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

FIRST SECTION

DECISION

Application no. 25578/11
Luca CASARINI
against Italy

The European Court of Human Rights (First Section), sitting on 30 August 2022, 16 April and 5 November 2024 as a Chamber composed of:

Marko Bošnjak*, President*,
Péter Paczolay,
Alena Poláčková,
Erik Wennerström,
Raffaele Sabato,
Lorraine Schembri Orland,
Davor Derenčinović*, judges*,

and Ilse Freiwirth, *Section Registrar,*

Having regard to the above application lodged on 18 April 2011,

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

Having deliberated, decides as follows:

THE FACTS

1. The applicant, Mr Luca Casarini, is an Italian national, who was born in 1967 and lives in Marghera. He was represented before the Court by Ms A. Mascia, a lawyer practising in Vérone.

2. The Italian Government ("the Government") were represented by their Agent, Mr L. D'Ascia, *Avvocato dello Stato*.

3. The facts of the case may be summarised as follows.

4. The Taxpayer Information Service (*Servizio per le informazioni sul contribuente – Serpico*) is a database of the Tax Registry (*Anagrafe tributaria*) which, as provided in Article 1 of Presidential Decree no. 605 of 29 September 1973 ("Decree no. 605/1973"), stores data and information from declarations and complaints addressed to the offices of financial authorities and from related investigations, as well as data and information

that may be relevant for tax purposes (see paragraphs 13 and 20 below). According to the evidence submitted by the applicant and not contested by the Government, it includes information on gas, water, electricity and telephone expenses, interest expenses on liabilities, social security contributions, bank transfers, data on vehicle registration in the public register of automobiles, sports club memberships, and taxpayers' travel expenses, among others.

5. On 19 October 2010 the applicant, a political activist and member of the "No Global" movement, learned from a newspaper article that F.D., an officer of the Revenue Police (*Guardia di finanza*), had unlawfully extracted information concerning him from the Tax Registry, in particular, from the Taxpayer Information Service database, and had passed it to G.A., a journalist working for a well-known Italian magazine. The article also reported that F.D. was accused of having repeatedly accessed the database to collect information concerning public persons at the request of G.A., who then used that information to publish articles on them.

6. On 21 January 2011 the applicant lodged a criminal complaint against F.D. and G.A. with the Milan public prosecutor's office.

7. Meanwhile, in response to reports lodged by the Revenue Police on 23 February, 14 July and 17 September 2010, criminal proceedings had been opened in respect of F.D. and G.A. on suspicion of having unlawfully accessed the Taxpayer Information Service database. The indictment listed three hundred and twenty-eight injured parties, including the applicant.

8. On 8 March 2011, at the end of a plea-bargaining procedure, the Brescia preliminary hearings judge sentenced F.D. and G.A. to suspended sentences of two and one years, respectively.

9. In the judgment, the Brescia preliminary hearings judge stated that while F.D. had the right to access the Taxpayer Information Service database in his capacity as a military officer working in the operations room of the Revenue Police, investigations had shown that in the years 2008 and 2009 he had accessed the database 1,372 times without any justification related to the fulfilment of his duties. The access had been aimed at wrongfully acquiring financial information on prominent figures in the Italian judiciary and cultural, political and institutional spheres, and had been carried out at the request of an unauthorised person, G.A., who had used the information in articles for the magazine he worked for and other newspapers belonging to the same editorial group.

10. It was explained in the judgment that access to the database by military personnel working in operations rooms was recorded on a special internal register which registered the call sign of the squad and the location, place and time of each access. Analysis of those data had shown that the unlawful access had been carried out using F.D.'s personal password and at a time when he was physically present in the operations room. On

11 February 2010 the head of the operations room had reported F.D.'s unlawful activities.

11. The Revenue Police subjected F.D. to disciplinary measures. On 18 October 2010 they suspended him from duty as a precautionary measure and on 21 April 2011 he was stripped of his rank and put at the disposal of another service as a common soldier.

12. On 1 March 2013 the Brescia preliminary investigations judge discontinued the criminal proceedings subsequently brought by the applicant on the basis that F.D. had already been sentenced on the basis of the same facts by the judgment of 8 March 2011.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

A. Relevant domestic law

1. *Presidential Decree no. 605 of 29 September 1973 (Provisions concerning the Tax Registry and the Taxpayers' Tax Identification Number)*

13. Article 1 of Presidential Decree no. 605/1973 sets forth the functions of the Tax Registry. It reads as follows:

> "1. The Tax Registry collects and organises on a national scale data and information from declarations and complaints addressed to the offices of financial authorities and from related investigations, as well as data and information that could be relevant for tax purposes.
>
> 2. The data and information collected are communicated to the Ministry of Finance bodies in charge of assessment and inspection activities relating to tax enforcement and, in particular, for the purpose of assessing overall fiscal capacity and any subsequent rectifications of declarations and assessments ..."

2. *Decree-Law no. 201 of 6 December 2011 (Urgent provisions for economic growth, equity and consolidation of public accounts), converted into law on 22 December 2011 (Law no. 214/2011)*

14. At the date of 28 December 2011, section 11 of Decree-Law no. 201/2011 read as follows:

> "...
>
> 2. As from 1 January 2012, financial operators are obliged to periodically communicate to the Tax Registry the transactions involving the [financial] relationships referred to in Article 7 § 6 of Presidential Decree no. 605 of 29 September 1973, and any information relating to the relationships mentioned above necessary for tax inspections, as well as the amount of the financial transactions referred to in the provision above. The data communicated are filed in the special section of the Tax Registry provided in Article 7 § 6 Presidential Decree no. 605 of 29 September 1973, and subsequent amendments.

3. By order of the Director of the Revenue Agency, after consulting the trade associations of financial operators and the Data Protection Authority, the procedures for the communication mentioned in § 2 shall be established, extending the obligation to communicate also to further information related to the relationships strictly necessary for tax inspections. The order shall also provide for adequate technical and organisational security measures for the transmission and storage of the data, which shall not exceed the maximum time-limits provided for income tax assessment."

15. The order of the Director of the Revenue Agency of 25 March 2013 specified that the data referred to in section 11 of Decree-Law no. 201/2011 should have been deleted by 31 December of the sixth year after the year to which the communication referred.

16. Section 11 of Decree-Law no. 201/2011 was amended by section 16-*quater*, subsection 1, of Decree-Law no. 119 of 23 October 2018, converted into Law no. 136 of 17 December 2018, which currently sets the maximum legal time-limit for storage of those data at ten years.

3. Legislative Decree no. 196 of 30 June 2003 (Personal Data Protection Code)

17. The relevant provisions of the Personal Data Protection Code, which was in force at the material time, read as follows:

Article 3: Principle of necessity of data processing

"Information systems and computer programs shall be configured to minimise the use of personal and identification data so as to avoid processing them when the purposes pursued in each case can be achieved by means of, respectively, anonymous data or appropriate methods which allow the person affected to be identified only when necessary."

Article 7: Right of access to personal data and other rights

"1. The person concerned has the right to obtain confirmation of the existence of personal data concerning him or her, and to have them communicated to him or her in an intelligible form.

2. The person concerned has the right to obtain information concerning:

(a) the origin of the personal data;

(b) the purposes and methods of processing;

(c) the logic applied in the event of electronic processing;

(d) the identification of the data controller, the data processor and the representative appointed in accordance with Article 5 § 2;

(e) the persons or entities or categories thereof to whom the personal data can be communicated ...

3. The person concerned has the right to obtain:

(a) the updating, rectification or, if requested, integration of personal data;

(b) the deletion, anonymisation or blocking of access to data processed in breach of the law, including data whose conservation is not necessary in relation to the purposes for which they were collected and subsequently processed;

...”

Article 11: Arrangements for the processing and categorisation of data

“1. Personal data subject to processing are:

(a) processed lawfully and fairly;

(b) collected and recorded for specific, explicit and legitimate purposes, and further processed in a manner that is compatible with those purposes;

(c) accurate and, where necessary, kept up to date;

(d) relevant, complete and limited to what is necessary in relation to the purposes for which they are collected or subsequently processed;

(e) kept, in a form that allows the identification of the person concerned, for a period not exceeding the time necessary to achieve the objectives for which the data have been collected and subsequently processed.

...”

Article 12: Codes of ethics and good conduct

“1. The Data Protection Authority shall promote within the categories concerned, in compliance with the principle of representativeness and taking into account the guiding criteria of the recommendations of the Council of Europe on personal data processing, the issuance of codes of ethics and good conduct for specific sectors, verify that they comply with laws and regulations, in particular, through the examination of stakeholders’ observations, and contribute to ensure their dissemination and compliance with them.

