by such measures as phone/mobile phone and internet users. They did not therefore demonstrate that, due to their personal situation, they were potentially at risk of being subjected to those measures

(see *Roman Zakharov*, cited above, § 171). The Constitutional Court therefore rejected their complaints as inadmissible.

69. In regard to the measures foreseen in sections 53(1) and (4), section 53a(1) and (2), section 54(2), (3) and (4) they complained solely in a general manner, without explaining how and why they were possibly affected by the measures (see paragraphs 55 and 56 above). Similarly, they failed to demonstrate that they could be affected by the use of recognition devices for registration plates under section 54(4b) of the SPA (see paragraph 64 above). Thus they did not show that they were in a situation comparable to cases in which the Court has exceptionally examined legislation on secret measures *in abstracto.*

70. Accordingly, the facts of the present case were never such as to allow the applicants to claim to be victims of a violation of their rights under Article 8 of the Convention. Their complaints are thus incompatible *ratione personae* with the provisions of the Convention within the meaning of Article 35 § 3 (a) and must be rejected in accordance with Article 35 § 4.

B. Complaint under Article 10 of the Convention

71. The applicants relied on Article 10 of the Convention, which reads as follows:

> "1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. ...
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

(a) The Government

72. The Government were of the view that the measures at issue did not hinder the reception and transmission of information. It was thus doubtful whether the measures fell within the scope of Article 10 of the Convention. Notwithstanding the above, the applicants lacked victim status for the same reasons as under Article 8 of the Convention.

(b) The applicants

73. The applicants argued that the impugned provisions of the Security Police Act and section 24 of the Data Protection Act 2000 also interfered with their right to freedom of expression. Secret collection and retention of communication data had a "chilling effect" on all users of communications

technologies, such as mobile phones or emails. Even though there was no surveillance of content, communication data might also allow conclusions on the content of a message. This could, for instance, result in sensitive data not being communicated.

(c) The Court's assessment

(i) Preliminary observations

74. The Court will only examine the applicants' complaints with regard to measures under section 53(3a) and (3b) of the SPA because the applicants only put forward arguments concerning communication by phone or internet. The rules on notification under Section 24 of the Data Protection Act 2000 will again not be examined separately, but in connection with the specific measures.

75. The Court also observes that the applicants did not further substantiate or submit any proof of how the existence of those powers for the police authorities affected their individual communication habits via telephone and internet. They solely maintained that such measures had a chilling effect on communicating sensitive data. There is no other information in the Court's possession suggesting that the police authorities' powers under section 53(3a) and (3b) of the SPA have generated a chilling effect for the applicants. Consequently, it is questionable whether Article 10 of the Convention is applicable in the circumstances of the present case (see, *mutatis mutandis*, *Petropavlovskis v. Latvia*, no. 44230/06, §§ 77-87, ECHR 2015).

76. However, the Court does not need to rule on this question as the complaints are in any event inadmissible for the reasons set out below.

(ii) Victim status

77. The Court finds - like under Article 8 of the Convention - that a system of effective remedies with access to judicial control existed (see paragraph 66 above, with references to *Ringler*, cited above, §§ 69-78, and the Constitutional Court´s decision of 1 July 2009, G 147, 148/08-14).

78. The applicants have then failed, as required in cases concerning the review of legislation *in abstracto,* to demonstrate that due to their personal situation they were potentially at risk of being subjected to those measures (see paragraph 62 above). They had solely asserted in a general manner that all of them were likely to be affected as mobile phone users or when communicating via email. Thus, they were not able to show the direct effect of the legislation on their individual communication habits or to refer to particular circumstances in which they had or would in any respect have been inhibited from receiving or imparting information (see, *mutatis mutandis*, *KRONE-Verlag GmbH and Druckerei und Zeitungshaus J. WIMMER Gesellschaft mbH v. Austria,* dec., no. 31564/96,

7 March 2000, in which the Court denied victim status under Article 10 although this had been granted at the domestic level before the Constitutional Court).

79. Accordingly, the facts of the present case were never such as to permit the applicants to claim to be victims of a violation of their rights under Article 10 of the Convention. The complaints are thus incompatible *ratione personae* with the provisions of the Convention within the meaning of Article 35 § 3 (a) and must be rejected in accordance with Article 35 § 4.

C. Complaint under Article 13 of the Convention

80. The applicants relied on Article 13 of the Convention which, insofar as relevant, reads as follows:

> "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority ..."

81. Having declared the complaints under Articles 8 and 10 of the Convention inadmissible, the Court concludes that the applicants have no arguable claims for the purposes of Article 13 of the Convention (see, for the same approach, *Valeriy Fuklev v. Ukraine*, no. 6318/03, § 98, 16 January 2014, and *Lolova and Popova* (dec.), no. 68053/10, § 52, 20 January 2015).

82. It follows that the complaints under Article 13 of the Convention must be rejected as being incompatible *ratione materiae* with the provisions of the Convention, pursuant to Article 35 §§ 3 (a) and 4 of the Convention.

For these reasons, the Court, unanimously,

Declares the application inadmissible.

Done in English and notified in writing on 22 October 2020.

Anne-Marie Dougin	Latif Hüseynov
Acting Deputy Registrar	President

Appendix

	Applicant's name	**Date of Birth**	**Place of Residence**	**Profession**
1.	TRETTER, Hannes	05.07.1951	Vienna	Professor, University of Vienna, Director L. Boltzmann Institute for Human Rights
2.	SCHEUCHER, Ewald	09.11.1960	Vienna	Lawyer
3.	SCHMAUS, Christian	22.10.1973	Gablitz	Lawyer
4.	TSCHOHL, Christof	12.05.1978	Vienna	Lawyer
5.	ZACH, Alexander	10.09.1976	Vienna	Businessman
6.	GREIFENEDER, Martin	06.01.1960	Wels	Judge
7.	FORGO, Nikolaus	27.05.1968	Vienna	Professor of IT law and Legal informatics
8.	HELIGE, Barbara	27.01.1958	Vienna	Judge
9.	HERRNHOFER, Manfred	17.11.1964	Liebenfels	Judge
10.	KIRCHENGAST, Josef	15.03.1951	Vienna	Journalist
11.	LANGER, Martin	16.02.1954	Perchtoldsdorf	Medical Specialist in gynaecology and obstetrics
12.	LECHNER, Eduard	06.06.1956	Vienna	Certified accountant and tax accountant
13.	MIRZAEI, Siroos	22.04.1963	Perchtoldsdorf	Medical Specialist for nuclear medicine
14.	NEUBAUER, Martin	28.02.1966	Vienna	Employee
15.	NILL, Ulrike	09.05.1955	Thalheim	Judge
16.	NOWAK, Manfred	26.06.1950	Vienna	Professor, University of Vienna, Human Rights Lawyer
17.	SCHINDLAUER, Dieter	14.06.1971	Vienna	Scientist, Chairman of Association ZARA
18.	STEINKELLNER, Astrid	08.08.1981	Vienna	Lawyer
19.	WITTMANN-TIWALD, Maria	16.03.1960	Vienna	Judge

20.	PETER, Helmut	02.12.1949	Röthis	Businessman
21.	HAVRANEK, Hannes	27.08.1972	Vienna	Lawyer
22.	Mainland Economic Consultants GmbH		Vienna	Registered company
23.	PROCHASKA, Stefan	21.11.1968	Vienna	Lawyer, Vice-President of the Vienna Bar Association