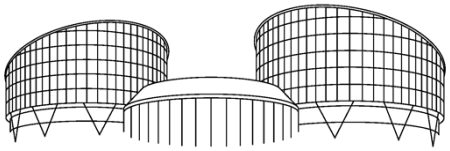

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

THIRD SECTION

CASE OF SHIPS WASTE OIL COLLECTOR B.V.
v. THE NETHERLANDS

(Application no. 2799/16)

JUDGMENT

Art 8 • Correspondence • Transmission and use in competition law proceedings of data lawfully obtained through telephone tapping in criminal investigations • Impugned data transmission sufficiently foreseeable under applicable domestic law • Extensive *ex post facto* judicial oversight • Adequate safeguards • Domestic system adequately capable of avoiding abuse of power • Art 8 not requiring *ex ante* authorisation by a court in specific case-context • Adequate balancing exercise between interests at stake • Relevant and sufficient reasons justifying necessity and proportionality of interference Art 13 (+ Art 8) • Effective remedy

STRASBOURG

16 May 2023

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

In the case of Ships Waste Oil Collector B.V. v. the Netherlands,

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

Pere Pastor Vilanova*, President*,
Yonko Grozev,
Jolien Schukking,
Darian Pavli,
Peeter Roosma,
Ioannis Ktistakis,
Andreas Zünd*, judges*,
and Milan Blaško, *Section Registrar,*

Having regard to:

the application (no. 2799/16) against the Kingdom of the Netherlands lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by Ships Waste Oil Collector B.V. ("the applicant company"), on 7 January 2016;

the decision to give notice to the Government of the Kingdom of the Netherlands ("the Government") of the complaints concerning Articles 8 and 13 of the Convention;

the parties' observations;

Having deliberated in private on 4 April 2023,

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

INTRODUCTION

1. The case concerns the transmission of data lawfully obtained in a criminal investigation to another law enforcement authority. The applicant company complains that the transmission of the data to and their use by the Competition Authority had not been foreseeable and that procedural safeguards were insufficient.

THE FACTS

2. The applicant company is a limited liability company incorporated under Dutch law, engaged in the collection of waste liquids from ships in the Rotterdam port region. The applicant company was represented by Mr G. van der Wal, then by Ms L.Y.M. Parret, and currently by Ms M.C. van Heezik, a lawyer practising in Brussels.

3. The Government were represented by their Agent, Ms B. Koopman, of the Ministry of Foreign Affairs.

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

I. CRIMINAL INVESTIGATION AND DATA TRANSMISSION

5. At the end of 2006, the Intelligence and Investigation Service (*Inlichtingen- en opsporingsdienst*) of the Ministry of Housing, Spatial Planning and the Environment (*Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer* – hereinafter, "VROM-IOD"), a special investigative service within the meaning of the Special Investigative Service Act (*Wet op de bijzondere opsporingsdiensten*; see paragraph 28 below) that operates under the authority of the public prosecutor (*officier van justitie*), began an investigation under the codename "Toto" into another collector of waste liquids from ships, the I. company, which was suspected of involvement in the disposal of polluted waste in contravention of environmental protection legislation.

6. In the context of this criminal investigation the VROM-IOD, duly authorised by an investigating judge (*rechter-commissaris*), intercepted telephone conversations made by some of the I. company's employees. Among them were conversations between an employee of I. company and an employee of the applicant company.

7. Certain of those intercepted conversations were identified as being of potential interest to the Netherlands Competition Authority (*Nederlandse Mededingingsautoriteit* – "the NMA") because they contained indications of price-fixing. In an official record (*proces-verbaal*) dated 21 April 2008 drawn up by an official of VROM-IOD, those indications of price-fixing were recorded and summary transcripts of some of these conversations were annexed to this report.

8. On 21 October 2008 the public prosecutor in charge gave permission in accordance with the Judicial and Criminal Data Act (*Wet Justitiële en Stravorderlijke gegevens* – "the WJSG"; see paragraph 18 below) for the official record, including the annexes, to be transmitted to the NMA by adding on the document "transmission to NMA approved" and dating and signing it by hand. The transmission to the NMA took place on 29 June 2009.

9. The NMA subsequently started an official investigation into possible violations of the Competition Act (*Mededingingswet*).

10. On several dates in 2009 and 2010 the public prosecutor in charge gave permission for the transmission to the NMA of a further selection of transcripts and audio files of the telephone conversations intercepted in the "Toto" criminal investigation. It transpires from information in the case-file that prior to those transmissions there had been contacts between VROM-IOD and NMA officials on the selection of the data that could be of relevance for the investigation into price-fixing.

11. On 29 and 30 June 2010 NMA inspectors visited the applicant company's premises. They questioned members of the applicant company's management under caution, in the course of which they played back a sound recording of an intercepted telephone conversation.

II. ADMINISTRATIVE PROCEEDINGS

12. Based on the results of its investigation, the NMA concluded that during the period between 30 August 2005 and 31 July 2007 several companies, including the applicant company, had coordinated their behaviour with the aim of allocating contracts and preventing or limiting price competition in the field of ship-generated waste collection. In doing so, these companies violated section 6 of the Competition Act (see paragraph 30 below). On 16 November 2011 the NMA imposed a fine on the applicant company in the amount of EUR 834,000.

13. The applicant company lodged a written objection (*bezwaarschrift*) with the NMA arguing, *inter alia*, that the intercepted telephone conversations should not be admitted as evidence because they did not qualify as 'criminal data' that could be transferred on the basis of the WJSG as the information had been irrelevant for the criminal investigation and protesting against the lack of prior judicial control on the transmission of the data to the NMA. It requested the NMA to give its consent to submit the objection directly to the Rotterdam Regional Court by way of appeal (*beroep*). The NMA gave its consent. The Regional Court joined the appeal of the applicant company with the appeals of other ships' waste disposal companies that were fined for breaching section 6 of the Competition Act, including the I. company, Port Invest B.V. (see application no. 3205/16) and Burando Holding B.V. (see application no. 3124/16).