...

3. Compliance with the provisions contained in the codes referred to in paragraph 1 shall constitute an essential condition for the lawfulness and correctness of personal data processing carried out by private and public entities.

...”

Article 15: Damage arising from data processing

“1. A person who causes damage to a third person as a consequence of the processing of his or her personal data must compensate the person concerned under Article 2050 of the Civil Code.

2. The person concerned is also entitled to obtain compensation for non-pecuniary damage resulting from a breach of Article 11.”

Article 18: Principles applicable to processing by public entities

“...

2. Any processing of personal data by public entities shall be permitted for the performance of their institutional duties only.

3. In processing the data, the public entity shall comply with the requirements and limits established by the present Code, also having regard to the nature of the data, statutes and regulations.

4. Without prejudice to what is provided for in Part II for health professionals and public health bodies, public entities do not have to request the consent of the person concerned.

5. The provisions of Article 25 on data communication and dissemination shall be complied with."

Article 19: Principles applicable to processing of data other than sensitive and judicial data

"1. Processing by a public authority of data other than sensitive and judicial data shall be permitted, without prejudice to what is provided for by Article 18, paragraph 2, even in the absence of a provision of law or regulation expressly providing for it.

2. Communication [of the data] by a public entity to other public entities is allowed when provided for by a statute or regulation. In the absence of such a rule, communication is allowed when it is necessary for the performance of institutional duties ...

3. Communication by a public entity to private persons or public economic entities and dissemination by a public body shall only be allowed when provided for by a statute or regulation."

Article 25 § 1: Prohibition on communication and dissemination

"Communication and dissemination are forbidden ..:

(b) for purposes other than those indicated in the notification of data processing, where required."

Article 29: Data processor

"...

2. If designated, the processor is chosen from among persons who by virtue of their experience, abilities and reliability, provide an adequate guarantee of full compliance with the provisions in force on data processing, including on security measures.

...

4. The tasks entrusted to the data processor shall be specified in writing by the data controller.

5. The processor shall carry out the processing in accordance with the instructions given by the data controller who, by means of periodic monitoring, shall ensure full compliance with the provisions set out in paragraph 2 and with his or her instructions."

Article 30: Persons in charge of data processing

"1. Processing may only be carried out by persons acting under the direct authority of the controller or the processor and in compliance with the instructions received.

2. The appointment shall be made in writing and shall specify the scope of the processing permitted. The same applies to the documented assignment of the physical

person to a unit, for which it is indicated, in writing, the scope of the treatment allowed to operators of that unit."

Article 31: Security obligations

"Personal data which are being processed shall be stored and checked, including in relation to knowledge acquired as a result of technical progress, the nature of the data and the specific features of processing, in such a way as to minimise, through the adoption of appropriate and preventive security measures, the risks of the destruction or loss, even accidental, of the data, unauthorised access, unlawful processing or any processing not in accordance with the purposes for which they were collected."

Article 34: Personal data processing carried out by means of IT tools

"1. Personal data processing carried out by means of IT tools is allowed provided that the following minimum measures are implemented, in compliance with the technical regulation included in Annex B [to the present Code]:

(a) digital authentication;

(b) implementation of authentication credentials management procedures;

(c) use of an authorisation system;

(d) periodic updating of the scope of the permitted data processing in relation to each person in charge of processing, managing and maintaining IT tools;

(e) protection of IT tools and data against unlawful data processing, unauthorised access and specific computer programs;

(f) adoption of procedures for storing back-up copies, restoring the availability of data and systems;

(g) maintaining an up-to-date security policy document;

..."

Article 39: Reporting obligations

"1. The data controller must communicate in advance to the Data Protection Authority the following events:

(a) communication of personal data by a public entity to another public entity not provided for by a statute or regulation, carried out in any form including by agreement;

...

2. Processing subject to reporting under paragraph 1 may begin forty-five days after receipt of the communication, unless the Data Protection Authority decides otherwise at a later date."

Processing by police forces

...

Article 53: Scope and data-processing controllers

"1. The following Articles of this Code shall not apply to the processing of personal data that is carried out either by the Data Processing Centre at the Public Security Department or by the police in respect of data that are intended to be transferred to that

centre under the law, or by other public bodies or public security entities for the purpose of protecting public order and security, or the prevention, detection or suppression of offences as expressly provided for by laws that specifically refer to such processing:

(a) Articles ... 12, ... 18[, 19] ... and ... 39 ...;

...

2. A decree of the Minister of the Interior ... shall identify processing operations referred to in paragraph 1 carried out using IT tools, and the relevant data controllers."

Article 54: Data-processing methods and data flows

"1. In cases where public security authorities or police forces are permitted, in compliance with statutes or regulations in force, to acquire data, information, deeds and documents from other individuals, that acquisition may also be carried out by means of IT tools. To this end, the bodies or offices concerned may avail themselves of agreements aimed at streamlining consultation, by means of IT tools, public registers, lists, records and databases, in accordance with the related provisions and principles set out in Articles 3 and 11. The Ministry of the Interior issues standard agreements, with the agreement of the Data Protection Authority, and sets out connection and access procedures, with the aim of ensuring selective access only to those data that are necessary for the purposes [of the protection of public order and safety, and the prevention, detection or prosecution of criminal offences].

...

4. Police bodies, offices and headquarters periodically verify the requirements under Article 11 including with regard to data processed without using IT tools, and keep them up to date ..."

Article 141: Remedies

"1. The person concerned may file with the Data Protection Authority:

(a) a detailed complaint in accordance with Article 142 in order to report an infringement of personal data-processing rules;

(b) where it is not possible to file a detailed complaint within the meaning of letter (a) above, a report requesting an investigation by the Data Protection Authority into whether those rules have been complied with;

..."

Article 142: Filing of complaints

"1. Complaints must include a description, as detailed as possible, of the facts and circumstances on the basis of which the complaint is being made, of the provisions allegedly infringed and of the measures requested, as well as the identity of the controller, the processor, if known, and the claimant.

..."

Article 143: Complaint procedure

"1. Further to the preliminary investigation, if the complaint is not manifestly ill-founded and the conditions for issuing a decision are met, the Data Protection Authority, even before taking a final decision:

(a) may, before ordering the measures under letter (b) or the prohibition or ban provided in letter (c), invite the data-processing controller ... to stop the behaviour spontaneously;

(b) order the data-processing controller to take appropriate measures or those which are necessary to make the data processing compliant with the regulations in force;

(c) order to stop or prohibit, entirely or in part, data processing which is unlawful or unfair as a result of the failure to adopt the necessary measures under (b), or when, taking account of the nature of the data, the data-processing methods or the effects that those methods may have, there is a concrete risk that a serious prejudice may arise for one or more persons concerned;

(d) may prohibit the data processing of single individuals or categories of individuals in full or in part, which goes against any relevant interest of the community.

2. The measures under paragraph 1 are to be published in the Official Gazette of the Italian Republic if the addressees are not easily identifiable owing to their number or the complexity of investigations."

Article 152: Standard judicial authorities

"1. A standard judicial authority (*autorità giudiziaria ordinaria*) has jurisdiction to settle all disputes concerning the application of the provisions contained in the present Code, including those relating to the decisions of the Data Protection Authority concerning personal data protection or its failure to issue them.

2. In order to institute proceedings concerning all disputes mentioned in paragraph 1 above, an appeal shall be lodged with the registry of the court serving the place of residence of the person whose [personal data] are being processed.

3. The court will decide [a case] sitting in a single-judge composition.

...

12. In the judgment the judge, also by way of derogation from the prohibition provided by Article 4 of Law no. 2248 of 20 March 1865, annex E), when it is necessary also with regard to a decision taken by the public data-protection controller or processor, grants or rejects the appeal, in whole or in part, prescribes the necessary measures, rules on compensation for damages, if any, and charges the unsuccessful party with the costs of the proceedings.

13. A judgment is not subject to an appeal on the merits before a second-instance court; however, it may be subject to an appeal on points of law before the Court of Cassation.

..."

Article 153: The Data Protection Authority

"1. The Data Protection Authority operates in full autonomy and independence of decision and assessment.

2. The Data Protection Authority is a collegial body composed of four members, two of which elected by the Chamber of Deputies and two elected by the Senate of the Republic with limited vote. The members are elected from among persons that ensure independence and who are experts with notorious competence in the fields of both law and informatics.

..."

Article 154: Tasks

"1. [T]he Data Protection Authority ... has the task of ...

(c) prescribing, including on its own initiative, the necessary or appropriate measures to the data controllers to ensure that processing is in compliance with the provisions in force, within the meaning of Article 143;

..."

Article 167: Unlawful data processing

"1. Unless a more serious crime has been committed, a person who, in order to make profit for himself or others or to cause damage to others, processes personal data in violation of the provisions of Articles 18, 19, 23, 123, 126 and 130, or in application of Article 129, shall be sentenced, if the act causes damage, to six to eighteen months' imprisonment, or, if the act represents data communication or dissemination, to six to twenty-four months' imprisonment.

2. Unless a more serious crime has been committed, a person who, in order to make profit for himself or others or to cause damage to others, processes personal data in violation of the provisions of Articles 17, 20, 21, 22 §§ 8 and 11, 25, 26, 27 and 45, shall be sentenced, if the act causes damage, to one to three years' imprisonment."

Article 169: Security measures

"1. A person who, despite being obliged to do so, fails to take the minimum measures provided in Article 33 shall be sentenced to up to two years' imprisonment ...

2. Upon investigation, or in more complex cases also upon an order by the Data Protection Authority, the offender shall be ordered to take measures to regularise the situation within a time-limit not exceeding the period technically necessary to do so, which may be extended either in the event of very complex cases or objective difficulty in completing the task, but which, however should not exceed six months. Sixty days after the deadline, in the event of completion within the time-limit, the Authority may propose to the offender that he or she pay an amount equal to one-quarter of the maximum fine provided for the administrative offence. Completion of the measures imposed and payment of the fine extinguish liability for the offence. ..."

"Annex B: Technical regulation on minimum security measures
Processing by means of IT tools

The following technical procedures are to be adopted by the controller, the processor and the person in charge of processing, where designated, when processing by means of IT tools:

Digital authentication

1. Personal data may be processed by electronic means only if the persons in charge have authentication credentials enabling them to pass an authentication procedure relating to a specific processing operation or set of operations.

2. Authentication credentials consist of a processor identification code associated with a confidential keyword known only to the processor, or an authentication device in the exclusive possession and use of the processor, possibly associated with an

identification code or keyword, or a biometric characteristic of the processor, possibly associated with an identification code or keyword.

3. Each person in charge of processing shall be individually assigned or associated with one or more authentication credentials.

4. The instructions given to the persons in charge of processing shall require them to take the necessary precautions to ensure that the confidential component of the credentials is kept secret and the devices in their exclusive possession and use be stored diligently.

5. When the authentication system provides for it, the password shall consist of at least eight characters or, if the IT tool does not allow it, of the maximum number of characters allowed; it shall not contain references that can be easily traced back to the authorised person and shall be changed by the latter upon first use and at least every six months thereafter. ...

6. The identification code, where used, may not be assigned to other appointees, even at different times.

7. Authentication credentials that have not been used for at least six months shall be deactivated, except for those authorised in advance for technical management purposes.

8. Credentials shall also be deactivated in the event of loss of the authorisation enabling the processor to access personal data.

9. Instructions shall be given to the processor not to leave the IT tool unattended and accessible during a processing session.

...

Authorisation system

12. An authorisation system shall be used where authorisation profiles of different scopes have been identified for processors.

13. Authorisation profiles, for each processor or for homogeneous classes of processors, shall be identified and configured before processing begins, so as to limit access only to the data necessary to perform processing operations.

14. Periodically, and in any event at least annually, the existence of the conditions for maintaining authorisation profiles shall be verified.

Other security measures

15. As part of the periodic update, at least once a year, of the scope of processing allowed to individual processors and persons in charge of the management or maintenance of IT tools, the list of processors may also be drawn up by homogeneous classes of assignment and related authorisation profiles.

16. Personal data shall be protected against the risk of intrusion and against the action of programs referred to in Article 615-quinquies of the Criminal Code, by means of suitable IT tools to be updated at least once every six months.

17. Periodic updates of computer programs aimed at preventing the vulnerability of IT tools and at correcting their flaws shall be performed at least annually. ...”

4. Article 2050 of the Civil Code

18. Article 2050 of the Civil Code sets out a general duty not to harm others in the performance of "dangerous activities". Anyone who causes damage is liable to pay compensation unless he or she can prove that he or she took all the appropriate measures to avoid causing harm.

5. Article 615-ter of the Criminal Code (Unlawful access to a computer system)

19. Article 615-*ter* of the Criminal Code provides for a punishment of up to three years' imprisonment for anyone who unlawfully accesses a computer system protected by security measures. A sentence of up to five years may be imposed if the offender is a public officer or a person in charge of a public service convicted of an abuse of power and violating institutional duties.

6. Decree of the Ministry of the Interior of 24 May 2017

20. The Decree of the Ministry of the Interior of 24 May 2017 defined the different data-processing activities carried out using IT tools for police purposes referred to in Article 53 § 1 of Legislative Decree no. 196/2003. In its Table 58, it identified data processing by the Revenue Police as follows:

> "Name: Website 'Tax Registry for the Revenue Police – ATWeb'
>
> Description of data processing: It allows access to information relating to the entire information base of the Tax Registry and is aimed at combating tax evasion and fraud, in all their manifestations, as well as the performance of economic and financial police duties entrusted to the Revenue Police.
>
> Data Controller: Commander-General of the Revenue Police
>
> ..."

B. Relevant domestic practice

1. Memorandum no. 262434 of 22 November 2006

21. Memorandum no. 262434 of 22 November 2006 of the Commander-General of the Revenue Police set out internal supervision mechanisms to ensure that data processing by the Revenue Police complied with the Personal Data Protection Code.

22. Authorisation to access the Tax Registry was granted to individual officers according to specific "user categories" which restricted access to different levels of information depending on the nature of the tasks they were in charge of. Access was by means of individual passwords and credentials and was registered in order to allow subsequent checks.

23. Since 1 December 2006, the following new security procedures have been in force:

(a) a pop-up window warning users each time they access the databases that searches are allowed only when related to the fulfilment of their professional duties;

(b) a second pop-up window requiring the officer to select from four options the category of tasks for which access to the databases is sought (judicial and security police activities; economic and financial police activities; activities at the request of external entities; and updating files);

(c) a monthly report made available to department chief officers indicating for each officer the date and time of access and the database consulted; on the basis of these reports the department chief officers can verify that on the registered dates and times the officers were actually carrying out tasks requiring access to the databases;

(d) a second report drawn up on the basis of an algorithm based on statistical parameters of normal use of the databases; on the basis of these reports the department chief officers could check specific instances of access that the report had identified as being out of the ordinary.

24. Further security procedures were implemented through Memorandum no. 12501 of 26 April 2012, which strengthened the system controlling access indicated above.

2. Circular no. 124501, protocol no. 359578 of 13 December 2013

25. Circular no. 124501, protocol no. 359578 of 13 December 2013 of the Commander-General of the Revenue Police updated the information technology (IT) rules of the Revenue Police.

26. It set out supervision mechanisms through monthly analytical reports on access carried out by each officer and quarterly statistical reports on specific searches in the databases that stood out because they significantly deviated from the statistical trends of normal use in access requests.

27. It set out that authorisation to access ATWeb was granted to all officers already authorised to access the Tax Registry, allowing access to different levels of information depending on the user category. Using ATWeb, officers are allowed access to several databases, including the Taxpayer Information Service database. This contains “all information of fiscal interest concerning any taxpayer (natural or legal person)”.

28. The Circular established that the officers authorised to access the databases had to comply with the rules set out in Annex B to the Personal Data Protection Code.

3. Memorandum no. 83028 of 23 March 2020

29. Memorandum no. 83028 of 23 March 2020 of the Commander-General of the Revenue Police updated the IT rules of the Revenue Police in the context of the launch on 2 April 2020 of a new platform to access the databases.

30. Since the new platform allowed more in-depth investigations, the Memorandum set out that officers should be trained on using it correctly and that department chief officers should carry out meticulous monitoring of their activities.

4. Decisions of the Data Protection Authority on security of access to the Tax Registry

31. On 14 December 2007 the Data Protection Authority began, of its own motion, an assessment on the compliance with domestic law on data protection of personal data processing carried out on the Tax Registry. By means of decisions issued in the years 2008 to 2011, it identified several shortcomings in the security of access to personal data and, under Article 154 of Legislative Decree no. 196/2003, ordered the tax authorities to put in place a comprehensive set of technological and administrative measures to enhance access security and to make the data processing compliant with the relevant domestic framework.