14. The Regional Court gave judgment on 11 July 2013 (ECLI:NL:RBROT:2013:5042), declaring the appeal well-founded. Referring to its recent judgment of 13 June 2013 (ECLI:NL:RBROTT:2013:CA3079), it reiterated that the intercepted telephone data did qualify as 'criminal data' within the meaning of the WJSG (see paragraph 18 below). Further, it found that no reviewable weighing of interests had been recorded since the public prosecutor had merely given handwritten permission for the transmission of the official record of 21 April 2008 (see paragraphs 7 and 8 above) and subsequently on pre-printed forms without reasoning. From this it followed that the transcripts were to be excluded as evidence. Since the NMA's investigation and their decisions had mainly relied on this evidence (see paragraph 12 *in fine* above), the Regional Court quashed the NMA's decisions.

15. The Consumer and Market Authority (*Autoriteit Consument en Markt* – hereinafter "the ACM"), the successor body to the NMA, lodged a further appeal (*hoger beroep*) with the Supreme Administrative Court for Trade and Industry (*College van Beroep voor het bedrijfsleven*). The ACM, *inter alia,* argued that the transmission of the data by the Public Prosecution Service to another public authority would only be contrary to domestic law or to Article 8 of the Convention if it could not be considered necessary with a view to a "compelling general interest" or if it did not comply with the

requirements of proportionality and subsidiarity. That assessment fell to be made, according to the WJSG, by the civil courts in the shape of an *ex post facto* judicial review. The transmission of data to another public authority on the basis of section 39f(1) of the WJSG was a factual act, not a decision within the meaning of the General Administrative Law Act (*Algemene wet bestuursrecht*; see paragraph 31 below) and therefore not amenable to judicial review by the administrative courts. Such a factual act required neither reasoning nor an *ex ante* judicial review of its lawfulness.

16. The applicant company lodged a cross-appeal (*incidenteel hoger beroep*) on the grounds that the Regional Court had failed to find that the recordings of the intercepted telephone conversations were not properly part of any criminal file and thus not "criminal data" that may be transmitted to another entity in accordance with section 39f(1) of the WJSG.

17. The Supreme Administrative Court for Trade and Industry gave judgment on 9 July 2015 (ECLI:NL:CBB:2015:192). It quashed the Regional Court's judgment, dismissed the applicant company's cross-appeal and referred the case back to the Regional Court. Its reasoning included the following:

> "3.5 ... Under section 1, introductory sentence and subsection (b), of the WJSG, the term criminal data in this Act and the provisions based on it is understood to mean: personal data or data concerning a legal person obtained in the context of a criminal investigation, which the Public Prosecution Service processes in a criminal file or by automated means.
>
> The Supreme Administrative Court for Trade and Industry agrees with the Regional Court that the telephone taps submitted to the ACM qualify as criminal data within the meaning of the above-mentioned provision. It follows from the passages in the Explanatory Memorandum ... that the legislature intended the term 'criminal file' [*strafdossier*] in this legislative provision to be broad. In this connection, the Supreme Administrative Court for Trade and Industry also refers to paragraph 3.4.6 of the judgment of the Supreme Court of 20 April 2012 in the *Trafigura* case (ECLI:NL:HR:2012:BV3436 [see paragraph 22 below]), in which it was considered, among other things, that a criminal file may relate to more acts than those for which the Public Prosecution Service institutes a prosecution. The assertion ... that the telephone tap data [*tapgegevens*] have no relevance for the prosecution and qualify as by-catch, for which reason this material does not belong in the criminal file, is not followed by the Supreme Administrative Court for Trade and Industry. Furthermore, as the ACM has stated, in this case it could not be ruled out that the telephone tap data at any stage of the criminal proceedings would have relevance ...
>
> In any case, the telephone tap data were stored digitally and to that extent processed automatically. In this respect, it should be noted that the concept of 'processing personal data' ... is broadly defined: any operation or set of operations which relates to personal data, including in any case the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of making available, alignment or combination, blocking, erasure or destruction of data. [..].
>
> 4.3 ... The Explanatory Memorandum ... states that, in view of Article 8, paragraph 2, [of the] ECHR, the term 'compelling general interest' must be understood to mean the

interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals or the protection of the rights and freedoms of others. The ACM is charged with the enforcement of the Competition Act and, in particular, the supervision and investigation of cartels, prohibited price-fixing and other forms of coordination between companies. In view of the nature of the cartel ban in Section 6 of the Competition Act, the [Supreme Administrative Court of Trade and Industry] is of the opinion that in this case there is a compelling general interest, namely the economic well-being of the country. In this regard, reference is also made to the ECHR judgment of 2 October 2014 in the case of *DELTA PEKÁRNY a.s. v. the Czech Republic*, no. 97/11, § 81, 2 October 2014. Furthermore, the provisions of section 39f(1), introductory sentence and subsection (c), of the WJSG have been complied with. After all, the information was transmitted in order for the ACM to supervise compliance with regulations.

4.4 With respect to the question of whether the transmission was necessary as referred to in section 39f(2) of the WJSG, the Regional Court correctly pointed out that the Explanatory Memorandum to the amendment of the WJSG shows that a careful balancing of interests must take place when the data relating to criminal records are transmitted.