(a) Decision of the Data Protection Authority on access carried out by tax authorities for tax-collection purposes

32. In a decision of 7 October 2009, the Data Protection Authority identified several shortcomings in the security of access to personal data in the context of tax collection. Responsibility for personal data processing was not clearly identified among tax authorities and the companies carrying out tax collection. Personal data were duplicated and stored in several autonomous databases which resulted in an increased risk of the information being used for purposes other than those for which access had been granted. Tax-collection entities did not set out rules on personal data storage, in particular with regard to searches in the Tax Registry on personal data and data on taxpayers' property. Several inadequate technological measures exposed the data stored in the Tax Registry to misuse of passwords and credentials. Even though according to the relevant legal framework access to personal data stored in the Tax Registry for collecting purposes was allowed only following formal registration of a case (*iscrizione a ruolo*), searches in the database in relation to case files related to tax collection started before 2005 could be carried out without any need to specify the case-file number in relation to which access was sought. Access-authorisation requests were not managed in a way which ensured the timely updating and revocation of authorisation by tax-collection entities.

33. The Data Protection Authority found that tax authorities had not put in place adequate audit procedures on access to personal data in the context of tax collection, in particular having regard to the absence of warning mechanisms, risk analysis on access and search tracking.

34. The Data Protection Authority ordered the tax authorities to put in place a comprehensive set of measures to redress the identified shortcomings within a time range varying from one to eighteen months depending on the complexity of the measure required.

(b) Decisions of the Data Protection Authority on access carried out by entities other than the tax authorities

35. In a decision of 18 September 2008, the Data Protection Authority found that the most serious and urgent issues identified in the context of its assessment of the operation of the Tax Registry concerned the security of access by public and private entities other than the tax authorities (*enti esterni*). The Data Protection Authority observed that approximately ten thousand entities, made up of about seventy-eight thousand users, had access to the Tax Registry by means of several connection systems, on the basis of specific regulations and under the terms of agreements with the tax authorities.

36. In this context, it identified several shortcomings in access security including, among others, the following. Tax authorities lacked knowledge of the total number of users having access to the Tax Registry and of their identity. This compromised their ability to monitor whether the users fulfilled the access requirements and thus to avoid unlawful access and misuse of information. Moreover, several agreements between tax authorities and external entities did not state clearly the purposes for which access had been granted. Some entities had authorised users to access the Tax Registry for purposes other than those identified in the agreements. Users did not have to provide reasons for accessing it, which also resulted in the impossibility to subsequently check the legality of the access. Access to personal data in the Tax Registry was not restricted according to the territorial competence of each entity, which therefore had access to personal data across the entire national territory.

37. The Data Protection Authority identified several inadequate technological measures which exposed the data stored in the Tax Registry to phishing and misuse of passwords and credentials. In some cases, using the same credentials it was possible to carry out simultaneous multiple access from different locations. External entities often assigned the task of managing authorisation to access to the Tax Registry to personnel lacking the professional skills needed to assess authorisation requests and to monitor abuse. Inadequate information concerning former staff's termination of duties led to a situation where authorisation was not immediately revoked when the user ceased to work for the entity having access to the Tax Registry. In some cases, passwords and credentials were passed on and shared among different individuals and authorisation was granted which exceeded the aims pursued. Some entities carried out massive duplication of personal data and created

autonomous databases in breach of the terms of their authorisation to access the Tax Registry.

38. Moreover, the Data Protection Authority identified in relation to each connection system several specific shortcomings, including the possibility of repeatedly downloading a file containing personal data without registering the downloads after the first time and the possibility of accessing sensitive data concerning deductible charges contained in tax declarations without any checks that the access was actually compliant with the relevant domestic law on sensitive data.

39. The Data Protection Authority found that tax authorities did not put in place adequate audit procedures on access to personal data by external entities. In relation to some of the connection systems to the Tax Registry, tax authorities did not monitor the activities of local managers, the number of users authorised by them, or their authorisation profiles and access. Local managers did not have tools to periodically and statistically monitor access; nor did they assess periodically that the authorised users still complied with the access requirements.

40. The Data Protection Authority ordered the tax authorities to put in place a comprehensive set of measures to redress the identified shortcomings within a time range varying from three to twelve months depending on the complexity of the measure required.

41. In a decision of 26 March 2009, the Data Protection Authority observed that the tax authorities had declared that they had put in place some of the measures ordered in the decision of 18 September 2008 and had requested an extension of the deadline set for several others, including the deadline within which it should have banned all access to the Tax Registry by the entities whose connection systems did not comply with the requirements set out by the Data Protection Authority. The tax authorities specified that agreements with approximately nine thousand entities would not be updated or renegotiated before March 2010 and only at that time would the security measures prescribed by the Data Protection Authority be put in place. The Data Protection Authority granted the request for the extension and ordered new measures to be implemented in the transition period to avoid unlawful access and the misuse of personal data. In particular, it ordered the tax authorities to verify that external entities were carrying out checks that each user still had a valid reason to access the Tax Registry, also in relation to the purposes for which access had been granted in the first place, and banning any access which appeared unjustified under the relevant legal framework. If external entities failed to carry out this assessment, tax authorities were to deactivate the credentials of those entities, other than those of the local managers, and inform them that, in order for those credentials to be reactivated, they would have to demonstrate that each user still had a valid reason to access the Tax Registry. The deadline for this measure was set for 31 July 2009. In a decision of 23 July 2009, upon a request of the tax

authorities, the Data Protection Authority extended the deadline to 30 October 2009 in relation to 332 municipalities which had failed to respond to the tax authorities' request to assess their users' access to the Tax Registry.

42. In decisions of 2 July, 17 July, 23 July and 26 November 2009 and 26 March and 2 December 2010, upon requests of the tax authorities, the Data Protection Authority granted extensions of the deadline to put in place security measures in relation to access to the Tax Registry by the National Social Security Institute (*Istituto Nazionale della Previdenza Sociale* – "the INPS"), the National Public Service Social Security Institute (*Istituto nazionale di previdenza per i dipendenti dell'amministrazione pubblica* – "the INPDAP"), the Authority for the Supervision of Public Contracts regarding Works, Services, and Supplies *(Autorità per la vigilanza sui contratti pubblici di lavori, servizi e forniture* – "the AVCP"), the National Social Security and Assistance Entity for Show Business Workers (*Ente nazionale di previdenza e di assistenza per i lavoratori dello spettacolo* – "the ENPALS"), the Agricultural Fund Agency (*Agenzia per le erogazioni in agricoltura* – "the AgEA"), and the chambers of commerce. A new deadline was set for 31 December 2010.

43. In decisions of 21 October 2010 and 16 February 2011, upon requests of the tax authorities, the Data Protection Authority granted extensions to the deadline set out in the decision of 18 September 2008 for tax authorities to verify that approximately nine thousand external entities still had a valid reason to access the Tax Registry, also in relation to the number of users having access within each entity, and to ban any access which appeared unjustified under the relevant legal framework. A new deadline was set for 15 April 2011. The Court has not been informed by the parties of any subsequent development.

C. International materials

1. Recommendation No. R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector

44. The relevant parts of this Recommendation, adopted by the Committee of Ministers on 17 September 1987, read as follows:

Principle 2: Collection of data

"2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

..."

Principle 3: Storage of data

"3.1. As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law.

..."

Principle 4: Use of data by the police

"4. Subject to Principle 5, personal data collected and stored by the police for police purposes should be used exclusively for those purposes."

Principle 5: Communication of data

"5.1. Communication within the police sector

The communication of data between police bodies to be used for police purposes should only be permissible if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

5.2.i. Communication to other public bodies

Communication of data to other public bodies should only be permissible if, in a particular case:

a. there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority, or if

b. these data are indispensable to the recipient to enable him to fulfil his own lawful task and provided that the aim of the collection or processing to be carried out by the recipient is not incompatible with the original processing, and the legal obligations of the communicating body are not contrary to this.

5.2.ii. Furthermore, communication to other public bodies is exceptionally permissible if, in a particular case:

a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if

b. the communication is necessary so as to prevent a serious and imminent danger.

..."

2. Council of Europe Convention for the Protection of Individuals with Regard to the Processing of Personal Data of 18 May 2018

45. The relevant provisions of this Convention, which updated the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS no. 108), read as follows:

Article 2: Definitions

"For the purposes of this Convention:

...

b. ’data processing’ means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data;

...”

Article 5: Legitimacy of data processing and quality of data

“1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, whether public or private, and the rights and freedoms at stake.

2. Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and unambiguous consent of the data subject or of some other legitimate basis laid down by law.

3. Personal data undergoing processing shall be processed lawfully.

4. Personal data undergoing processing shall be:

a. processed fairly and in a transparent manner;

b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is, subject to appropriate safeguards, compatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are processed;

...

e. preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.”

Article 6: Special categories of data

“1. The processing of:

– genetic data;

– personal data relating to offences, criminal proceedings and convictions, and related security measures;

– biometric data uniquely identifying a person;

– personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life,

shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.

2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.”

Article 7: Data security

"1. Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.

..."

Article 10: Additional obligations

"1. Each Party shall provide that controllers and, where applicable, processors, take all appropriate measures to comply with the obligations of this Convention and be able to demonstrate, subject to the domestic legislation adopted in accordance with Article 11, paragraph 3, in particular to the competent supervisory authority provided for in Article 15, that the data processing under their control is in compliance with the provisions of this Convention.

2. Each Party shall provide that controllers and, where applicable, processors, examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects prior to the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

3. Each Party shall provide that controllers, and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

4. Each Party may, having regard to the risks arising for the interests, rights and fundamental freedoms of the data subjects, adapt the application of the provisions of paragraphs 1, 2 and 3 in the law giving effect to the provisions of this Convention, according to the nature and volume of the data, the nature, scope and purpose of the processing and, where appropriate, the size of the controller or processor."

Article 11: Exceptions and restrictions

"1. No exception to the provisions set out in this Chapter shall be allowed except to the provisions of Article 5 paragraph 4, Article 7 paragraph 2, Article 8 paragraph 1 and Article 9, when such an exception is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for:

a. the protection of national security, defense, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest;

..."

D. European Union Law Materials

1. Directive 95/46/EC of 24 October 1995

46. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data was designed to

protect individuals' fundamental rights and freedoms (including their right to privacy) in the processing of personal data, while at the same time removing obstacles to the free flow of such data. Article 17 read as follows:

Security of processing

"1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

– the processor shall act only on instructions from the controller,

– the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

..."

2. General Data Protection Regulation

47. Regulation (EU) 2016/679 of the European Parliament and of the European Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), published in OJ 2016 L 119/1, came into force on 24 May 2016 and repealed Directive 95/46/EC with effect from 25 May 2018. The relevant provisions of the Regulation read as follows:

Article 5: Principles relating to processing of personal data

"1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

...

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Article 6: Lawfulness of processing

"1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, *inter alia*: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, *inter alia*:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."

Article 32: Security of processing

"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law."

COMPLAINT

48. The applicant complained that the national authorities had failed to protect his personal data stored in the Taxpayer Information Service database from misuse and abuse, in breach of his right to respect for his private life as provided in Article 8 of the Convention.

THE LAW

Alleged violation of Article 8 of the Convention

49. The applicant complained under Article 8 of the Convention, the relevant parts of which read as follows:

"1. Everyone has the right to respect for his private ... life ...

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."

1. Scope of the applicant's complaint

(a) The parties' submissions

50. The Government submitted that the applicant's complaint did not concern the unlawful access carried out by F.D. and G.A., but the State's alleged failure to afford appropriate safeguards to prevent abuse of his personal data. Moreover, according to them, the scope of the applicant's complaint was limited to access to and use of his personal data by the Revenue Police and not by third parties. They argued that the decision of the Data Protection Authority of 18 September 2008 (see paragraph 35 above) did not refer to the IT system managed by the Revenue Police, but to access to the Tax Registry by entities other than the Revenue Police. Therefore, it was irrelevant to the present case.

51. The applicant maintained that in his application he had complained about the failure of the national authorities to protect his personal data stored in the Taxpayer Information Service database, a database to which numerous

entities – and not only the Revenue Police – had access. He relied on the decisions issued in the years 2008 to 2011 by the Data Protection Authority, which had identified several shortcomings in the rules concerning access to the Tax Registry by several public and private entities.

(b) The Court's assessment

52. Having examined the material in its possession, the Court observes the following. In his application the applicant stated that after reading a newspaper article he had become aware that his personal data stored in the Taxpayer Information Service database had been unlawfully accessed in the years 2008 to 2009 by an official of the Revenue Police. He also pointed out that in the same article it had been reported that the official had been able to unlawfully access the database hundreds of times and to extract information on a long list of public figures. According to him, these events proved that the rules and management system in force at that time had not afforded appropriate safeguards against misuse and abuse of his personal data and were therefore inconsistent with the guarantees of Article 8. The Court thus considers that the applicant's complaint does not concern the unlawful access carried out by F.D. and G.A., but the State's alleged failure to prevent the misuse and abuse of his personal data stored in the Taxpayer Information Service database.

53. The application form contains several indications that the applicant intended to complain of the absence of appropriate measures in relation to the use of the database not only by the Revenue Police, but also by the other entities which had access to it for the performance of their institutional mandate. In the statement of facts, the applicant submitted that under the national provisions in force at that time, the Taxpayer Information Service database was accessible to, besides the Revenue Police, other tax authorities and, more generally, to public and private entities such as local authorities, social security institutions, independent authorities, judicial institutions, police forces, chambers of commerce, and tax-collection agents. He also submitted that in several decisions issued between 2008 and 2011 the Data Protection Authority had identified numerous shortcomings in the security of access to the Tax Registry and ordered the tax authorities to put in place a comprehensive set of technological and administrative measures to enhance access security and to make data processing compliant with the relevant domestic framework. The applicant argued that at the time he had lodged his application, several of these measures had not yet been put in place, as the deadlines originally fixed by the Data Protection Authority had been repeatedly extended. The above-mentioned decisions of the Data Protection Authority provided further proof of the alleged violation of Article 8 of the Convention.

54. Therefore, contrary to what was argued by the Government, the Court finds that in his application the applicant expressly indicated his intention to complain of the alleged failure of the State to protect his personal data stored in the Taxpayer Information Service database from misuse and abuse not only in relation to the activities of the Revenue Police, but also with regard to access to the database by entities other than the Revenue Police.

2. The applicability of Article 8 of the Convention and the applicant's victim status

55. The Court notes that the Government have not raised any objection to the admissibility *ratione materiae* and *ratione personae* of the present application. However, the Court has already held that it is not prevented from examining of its own motion those issues, since they concern matters which go to the Court's jurisdiction (see, among other authorities, *Vegotex International S.A. v. Belgium* [GC], no. 49812/09, § 59, 3 November 2022, as regards the question of the applicability *ratione materiae* of the Convention; see also *Unifaun Theatre Productions Limited and Others v. Malta*, no. 37326/13, § 64, 15 May 2018, and *Goulandris and Vardinogianni v. Greece*, no. 1735/13, § 34, 16 June 2022, with further references, as regards the question of the applicant's victim status).

(a) The applicability of Article 8 of the Convention

56. As regards the question whether Article 8 of the Convention is applicable to the facts of the present case, the Court notes that the information stored in the Taxpayer Information Service database comprised the name, tax identification number, date of birth and address of all taxpayers, including the applicant, and a wide range of financial information that could be relevant for tax purposes. It also provided details of taxpayers' income and net assets, and any pending cases with the tax authorities, among other information. According to the evidence submitted by the applicant, it included information on gas, water, electricity and telephone expenses, interest expenses on liabilities, social security contributions, bank transfers, data on vehicle registration in the public register of automobiles, sports club memberships, and taxpayers' travel expenses, among others (see paragraph 4 above).

57. The Court considers that at least certain data contained in the Taxpayer Information Service database, and accessible to the Revenue Police and a large number of other entities, such as the applicant's name, date of birth and address, details on income and net assets and any pending cases with the tax authorities, clearly concerned the applicant's private life (see, in relation to taxation data, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13, § 138, 27 June 2017, and *L.B. v. Hungary* [GC], no. 36345/16, § 104, 9 March 2023, and in relation to financial information contained in banking documents, *M.N. and Others v. San Marino*,

no. 28005/12, § 51, 7 July 2015). Article 8 of the Convention therefore applies to the facts of the present case.

(b) The applicant's victim status

58. As regards the question whether the applicant can claim to be a victim of the violation alleged in the present case, the Court considers that it is necessary to stress from the outset that the present case differs from those in which the Court accepted that an applicant could claim to be a victim of a violation of Article 8 occasioned by the mere existence of secret-surveillance measures, or legislation permitting secret-surveillance measures. In those cases, the Court considered, provided that certain criteria were fulfilled, that the threat of surveillance could be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8 (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 171, ECHR 2015; see also *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, § 167, 25 May 2021, and *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, § 262, 11 January 2022).