However, the Supreme Administrative Court for Trade and Industry does not follow the Regional Court's opinion that, in view of what is stated in the Explanatory Memorandum, the transmission of criminal data must be based on a weighing of interests by the public prosecutor that is known and can be assessed by the court – made at the time of the transmission and apparent at that time. The availability of written reasoning from the public prosecutor at the time of the transmission may simplify the verification of compliance with section 39f of the WJSG, but neither the law nor legislative history suggests that the unavailability of written reasoning at the time of transmission means that the requirements for transmission have not been met. In view of the foregoing, the judgment under appeal must be quashed to that extent.

4.5 The Supreme Administrative Court for Trade and Industry will now assess on the basis of the parties' arguments whether the evidence obtained in the context of a criminal investigation was lawfully provided to a public authority that used this material in proceedings for the imposition of an administrative fine.

4.6 In this connection, it must first be established whether the transmission of criminal data, in this case consisting of telephone tap data, in accordance with section 39f of the WJSG, violates Article 8 of the ECHR. Under the second paragraph of Article 8 of the ECHR, an interference with the right to privacy is only permitted to the extent that it is provided for by law and is necessary in a democratic society in the interest of, *inter alia*, the economic well-being of the country.

The starting-point for the assessment is that the telephone taps from which the data in question were obtained were conducted after the investigating judge had given permission to do so. [...]

The public prosecutor's competence to transmit the telephone tap data is statutorily grounded in the WJSG. Moreover, as to the lawfulness of this obtainment [sc. by the ACM], the law provides for a judicial procedure with sufficient guarantees, both under civil law in the context of the transmission of the data and under administrative law in the context of the review of the decision to impose a fine based on these data. The report in these cases shows that the ACM extensively assessed the evidence, including the telephone tap data, within the framework of the determination of whether there had been a violation of section 6(1) of the Competition Act. After the report was published

and before the ACM decided to impose a fine, the appellants were given the opportunity to put forward their views on the report, which they did.

Finally, the Supreme Administrative Court of Trade and Industry considers a sufficient case has been made out that the information about the alleged price-fixing could not in reason have been obtained by the ACM in a different, less intrusive manner, since such agreements are not, as a rule, put in writing. In the judgment of the provisional-measures judge of the Regional Court of The Hague of 26 June 2009 (ECLI:NL:RBSGR:2009:BJ0047), which was also cited by the parties, the provisional-measures judge gave judgment in a case comparable to the present one about the lawfulness of the transmission of telephone taps by the Public Prosecution Service to the ACM, and in doing so he also arrived at this conclusion with regard to the proportionality of the provision.

In view of the foregoing, the Supreme Administrative Court for Trade and Industry sees no evidence that the transmission of the telephone tap data to the ACM in accordance with section 39 of the WJSG violates Article 8 of the ECHR or any other treaty provision. [..].

The circumstance that the ACM itself does not have the competence to intercept telephone conversations does not constitute a ground for the finding that the use of the intercepted telephone conversations by the ACM should be considered unacceptable. The WJSG provides precisely for the possibility that such data, obtained using coercive measures in criminal proceedings, may be transmitted to, among others, public authorities that do not themselves have the competence to make use of such coercive measures.

Contrary to the argument made by the I. company, Port Invest B.V. and Burando Holding B.V., the circumstance that the ACM – in consultation with the VROM-IOD – had, having [taken cognisance of transcripts and recordings of intercepted telephone conversations], made a selection from a bulk of the data that were available and provisionally considered relevant by the VROM-IOD, does not, in the given situation, lead the Supreme Administrative Court for Trade and Industry to find that the transmission took place contrary to the WJSG."

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. THE JUDICIAL AND CRIMINAL DATA ACT

A. Relevant provisions

18. At the relevant time the WJSG provided as follows:

Section 1

"In this Act and the provisions made pursuant thereto, the following definitions shall apply:

...

(b) criminal data: personal data or data concerning a legal person obtained in the context of a criminal investigation, which the public prosecutor processes in a criminal file or by automated means; ..."

Section 39b

"(1) The Board of Procurators General shall only process criminal data if this is necessary for the proper discharge of the duties of the Public Prosecution Service or to comply with another statutory obligation. ..."

Section 39f

"(1) The Board of Procurators General may ... in so far as it is necessary in view of a compelling general interest [*zwaarwegend algemeen belang*], transmit criminal data to persons or public authorities [*instanties*] for the following purposes: ...

(c) enforcement of legislation;

(2) The Board of Procurators General may only transmit criminal data to persons or official bodies as referred to in the first paragraph to the extent that those data, for those persons or official bodies:

(a) are necessary in view of a compelling general interest or the determination, exercise or defence of a right in law ..."

B. Legislative history

19. Section 39f of the WJSG was enacted pursuant to a transitional provision of the Personal Data Protection Act, which required a *lex specialis* for the transmission of personal criminal data.

20. The following extracts are taken from the Explanatory Memorandum (*Memorie van Toelichting*) to the bill that led to the amendment of the WJSG (Lower House of Parliament, parliamentary year 2002-03, 28 886, no. 3, pp. 3, 5, 7-8 and 13):

"The proposed section 1(b) of this bill defines criminal data as data processed about a natural or legal person in the context of a criminal investigation. These data can be included in the case documents and processed in a criminal file, [the Public Prosecution Service's case management system] or the higher appeal systems. The Code of Criminal Procedure does not contain a definition of the term 'case documents' [*processtukken*]. In practice, the concept is broadly interpreted. [..].

The proposed sections 39e and 39f require the provision of criminal data to third parties to be 'necessary in view of a compelling general interest'. [..].

In view of Article 8 § 2 of the ECHR, the term 'compelling general interest' must be understood to mean the interests of national security, public safety or the economic well-being of the country, the prevention of disorder and crime, the protection of health or morals or the protection of the rights and freedoms of others. [..].