59. By contrast, in the present case the applicant complained of the failure of the domestic authorities to protect his personal data stored in the Taxpayer Information Service database from abuse and misuse. The Court must therefore assess whether the applicant can claim to be a victim of the alleged violation.

60. In this regard, the Court reiterates that Article 34 of the Convention does not provide for the institution of an *actio popularis*, meaning that applicants may not complain about a provision of domestic law, a domestic practice or public acts simply because they appear to contravene the Convention (see *Communauté genevoise d'action syndicale (CGAS) v. Switzerland* [GC], no. 21881/20, § 106, 27 November 2023, and *Centre for Legal Resources on behalf of Valentin Câmpeanu v. Romania* [GC], no. 47848/08, § 101, ECHR 2014). The Court's 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, among many others, *Roman Zakharov*, cited above, § 164).

61. Accordingly, in order to be able to lodge a petition by virtue of Article 34, a person, non-governmental organisation or group of individuals must be able to claim to be a "victim" of a violation of the rights set forth in the Convention (see *Aksu v. Turkey* [GC], nos. 4149/04 and 41029/04, § 50, ECHR 2012, and *Michaud v. France*, no. 12323/11, § 51, ECHR 2012). In general, the word "victim" under Article 34 denotes the following categories of persons: those *directly* affected by the alleged violation of the Convention (the direct victims); those *indirectly* affected by the alleged violation of the Convention (the indirect victims); and those *potentially* affected by the

alleged violation of the Convention (the potential victims) (see *Verein KlimaSeniorinnen Schweiz and Others v. Switzerland* [GC], no. 53600/20, § 463, 9 April 2024). In any event, whether the victim is direct, indirect or potential, there must be a link between the applicant and the harm which he or she claims to have sustained as a result of the alleged violation (see *Akdeniz v. Turkey* (dec.), no. 20877/10, § 21, 11 March 2014, and *Mansur Yalçın and Others v. Turkey*, no. 21163/11, § 40 *in fine*, 16 September 2014).

62. In order to fall into the category of direct victims, the applicant must be able to show that he or she was "directly affected" by the measure complained of (see *Lambert and Others v. France* [GC], no. 46043/14, § 89, ECHR 2015 (extracts)). This implies that the applicant has been personally and actually affected by the alleged violation of the Convention, which is normally the result of a measure applying the relevant law or a decision allegedly in breach of the Convention or, in some instances, of the acts or omissions of State authorities or private parties allegedly infringing the applicant's Convention rights (see, for instance, *Aksu*, cited above, § 51; see also *Karner v. Austria*, no. 40016/98, §§ 24-25, ECHR 2003-IX, and *Berger-Krall and Others v. Slovenia*, no. 14717/04, § 258, 12 June 2014). However, this does not necessarily mean that the applicant needed to be personally targeted by the act or omission complained of. What is important is that the impugned conduct personally and directly affected him or her (see, for instance, *Aksu*, cited above, §§ 51-54).

63. Two types of potential victim status may be found in the case-law (see see *Verein KlimaSeniorinnen Schweiz and Others*, cited above, § 469). The first type concerns persons who claim to be presently affected by a particular general legislative measure. The Court has specified that it may accept the existence of victim status where applicants contend that a law violates their rights, in the absence of an individual measure of implementation, if they belong to a class of people who risk being directly affected by the legislation, or if they are required either to modify their conduct or risk being prosecuted (ibid.; see also *Tănase v. Moldova* [GC], no. 7/08, § 104, ECHR 2010, and *M.A. and Others v. France* (dec.), nos. 63664/19 and others, § 34, 27 June 2023). The second type concerns persons who argue that they may be affected at some future point in time. The Court has made clear that the exercise of the right of individual petition cannot be used to prevent a potential violation of the Convention and that, in theory, the Court cannot examine a violation other than *a posteriori*, once that violation has occurred. It is only in highly exceptional circumstances that an applicant may nevertheless claim to be a victim of a violation of the Convention owing to the risk of a future violation. In general, the relevant test to examine the existence of such victim status is that the applicant must produce reasonable and convincing evidence of the likelihood that a violation affecting him or her personally will occur; mere suspicion or conjecture being insufficient in this regard (see *Verein KlimaSeniorinnen Schweiz and Others*, cited above, § 470).

64. The term "potential" therefore refers, in some circumstances, to victims who claim that they are at present, or have been, affected by the general measure complained of, and, in other circumstances, to those who claim that they might be affected by such a measure in the future. In some instances, these two types of situations may coexist or may not be easily distinguishable and the relevant case-law principles may apply interchangeably (ibid., § 471).

65. Having regard to the principles reiterated above, and taking into account the scope of the applicant's complaints (see paragraph 54 above), the Court considers that it must determine whether the applicant can claim to be a victim of the measure he complained of in the present case, namely the omission of the domestic authorities to protect his personal data stored in the Taxpayer Information Service database from misuse and abuse by (1) the Revenue Police and (2) the third entities which had access to the database.

(i) The complaint concerning the misuse and abuse of the applicant's personal data by the Revenue Police

66. As regards the complaint concerning the omission of the State to protect the applicant's personal data from misuse and abuse by the Revenue Police, the Court considers that the applicant has shown that he was personally and directly affected by the omission complained of (see paragraph 62 above).

67. In particular, the applicant demonstrated that he had learned from a newspaper article that F.D., an officer of the Revenue Police, had unlawfully extracted information concerning him from the Taxpayer Information Service database (see paragraph 5 above), and argued that abuse of his personal data had been facilitated by the omission of the State to put in place adequate measures to prevent it from happening (see paragraph 53 above).

68. The Court therefore concludes that the applicant can claim to be a victim of the alleged omission of the State to protect his personal data from misuse and abuse by the Revenue Police.

(ii) The complaint concerning the misuse and abuse of the applicant's personal data by third entities

69. As regards the complaint concerning the omission of the State to protect the applicant's personal data from misuse and abuse by third entities which had access to the database, the Court notes that the applicant has not argued that he was the victim of such a measure. In essence, the applicant relied on the fact that, as an Italian taxpayer, he belonged to a category of persons whose data were stored in the Taxpayer Information Service database pursuant to Article 1 of Presidential Decree no. 605/1973 (see paragraph 13 above) and that, accordingly, he had been exposed to the risk of being subjected to such a measure in the light of the wide access conferred on third

entities to that database and of the insufficient protection afforded by the domestic legal framework.

70. In this context, the Court must examine whether the applicant can be regarded as a potential victim of the alleged violation, within the two possible meanings reiterated above, taking into account that those different situations might not be easily distinguishable and that the relevant principles apply interchangeably (see paragraph 63-64 above).

71. The Court would begin by noting that it is indisputable that the present case does not concern a situation in which the applicant was required to either modify his conduct or risk being prosecuted. His situation must therefore be distinguished from that of applicants who faced the dilemma of either complying with the impugned legal provision or refusing to do so and, in so doing, exposing themselves to sanction (compare *Dudgeon v. the United Kingdom*, 22 October 1981, §§ 40-41, Series A no. 45; *Norris v. Ireland*, 26 October 1988, § 29, Series A no. 142; *Michaud*, cited above, § 92; and *S.A.S. v. France* [GC], no. 43835/11, § 57, ECHR 2014 (extracts)).

72. As observed above, the present case also differs from those in which the Court accepted that an applicant could claim to be a victim of violations occasioned by the mere existence of secret-surveillance measures, or legislation permitting secret-surveillance measures (see paragraphs 58-59 above).

73. The Court must therefore assess whether the applicant can claim that he may be affected by the contested measure at some future point in time. As observed above, this requires the assessment of whether the applicant provided reasonable and convincing evidence of the likelihood that a violation affecting him personally will occur (see paragraph 63 above).

74. In this connection, the Court considers that the mere fact of being an Italian taxpayer whose personal data are stored in the Taxpayer Information Service database does not suffice to consider that the applicant has already been exposed to, or was potentially at risk of being subjected to, abuse and misuse of his personal data by third entities which had access to the database.

75. In this regard, the Court notes that in several cases it stressed that it was not sufficient to belong to a class of persons that, in the abstract, could be affected by the impugned measure, it being also necessary to produce reasonable and convincing evidence of the likelihood that a violation affecting the applicant directly would occur. For example, in *Willis v. the United Kingdom* (no. 36042/97, ECHR 2002-IV), the risk to the applicant of being refused a widow's pension on grounds of sex at a future date was found to be hypothetical, since it was not certain that the applicant would otherwise fulfil the statutory conditions for the payment of the benefit at the date when a woman in his position would become entitled to receive it. In *Dimirtas and Others v. Greece* ((dec.), nos. 59573/09 and 65211/09, § 31, 4 July 2017), the Court considered that the mere fact of being a Greek citizen who was eligible to vote did not suffice in order to complain of domestic legislation which

prevented the dissemination of opinion polls. Similarly, the Court held that, to be a victim of a statutory restriction on prison visits, the applicant prisoner had to demonstrate that he had potential visitors and had optimised his visiting rights up to that point in time (see *Chernenko and Others v. Russia* (dec.), no. 4246/14, § 45, 5 February 2019). In *Shortall and Others v. Ireland* ((dec.), no. 50272/18, 19 October 2021), the Court found that, in order to complain of the religious nature of the declaration made by the President of Ireland upon being elected and by persons appointed to be members of the Council of State, the applicants would have had to demonstrate, respectively, that they had a real intention of seeking the office of President and that they had some realistic prospects in that regard (ibid., § 53), or that their appointment to the Council of State was a realistic possibility (ibid., § 50). More recently, in *A.M. and Others v. Poland* ((dec.), nos. 4188/21 and 7 others, § 86, 16 May 2023), the Court observed that the applicants, as women of child-bearing age in Poland, could be affected by the impugned restriction on access to therapeutic abortion in the event of foetal abnormalities, but concluded that they had failed to advance any convincing evidence that they were at real risk of being affected by the contested legislative amendment (see also *K.B. and K.C. v. Poland* (dec.), nos. 1819/21 and 3639/21, § 63, 4 June 2024).

76. In the light of the above, the Court reiterates once again that it is only in highly exceptional circumstances that an applicant may claim to be a victim of a violation of the Convention owing to the risk of a future violation (see *A.M. and Others v. Poland*, cited above, § 77, and *K.B. and K.C. v. Poland*, cited above, § 58).

77. In the present case, the applicant has not provided any evidence capable of demonstrating that he was exposed, owing to his personal situation, to the risk of misuse or abuse of his personal data by third entities which had access to the database. The Court therefore concludes that his fear of being subjected to such a measure is based on a mere hypothesis, which is too remote and abstract for the applicant to make an arguable claim to be a "victim" within the meaning of Article 34 of the Convention.

78. Therefore, the Court finds that the applicant cannot claim to be a victim of an omission of the State to prevent the misuse and abuse of his personal data by third parties, in breach of Article 8, solely on account of the alleged insufficiencies in the applicable legal framework or in the practice of the competent domestic authorities to prevent it happening.

79. Accordingly, this part of the complaint is 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.

3. The Government's non-exhaustion objection

80. The Court has accepted that, insofar as he complained of the omission of the State to protect his data from abuse and misuse by the Revenue Police, the applicant can claim to have victim status (see paragraph 68 above).

81. The Court will therefore address the Government's objection of non-exhaustion of domestic remedies in respect of that complaint.

(a) The parties' submissions

82. The Government submitted that the applicant had not correctly exhausted domestic remedies. The criminal complaint he had brought had concerned only the private conduct of F.D. and G.A. and thus could not have offered appropriate redress in respect of the State's alleged failure to afford appropriate safeguards to prevent abuse of the applicant's personal data. According to the Government, there were other available and effective remedies which the applicant should have exhausted instead. First, the applicant could have lodged a claim for damages against the Revenue Police under Article 15 of Legislative Decree no. 196/2003 (Personal Data Protection Code) and Article 2050 of the Civil Code. Secondly, he could have availed himself of the complaint procedure provided for in Articles 141 and 143 of Legislative Decree no. 196/2003 (Personal Data Protection Code). By using this remedy, coupled with the subsequent lodging, where necessary, of an appeal against the decisions of the Data Protection Authority, the applicant could have obtained, in the Government's view, the adoption by the Data Protection Authority of the measures necessary to prevent abuse of his personal data. In particular, according to the Government, it could have invited the data controller to carry out the blocking of access to the data voluntarily; prescribed the data controller the appropriate or necessary measures aimed at complying with the relevant domestic provisions on data processing; or ordered the blocking of access to or prohibited, in whole or in part, the processing of the relevant data.

83. The applicant replied that by lodging a complaint against F.D. and G.A. he had exhausted a potentially effective remedy to redress the unlawful interference with his personal data. The fact that the remedy had proved *in concreto* to be ineffective – following the end of the plea-bargaining procedure and the subsequent discontinuation of the criminal proceedings brought by him – did not impose on him a burden to use other remedies which would have had essentially the same objective. Moreover, the remedies identified by the Government would not have been effective. As to the general compensatory remedy, the applicant observed that the Government had not submitted case-law in which the domestic courts had ordered compensation to be paid in circumstances similar to those in the present case. With regard to the administrative remedy provided for in Articles 141 and 143 of Legislative Decree no. 196/2003 (Personal Data Protection Code), the

applicant stressed that the Data Protection Authority was not a judicial authority. The applicant further observed that the enforcement of the Data Protection Authority's instructions is not binding, and that the Authority had already ordered several times to adopt concrete operational measures aimed at protecting the data stored in the Taxpayer Information Service database from misuse and abuse by third parties, but those measures were not enforced.

(b) The Court's assessment

84. The Court reiterates that the obligation to exhaust domestic remedies requires an applicant to make normal use of remedies which are available and sufficient in respect of his or her Convention grievances. The existence of the remedies in question must be sufficiently certain not only in theory but in practice, failing which they will lack the requisite accessibility and effectiveness (see *Vučković and Others v. Serbia* (preliminary objection) [GC], nos. 17153/11 and 29 others, § 71, 25 March 2014, and *Communauté genevoise d'action syndicale (CGAS)*, cited above, § 139). To be effective, a remedy must be capable of directly redressing the impugned state of affairs and must offer reasonable prospects of success (ibid., with further references).

85. However, there is no obligation to have recourse to remedies which are inadequate or ineffective (see *Vučković and Others*, cited above, § 73; *Communauté genevoise d'action syndicale (CGAS),* cited above, § 141). The issue of determining whether a domestic procedure constitutes an effective remedy within the meaning of Article 35 § 1, which an applicant must exhaust, depends on a number of factors, notably the applicant's complaint, the scope of the obligations of the State under that particular Convention provision, the available remedies in the respondent State and the specific circumstances of the case (see, among others, *Lopes de Sousa Fernandes v. Portugal* [GC], no. 56080/13, § 134, 19 December 2017, and *Ražnatović v. Montenegro*, no. 14742/18, § 27 2 September 2021). This means that an applicant is not requested to lodge applications with bodies or institutions which have no power or competence to offer effective redress for the complaint at issue under the Convention (see, *mutatis mutandis*, *Mukhametov and Others v. Russia*, nos. 53404/18 and 3 others, § 27, 14 December 2021).

86. The Court has, nevertheless, also frequently underlined the need to apply the exhaustion rule with some degree of flexibility and without excessive formalism. It has therefore recognised that the rule of exhaustion is not capable of being applied automatically; in reviewing whether it has been observed it is essential to have regard to the particular circumstances of each individual case (see *Communauté genevoise d'action syndicale (CGAS),* cited above, § 140, with further references).

87. As regards the burden of proof, the Court reiterates that it is incumbent on the Government claiming non-exhaustion to satisfy the Court that the remedy was an effective one, available in theory and in practice at the relevant

time. Once this burden has been satisfied, it falls to the applicant to demonstrate that the remedy advanced by the Government was in fact exhausted, or was for some reason inadequate and ineffective in the particular circumstances of the case, or that there existed special circumstances exempting him or her from this requirement (see, among many other authorities, *Vučković and Others*, cited above, § 77, and *Communauté genevoise d'action syndicale (CGAS),* cited above, § 143).

88. The Court agrees with the Government that lodging a criminal complaint against F.D. and G.A. (see paragraph 6 above) was not a remedy that could have provided redress in respect of the applicant's grievances. Even if the applicant had succeeded in obtaining compensation from the perpetrators of the unlawful access, this would not have entailed any obligation on the part of the national authorities to act to prevent further abuse of his personal data. It thus remains to be determined whether there were other remedies available to the applicant which he was obliged to exhaust before complaining to the Court.

89. Turning to the specific remedies listed by the Government, the Court notes that the remedy under Article 15 of the Personal Data Protection Code (see paragraph 17 above) and Article 2050 of the Civil Code (see paragraph 18 above), whose purpose is to grant compensation, cannot be considered adequate in respect of the applicant's complaint. The applicant complained about a continuing situation of inadequate protection of his personal data stored in the Taxpayer Information Service database and the State's long-standing failure to take action to prevent abuse in the context of access to the database. It follows that such a remedy would not be capable of directly addressing important aspects of the applicant's grievances.