In weighing the interests [of the suspect and the compelling general interest against each other], the Public Prosecution Service should also, considering the need for the transmission which it must be able to demonstrate, take into account the principles of proportionality and subsidiarity. In addition to weighing these interests, the Public Prosecution Service should consider whether the requested transmission of information, being a form of further processing of the requested data, is not incompatible with the aim for which these were added to the criminal file at the time, namely the prosecution of one or more criminal acts. As a final matter, the receiver of the information should have a basis on which to be permitted to receive the information requested. [..].

> The decision of the Public Prosecution Service to transmit criminal data of the person concerned to a third party under the proposed sections 39e or 39f cannot be regarded as a decision within the meaning of section 1:3, first paragraph, of the General Administrative Law Act [see paragraph 31 below]. ... The act is aimed solely at the factual transmission of information relating to criminal data."

C. Relevant domestic case-law

21. In his advisory opinion to the Supreme Court of 3 February 2012 in the *Trafigura* case (ECLI:NL:PHR:2012:BV3436 – see paragraph 17 above), which concerned a civil action against a transmission of data under section 39f of the WJSG, the Procurator General stated the following (footnotes omitted):

> "3.6. This case does not concern an appeal against a decision of the public prosecutor [within the meaning of the General Administrative Law Act (*Algemene Wet Bestuursrecht* – "the AWB")]. In connection with what was claimed, the provisional-measures judge had to give a preliminary judgment about the lawfulness of a factual act [*feitelijke gedraging*] of the public prosecutor, namely the transmission of the data to [company A]. This is in line with the design of the WJSG. ... The lawfulness of the factual act of the Public Prosecution Service (the transmission) does not depend on the reasons given by the person who carried out the act at the time or, as in this case, sometime later in an email. The assessment of the lawfulness of a factual act can be carried out by the court afterwards and independently."

22. In its judgment of 20 April 2012 in that case (ECLI:NL:HR:2012:BV3436), the Supreme Court took the same approach. With regard to the definition of criminal data, it considered:

> "Section 39f(1) of the WJSG does not require that the transmission of criminal data ... relate solely to offences which are the subject of a prosecution, since a criminal file may relate to more facts than those which are the subject of a prosecution."

D. The Transmission (Designation) Order

23. The Judiciary (Organisation) Act (*Wet op de Rechterlijke Organisatie*) provides a legal basis for the Board of Prosecutors General to give instructions, in the format of (designation) orders, to the Public Prosecution Service on the performance of its tasks and the exercise of its powers.

24. The Transmission of criminal data for purposes other than criminal law enforcement (Designation) Order (*Aanwijzing verstrekking van strafvordelijke gegevens voor buiten de strafrechtspleging gelegen doeleinden*; "the Transmission (Designation) Order"), as it stood at the relevant time (published in the Official Gazette (*Staatscourant*) of 28 January 2008, no. 19), provided further details about the cases in and the conditions under which the Public Prosecution Service might transmit information under the WJSG.

25. As relevant to the case before the Court, the Transmission (Designation) Order provided that the Board of Procurators General could delegate (*mandateren*) its power to transmit criminal data within the meaning of section 39f of the WJSG, to, *inter alios*, the chief advocates general (*hoofdadvocaten-generaal*), who had the power to sub-delegate to individual advocates general and public prosecutors.

26. The Transmission (Designation) Order also contained further principles and instructions, including a flowchart, for the exercise of the power to transmit. The power to transmit was a discretionary power, not an obligation. It could be exercised upon request or *proprio motu*, but only after a balancing of interests. As regards the applicable principles of subsidiarity, necessity and proportionality, it was explained that these are closely interrelated in the assessment of whether, and if so, in what form, criminal data could be transmitted. Such data might only be transmitted to public authorities (*bestuursorganen*) if there is a legal basis for that authority to receive such information; if there was no other way for that authority to obtain the information that was less intrusive into the privacy of the person concerned; and if it was necessary for a purpose defined in section 39f of the WJSG.

27. The Transmission (Designation) Order emphasised that a decision to transmit was not a decision within the meaning of the AWB and thus not subject to administrative legal remedies. If a concerned party was of the opinion that a transmission had been unlawful, the only legal remedy was an appeal to the civil judge in tort proceedings (*onrechtmatige daad*).

II. THE SPECIAL INVESTIGATIVE SERVICES ACT

28. At the relevant time the Special Investigative Services Act provided as follows:

Section 1

"In this Act and the provisions based thereon, the following definitions shall apply:

a. special investigation service: one of the services referred to in section 2;

...

c. Our minister concerned: Our minister under whom a special investigation service falls.

Section 2

There are four special investigation services, namely:

...

b. special investigation service, falling under Our Minister of Housing, Spatial Planning and the Environment ...

Section 3

A special investigation service, under the authority of the public prosecutor, is charged with:

a. the criminal enforcement of law and order in the policy areas for which Our Minister concerned is responsible ...”

III. THE COMPETITION ACT

29. Section 5 of the Competition Act, as it stood at the relevant time, provided that the NMA was charged with the enforcement of that Act.

30. Section 6(1) of the Competition Act, as it stood at the relevant time, prohibited agreements between enterprises, decisions by associations of enterprises and concerted practices aimed at or with the effect of the prevention, restriction or distortion of competition within the Netherlands market (price-fixing).

IV. THE GENERAL ADMINISTRATIVE LAW ACT

31. Section 1:3 of the AWB defines a “decision” as a written decision by an administrative body, involving a legal act under public law. Section 3:46 of the AWB provides that a decision must be based on proper reasoning. It follows from sections 7:1 and 8:1 of the AWB that the administrative legal remedies of objection (*bezwaar*) and appeal to the administrative judge (*beroep*) may be instituted against decisions within the meaning of section 1:3.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

32. The applicant company complained that the transmission to the NMA of data that were irrelevant to the criminal investigation had constituted a violation of its rights under Article 8 of the Convention, which reads as follows:

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

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

A. Admissibility

33. The Government did not submit any objections against the admissibility of the complaint.

34. The Court notes that the complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

(a) The applicant company

35. The applicant company submitted that the transmission of the tapped information to the NMA had not been in accordance with the law. It argued that it had not been foreseeable that the data which had no relevance to the criminal investigation were "criminal data" within the meaning of the WJSG. Furthermore, it argued that it had not been foreseeable that the NMA would be in a position to receive and use such data in the light of the fact that it had no powers of its own to intercept communications and that this government body was not explicitly mentioned in the relevant legal instrument. It further submitted that it had not been foreseeable that the data could be transmitted without any prior knowable weighing of interests in written form and that this balancing test could be carried out afterwards by the courts instead. It considered their case to be comparable to that in *Dragojević v. Croatia* (no. 68955/11, 15 January 2015). Lastly, it argued that it had not been foreseeable on the basis of the applicable domestic law that the NMA could have contacts with the VROM-IOD on the selection of the data that it wished to be transmitted to it. In its opinion the legislature had failed to set out in sufficient detail in the domestic law the extent of the authorities' discretion and the manner it is to be exercised, relying on *Valenzuela Contreras v. Spain*, 30 July 1998, § 60, *Reports of Judgments and Decisions* 1998-V.

36. The applicant company further submitted that the interference had not been "necessary in a democratic society", arguing that the WJSG did not contain sufficient guarantees against arbitrary interferences and that the interference was not proportionate. Relying on *Sanoma Uitgevers B.V. v. the Netherlands* ([GC], no. 38224/03, § 90, 14 September 2010), it argued that an *ex ante* assessment of the transmission carried out by a judge had been necessary; such an assessment should not have been entrusted to the public prosecutor. Further, it argued that the *ex post* review of the transmission by the courts as provided under the domestic law was not sufficient, as it could not prevent irreparable harm. They suggested that the case-law of the civil courts showed that in practice they were reluctant to find a violation of fundamental human rights if administrative proceedings in which such questions could be addressed could subsequently be instituted. In that context

the applicant company noted that the review by the administrative courts did not suffice because it only related to the question whether evidence obtained by a transmission of data was lawful, and not to the transmission as such.

(b) The Government

37. The Government submitted that the foreseeability and safeguards required under Article 8 of the Convention should be established with reference to the seriousness of the interference. Since the transmission of data lawfully collected is not equivalent to an interception of communications, the procedural safeguards did not, in their opinion, need to be as stringent as those required in cases of interferences of that type.

38. In their view, the applicable law clearly described what information might be transmitted, by whom, to whom, under what conditions and to what end. They noted that the data transmitted in the present case were obtained in a criminal investigation with the authorisation of the investigating judge, that those data were subsequently stored digitally, thus processed electronically by the Public Prosecution Service, and therefore qualified as "criminal data" within the meaning of section 1 of the WJSG (see paragraph 18 above). That the transmitted data had not been used for the criminal prosecution does not mean that they are no criminal data as defined by law. The data had been transmitted to the NMA, an official body charged with the enforcement of legislation within the meaning of section 39f of the WJSG in the compelling general interest of the protection of the economic well-being of the country and for a purpose listed in section 39b of the WJSG. That the NMA had no power to intercept communications is not relevant for the question of foreseeability of the interference. In the WJSG the legislature set the scope for the transmission of lawfully obtained information precisely with person or bodies who do not themselves have the power to obtain such information.

39. The Government further submitted that adequate safeguards had been in place and that the interference was not disproportionate. They pointed out that criminal data may only be transmitted on the basis of strict criteria laid down in the WJSG. A 'compelling general interest' must exist, and information may only be transmitted in pursuit of one of the statutory purposes exhaustively listed in section 39f, paragraph 1, of the WJSG. For every transmission a balancing exercise by the Public Prosecution Service, guided by the principles set out in the Transmission (Designation) Order (see paragraphs 23-26 above), was required beforehand. The law did not prescribe that the reasoning of such a balancing test had to be provided in writing. This had been a conscious choice by the legislature. In addition, the law provided for safeguards in the form of judicial review *ex post facto*. The civil courts were competent to adjudicate on the transmission in tort proceedings, while the administrative courts could rule on the lawfulness of evidence obtained by transmission. *Ex ante* judicial review was not required either under domestic law or under Article 8 of the Convention.

2. The Court's assessment

(a) Whether there has been an interference

40. The Government have not disputed that the transmission of the data constituted an interference with the applicant company's rights under Article 8.

41. The Court reiterates that legal persons may, under certain circumstances, claim rights to respect of their business premises and correspondence under Article 8 (see, *inter alia*, *Naumenko and SIA Rix Shipping v. Latvia*, no. 50805/14, § 46, 23 June 2022, and *Bernh Larsen Holding AS and Others v. Norway*, no. 24117/08, §§ 105-06, 14 March 2013). It further notes that the transmission of data obtained through the interception of telecommunications to and their use by other authorities may constitute a separate interference with rights protected by this provision (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI, with further references; see also *Karabeyoğlu v. Turkey*, no. 30083/10, §§ 112-21, 17 June 2016).