90. The Court further notes that, according to the Government, the applicant could have lodged a complaint with the Data Protection Authority under Article 143 of the Personal Data Protection Code (see paragraph 17 above), which provided that the Data Protection Authority could order the data-processing controller to take appropriate measures to make the data processing compliant with the regulations in force with a view to preventing the misuse and abuse of personal data. In particular, the Government pointed out that the Data Protection Authority could have ordered the data controller to voluntarily block access to the data, prescribed the appropriate or necessary measures aimed at making the data processing compliant with the applicable provisions or ordered the blocking of access to or prohibited, in whole or in part, the processing of such data. Therefore, the applicant could have requested the Data Protection Authority to order the domestic authorities to put in place the necessary operational and technological measures aimed at protecting his personal data against misuse and abuse.

91. The applicant, on his part, objected in general terms that the DPA was not a judicial body.

92. In this connection, the Court reiterates that its case-law does not require that all instances of a domestic remedy be judicial in the strict sense (see, among many authorities, *Rotaru v. Romania* [GC], no. 28341/95, § 69, ECHR 2000-V; *Driza v. Albania*, no. 33771/02, § 116, 13 November 2007; *Centre for Legal Resources on behalf of Valentin Câmpeanu*, cited above, § 149; and *Abdilla v. Malta*, no. 36199/15, § 69, 17 July 2018). Nevertheless, the powers and procedural guarantees an authority possesses are relevant in determining whether the remedy before it is effective (see *Driza v. Albania*, no. 33771/02, § 116, ECHR 2007-V (extracts); *Vrioni and Others v. Albania and Italy*, nos. 35720/04 and 42832/06, § 83, 29 September 2009; and *Tagayeva and Others v. Russia*, nos. 26562/07 and 6 others, § 620, 13 April 2017). In cases of non-judicial authorities, the Court assesses whether they are independent (see *Khan v. the United Kingdom*, no. 35394/97, §§ 44-47, ECHR 2000-V) and whether sufficient procedural safeguards are afforded to the applicant (see *Allanazarova v. Russia*, no. 46721/15, § 93, 14 February 2017).

93. The Court notes that Article 153 § 1 of the Personal Data Protection Code, as in force at the material time (see paragraph 17 above), provided that the Data Protection Authority was an independent administrative body, fully autonomous and with independence of decision and assessment. The second paragraph provided that its members were appointed by Parliament from among persons who could prove their independence. Having regard to the manner and conditions of appointment of its members, and in the absence of any indication of a lack of sufficient and adequate safeguards against possible external pressure, the Court considers that there is no reason to doubt the Data Protection Authority's independence with regard to any other power or authority, and especially with regard to the executive.

94. As to the procedural guarantees, proceedings before the Data Protection Authority were adversarial in nature, individuals could be legally represented, and the proceedings led to the adoption of binding decisions.

95. It is true that the Data Protection Authority's decisions were formally administrative in nature, and that the Authority retained discretion on how to exercise its functions and powers.

96. However, the Court observes that under Article 152 of the Personal Data Protection Code, the applicant could have lodged an appeal against the decision of the Data Protection Authority with the competent judicial authorities. Furthermore, any decision adopted in such proceedings would have been subject to an appeal on points of law before the Court of Cassation. Therefore, the Court considers that, taking into account the arguments of the parties, there is no reason to consider that, in the present case, a complaint to the Data Protection Authority of the alleged failure of the domestic authorities to adopt technological and operational measures aimed at protecting his personal data stored in the Taxpayer Information Service database from misuse and abuse coupled, if need be, with an appeal to the competent judicial

authorities, would not have constituted an aggregate of remedies which would have provided the applicant with at least reasonable prospects of success.

97. In view of the foregoing, there is no doubt that the remedy consisting in a complaint to the Data Protection Authority was available in theory, as it was clearly set out in the statutory law.

98. As to the practical availability of the remedy, the Court reiterates once again that it is incumbent on the Government claiming non-exhaustion to satisfy the Court that the remedy was an effective one, available in theory and in practice at the relevant time (see paragraph 87 above).

99. In this respect, the Court has held that the availability of a remedy said to exist, including its scope and application, must be clearly set out and confirmed or complemented by practice or case-law, which must in principle be well established and date back to the period before the application was lodged (see *Guðmundur Gunnarsson and Magnús Davíð Norðdahl v. Iceland*, nos. 24159/22 and 25751/22, § 44, 16 April 2024; and *Guravska v. Latvia* (dec.), no. 41553/18, § 24, 7 July 2020). However, the Court has also held that the said principle is subject to exceptions which may be justified by the particular circumstances of the case (see *Gherghina v. Romania* (dec.) [GC], no. 42219/07, § 88, 9 July 2015). Accordingly, the Court has found the absence of a well-established body of domestic case-law to be justified in cases concerning the use of an existing remedy in respect of a relatively recent branch of domestic law (ibid., § 100), and in cases concerning newly introduced remedies which had not been in place long enough to be tested before the domestic courts by interested individuals (see *Bistieva and Others v. Poland*, no. 75157/14, § 62, 10 April 2018; and *Stella and Others v. Italy* (dec.), nos. 49169/09 and 10 others, § 65, 16 September 2014). In similar cases, the Court stressed that in a legal system in which fundamental rights are protected by the Constitution and the law, it is incumbent on the aggrieved individual to test the extent of that protection and allow the domestic courts to apply those rights and, where appropriate, develop them in exercising their power of interpretation, and considered that, if the applicant had any doubts about the effectiveness of the remedy in question, it was for him or her to dispel those doubts by lodging a complaint before the competent body (see *Gherghina*, cited above, § 101, and *Fullani v. Albania* (dec.), no. 4586/18, § 70, 20 September 2022).

100. In the absence of examples of domestic case-law demonstrating the effectiveness and availability in practice of a remedy, the Court examined whether, in the material submitted before it, there was any other indication of the prospects of success of the remedy in question (see *Ádám and Others v. Romania*, nos. 81114/17 and 5 others, § 49, 13 October 2020), and whether the Government had provided explanations concerning any structural reason which would have indicated that, even without specific examples, the remedy could have been effective (see *Voynov v. Russia*, no. 39747/10, § 45, 3 July 2018).

101. In the present case, the Court notes that the Government did not provide any examples of domestic case-law in respect of the specific complaints raised by the applicant concerning the absence of sufficient safeguards to prevent abuse and misuse of the personal data stored in tax Taxpayer Information Service Database.

102. However, there is nothing indicating that the remedy in question would have been obviously futile in the applicant's case and, by contrast, the material submitted to the Court indicates the opposite. In particular, both the applicant and the Government provided the Court with decisions adopted by the Data Protection Authority, on its own motion, in respect of the different but related issue concerning the lack of safeguards aimed at protecting the data stored in the Taxpayer Information Service database from abuse and misuse by third entities (see paragraphs 31-43 above). In this context, in which the domestic legal system sets out a specific body with a general competence in the field of data protection, and which had moreover already ruled on similar issues, the Court does not see any reason why the Data Protection Authority would have refused, upon the applicant's complaint, to deal with the issue concerning the safeguards necessary to protect the data stored in the Taxpayer Information Service database from abuse and misuse by the Revenue Police.

103. Insofar as the applicant argued that the remedy in question was somehow inadequate or ineffective as the decisions previously adopted by the Data Protection Authority had not been enforced (see paragraph 83 above), the Court considers that mere delays in the enforcement of the decisions of a domestic authority which are not reiterated and systemic are insufficient to raise doubts as to the effectiveness of the remedy in question (see, *mutatis mutandis*, *Simaldone v. Italy*, no. 22644/03, §§ 81-84, 31 March 2009).

104. In conclusion, the Court considers that the applicant did not provide the national authorities with the opportunity which is in principle intended to be afforded to Contracting States by Article 35 of the Convention, namely the opportunity to prevent or put right Convention violations through their own legal system (see *Gerghina*, cited above, § 115, and *Communauté genevoise d'action syndicale (CGAS),* cited above, § 164).

105. In the light of the foregoing, the Court upholds the Government's objection. Accordingly, the applicant's complaint concerning the alleged failure on the part of the respondent State's authorities to protect his personal data from abuse and misuse by the Revenue Police is inadmissible for failure to exhaust domestic remedies and must be dismissed in accordance with Article 35 § 1 of the Convention.

For these reasons, the Court, unanimously,

Declares the application inadmissible.

Done in English and notified in writing on 28 November 2024.

Ilse Freiwirth Registrar	Marko Bošnjak President