42. Turning to the present case, the Court accepts that the transmission to the NMA of data obtained in the "Toto" criminal investigation through tapping of telephone conversations in which an employee of the applicant company took part, constituted an interference with this company's rights under Article 8 of the Convention (see, *mutatis mutandis*, *Kruslin v. France*, 24 April 1990, § 26, Series A no. 176-A; *Lambert v. France*, 24 August 1998, § 21, *Reports of Judgments and Decisions* 1998-V, and *Amann v. Switzerland* [GC], no. 27798/95, § 45, ECHR 2000-II).

(b) Whether the interference was justified

(i) Introductory remarks

43. As noted above, the complaints in the present case concern the transmission of certain data; they do not concern the interception of those data. The applicant company has raised Convention issues on the transmission of data in the context of competition law proceedings (see paragraphs 12-17 above). It is not in dispute between the parties that those data were lawfully obtained in the context of the criminal proceedings in which the interception orders were authorised by the investigating judge (see, by contrast, *Versini-Campinchi and Crasnianski v. France,* no. 49176/11, §§ 35 and 40, 16 June 2016, and *Adomaitis v. Lithuania,* no. 14833/18, §§ 79-80, 18 January 2022). Nor are there any indications that the applicant company would not have been able to effectively challenge the telephone tapping if it had wished to do so (compare *Bosak and Others v. Croatia,* no. 40429/14, §§ 62-65, 6 June 2019). The Court will, accordingly, proceed on the basis that the data were obtained through methods compatible with Article 8 of the Convention.

44. It remains, however, a fact that the subsequent transmission of the data took place without the applicant company' knowledge. It is for that reason that the Court considers the standards it has developed in the context of secret surveillance measures also relevant to the present case. Those standards may be summarised as follows.

45. The Court has held that the law's "foreseeability" requirement in the context of secret surveillance measures cannot mean that an individual should be able to foresee when the authorities are likely to intercept his or her communications so that he or she can adapt his or her conduct accordingly. However, where a power of the executive is exercised in secret the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, that are sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Dragojević*, cited above, § 81; *Roman Zakharov v. Russia* [GC], no. 47143/06, § 229, ECHR 2015; and *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, § 333, 25 May 2021).

46. Further, the Court has stressed the need for safeguards to avoid abuse of the power of secret surveillance; it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power (see *Bykov v. Russia* [GC], no. 4378/02, § 78, 10 March 2009, and *Dragojević*, cited above, § 82). The Court developed minimum safeguards that must be set out in domestic law, including the precautions to be taken when communicating the data obtained through interception of communications to other parties (see *Weber and Saravia* (dec.), cited above, § 95). On this latter safeguard, the Court has not yet provided specific guidance except in the special context of sharing intelligence material by a Contracting State to a foreign state or international organisations. In that context the Court adapted the minimum safeguards to the specific features of a bulk interception regime (see *Big Brother Watch and Others* [GC], cited above, § 347) and considered that the transmission should be limited to such material as had been collected and stored in a Convention compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself. It held, *inter alia*, that the circumstances in which such a transfer may take place must be set out clearly in domestic law and that the transfer of material obtained through bulk interception to foreign intelligence partners should also be subject to independent control (see *Big Brother Watch and Others* [GC], cited above, § 362). What is required by way of safeguards will thus depend on the context and, to some extent at least, on the nature and extent of the interference in question (see *P.G. and J.H. v. the United Kingdom*, no. 44787/98, § 46, 25 September 2001).

47. It is for the Court, when reviewing whether measures of covert surveillance are "in accordance with the law", to determine whether the

applicable domestic law, including the way in which it was interpreted by the domestic courts, indicated with reasonable clarity the scope and manner of exercise of the discretion conferred on the public authorities. Such a review necessarily entails some degree of abstraction. Nevertheless, in cases arising from individual applications, the Court must as a rule focus its attention not on the law as such but on the manner in which it was applied to the applicant in the particular circumstances. When reviewing whether the impugned interference was "necessary in a democratic society", the Court must determine whether the domestic system of covert surveillance, as applied by the domestic authorities, afforded adequate safeguards against abuse (see *Dragojević*, cited above, §§ 86 and 89; and *Kennedy v. the United Kingdom*, no. 26839/05, § 153, 18 May 2010).

48. The Court has acknowledged that the national authorities enjoy a certain margin of appreciation in assessing the existence and extent of such necessity. When a measure targets legal persons a wider margin of appreciation could be applied than would have been the case had it concerned an individual (see *Bernh Larsen Holding AS and Others*, cited above, §§ 158-59, and *Naumenko and SIA Rix Shipping*, cited above, § 51).

(ii) Whether the interference was in accordance with the law

49. The applicant company argued that the transmission of data which had no relevance to the criminal investigation had been insufficiently foreseeable (see paragraph 35 above). The Government contested that argument (see paragraphs 37-39 above).

50. The Court notes that the interference had a legal basis under Dutch law, namely section 39f of the WJSG (see paragraph 18 above). As to the requirement of the law's "foreseeability", the Court has accepted on different occasions that investigative methods may have to be used covertly (see, for example and amongst many other authorities, *Klass and Others v. Germany*, 6 September 1978, § 48, Series A no. 28). The criminal investigation against the I. company was still underway at the time of the first data transmissions, and at the time of the later transmissions the applicant company was under investigation by the NMA for price-fixing. Notification could thus have compromised that criminal investigation, its deployment of covert investigative measures, and an investigation of the applicant company by the NMA. Therefore, the Court accepts that, in the circumstances of the present case, the transmission of the data had to take place without the applicant company's prior knowledge. Similar to what the Court has held with regard to secret surveillance measures such as interception of communications (see paragraph 45 above), the requirement of foreseeability in the context at issue cannot be taken to mean that the authorities were obliged to notify the applicant company that they were going to transmit criminal data to the NMA.

51. The Court notes that there is also a difference between the situation of covert investigative measures in the case-law mentioned (see

paragraphs 45-47 above) and the interference posed by the transmission of data in the present case. The transmission of data was derivative of an interference which already provided for safeguards against arbitrariness and which the Court assumes was in accordance with Article 8 (see paragraph 43 above). For this reason already, the power to transmit the data obtained by that interference was not "unfettered". The Court considers that this difference is relevant for its assessment in the present case. Nevertheless, it will review, like in covert surveillance cases, whether the applicable domestic law, including the way in which it was interpreted by the domestic courts, gave an adequate indication to the applicant company as to the scope and manner of exercise of the authorities' discretion to transmit the data.

52. The Court notes, firstly, that section 39f of the WJSG – enacted pursuant to a transitional provision of the Personal Data Protection Act which required a *lex specialis* for the transmission of criminal data – sets out in law the limits of and the conditions for the transmission of data by the Public Prosecution Service. It further notes that the Transmission (Designation) Order provides clear instructions on the exercise of the power to transmit (see paragraph 18 above).

53. Further, in addressing the arguments raised by applicant company in support of its complaint that the impugned data transmission had not been sufficiently foreseeable (see paragraph 35 above), the Court notes the following.

54. On the basis of section 39f of the WJSG (see paragraph 18 above), the Court considers it sufficiently foreseeable that the NMA was authorised to receive criminal data from the Public Prosecution Service. Although the NMA was not mentioned as such, it is clear it is charged with the enforcement of the Competition Act (see paragraph 29 above). Authorities charged with enforcement of legislation are listed in section 39f of the WJSG as authorised to receive criminal data. Further, contrary to what the applicant company seems to suggest, the authorisation to receive those data is not made in some way dependent in the provision in question on the investigative powers of the receiving entity. In this connection the Court also notes that it follows from the Supreme Administrative Court for Trade and Industry's considerations that the WJSG precisely provides for the possibility, under strict conditions, that data obtained through coercive measures in criminal proceedings may be transmitted to defined other public authorities that do not have themselves the competence to use such coercive measures (see paragraph 17 above).

55. As regards the question whether it was sufficiently foreseeable on the basis of the applicable law that data not used for the criminal prosecution could also be transmitted, the Court notes the following. Criminal data were defined in section 1 of the WJSG in relation to the context in which they were obtained, as processed into the criminal file. Their definition does not relate to (possible) relevance to a prosecution, let alone to their final use by the prosecution in that case (see paragraph 18 above). Furthermore, as noted by

the Regional Court and the Supreme Administrative Court for Trade and Industry, it follows from the Explanatory Memorandum to the bill (see paragraph 20 above) that the legislature intended the term "criminal file" in this provision to be broad. This interpretation has been confirmed in the case-law of the Supreme Court (see paragraph 22 above).

56. Next, the Court observes that, while the text of section 39f of the WJSG (see paragraph 18 above) contains strict conditions for the transmission of criminal data by the Board of Procurators, it does not specify in which form the required balancing test should be carried out. However, it cannot be ignored that it clearly follows from the Explanatory Memorandum to the bill, as well as from the Transmission (Designation) Order, that the decision to transmit criminal data is qualified under the domestic legal framework as a factual act, not as a decision under the AWB (see paragraphs 19, 21-22, 27 and 31 above). In this regard, the present case is already to be distinguished from that in *Dragojević* (cited above), where formal requirements were explicitly provided for in the relevant domestic law (compare and contrast also *Liblik and Others v. Estonia*, nos. 173/15 and 5 others, § 140, 28 May 2019). That being so, the Court sees no reason to question the Supreme Administrative Court for Trade and Industry's conclusion that the decision of the public prosecutor to transmit criminal data is not one in the sense of the AWB and that it should carry out its own balancing test when assessing whether the evidence obtained in the context of a criminal investigation was lawfully provided to the NMA that used this material in proceedings for the imposition of an administrative fine and, in that context, whether the transmission of the data concerned was in compliance with Article 8 of the Convention (see paragraph 17 above). This approach also follows from the Supreme Court's case-law (see paragraphs 21 and 22 above).

57. Given the foregoing, the Court finds that the applicable law gave the applicant company an adequate indication as to the circumstances in which and the conditions on which the Public Prosecution Service was empowered to resort to the impugned data transmission. The exploratory interactions between officials of the VROM-IOD and the NMA were sufficiently foreseeable as part thereof. Within the relevant domestic legal framework described above, the two authorised public authorities, who had separate tasks and expertise, would need to coordinate in order to identify the data relevant for the required compelling general interest. There is no indication that anyone other than the VROM-IOD was in charge of the selection of data that the NMA was able to access or that it accessed more information than necessary for the authorised purpose.

58. The Court therefore accepts that the interference was "in accordance with the law". The Court finds it appropriate to examine the existence of adequate safeguards to avoid abuse as part of the question of whether the interference was "necessary in a democratic society" (compare *Kennedy*

v. United Kingdom, cited above, § 153, and *Naumenko and SIA Rix Shipping*, cited above, §§ 52-62).

(iii) Whether there was a legitimate aim for the interference

59. The Government argued that the data transmission had served the legitimate aim of protecting the economic well-being of the country, which was initially acknowledged by the applicant company and later contested.

60. Having regard to its previous findings in competition-law cases (see, for example, *Naumenko and SIA Rix Shipping*, cited above, § 49, with further references), the Court sees no reason to take a different view.

(iv) Whether the interference was necessary in a democratic society

61. The applicant company argued that the applicable domestic law, which does not provide for a judicial *ex ante* review of the data transmission, lacked sufficient guarantees against abuse and that the interference had been disproportionate (see paragraph 36 above). The Government contested that argument (see paragraph 39 above).

62. The Court reiterates that what is required by way of safeguards will depend on the context and on the nature and extent of the interference in question.

63. As to the question whether there were adequate safeguards to avoid abuse in the case at hand, it has already been noted that section 39f of the WJSG sets out in law the limits of and the conditions for the transmission of criminal data by the Public Prosecution Service (see paragraph 56 above). It further follows from the legislative history of the WJSG that the existence of a "compelling general interest" is explicitly linked to the legitimate aims listed in Article 8 § 2 of the Convention (see paragraph 19 above). In addition, the Transmission (Designation) Order provides clear guidance to the Public Prosecution Service for the exercise of the power to transmit, emphasising that such data might only be transmitted to public authorities if there is a legal basis for that authority to receive such information, if there was no other way for that authority to obtain the information that was less intrusive and if it was necessary for a purpose defined in section 39f of the WJSG (see paragraphs 23-27 above).

64. Also, there is an extensive *ex post facto* judicial oversight in place. In the administrative proceedings concerning the NMA's decision to impose a fine the applicant company could, and did, challenge the lawfulness and Convention compliance of the data transmission. As far as the transmitted data that were used for the NMA's decision are concerned, the applicant company's complaints could thus be redressed.

65. The fact that the object of these proceedings was the administrative decision by the NMA and not the transmission in itself cannot lead to the conclusion that insufficient safeguards were available, because the applicant

company, in addition to these proceedings, had access to proceedings before the civil courts. It was clear from the legislative history of the WSJG and the Transmission (Designation) Order that the civil courts were competent to rule on the lawfulness of the transmission in tort proceedings (see paragraphs 19 and 27 above). The civil courts could have prevented the data from being used by the NMA, if the transmission had been found to be unlawful. The applicant company submitted that in practice civil proceedings would not provide for a sufficiently thorough review, but it has not provided any substantiation or examples of this.

66. The present case is not comparable to that in *Sanoma Uitgevers B.V.*, cited by the applicant company (see paragraph 36 above), which concerned the vital importance to press freedom of the protection of journalistic sources and of information that could lead to their identification, and did not concern transmission of lawfully obtained data between law enforcement authorities.

67. Given the nature and extent of the interference in the present case, in combination with the safeguards that were in place under the domestic legal framework, including the precautions taken when communicating the data obtained through interception of communications to another public authority, the Court is satisfied that the system was adequately capable of avoiding abuse of power and finds that Article 8 did not require *ex ante* authorisation by a court in the context at issue.

68. Turning to the question of whether the interference was proportionate, the Court notes that the domestic courts carefully examined the facts, assessed the lawfulness of the transmission under the WSJG and conducted an adequate balancing exercise under Article 8 of the Convention between the interests of the applicant company and the authorities' interests to protect the economic well-being of the country (see paragraph 17 above). In that connection the Court also takes account of the fact that the applicant company has not put forward any arguments as to why the interference did not pursue a legitimate aim or as to why the balance struck by the domestic authorities was not fair in their particular case.

69. The foregoing leads the Court to the conclusion that the domestic authorities have put forward relevant and sufficient reasons to justify the necessity and proportionality of the data transmission for the purposes of enforcement of competition law.

(c) Conclusion

70. There has accordingly been no violation of Article 8 of the Convention.

II. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

71. The applicant company complained that in respect of its complaint under Article 8 it had not had access to an effective remedy as provided in Article 13 of the Convention, which reads as follows:

> "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

A. Admissibility

72. The Government did not wish to submit any observations on the admissibility of the complaint.

73. The Court notes that this complaint is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

74. The applicant company complained that it had been deprived of an effective remedy because it had not been notified of the transmission beforehand, and that it had not had access to *ex ante* judicial oversight. Relying on *Čonka v. Belgium* (no. 51564/99, § 79, ECHR 2002-I), the applicant company argued that this had been required to prevent irreversible harm, as the NMA officials with access to the data could not forget what they had seen.

75. The Government argued that the applicant company had had effective remedies at their disposal in civil and administrative proceedings. In their view, Article 13 did not require judicial review prior to transmission.

76. In the light of its considerations and findings under Article 8 of the Convention (see paragraphs 43-70 above), the Court finds that the applicant company had an effective remedy at its disposal to raise its complaints under that provision.

77. There has accordingly been no violation of Article 13 of the Convention in conjunction with Article 8 of the Convention.

FOR THESE REASONS, THE COURT

1. *Declares,* unanimously, the application admissible;

2. *Holds*, by four votes to three, that there has been no violation of Article 8 of the Convention;

3. *Holds*, unanimously, that there has been no violation of Article 13 of the Convention in conjunction with Article 8 of the Convention.

Done in English, and notified in writing on 16 May 2023, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Milan Blaško	Pere Pastor Vilanova
Registrar	President

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

P.P.V.
M.B.

JOINT DISSENTING OPINION OF JUDGES GROZEV, PAVLI AND KTISTAKIS

We regret that we are unable to follow the majority in its conclusion that there has been no violation of Article 8 of the Convention in the present case. In our joint dissenting opinion in *Janssen de Jong Groep B.V. and Others v. the Netherlands* (no. 2800/16, 16 May 2023), decided on the same day, we have elaborated on what we consider to be certain significant flaws in the national legal framework and practice which rendered the transmission of the secret surveillance data to the Dutch Competition Authority inconsistent with the safeguards required by Article 8 of the Convention. As these shortcomings are primarily related to the role of the public prosecutor under section 39f of the Judicial and Criminal Data Act, they are equally applicable to the present case. Furthermore, the administrative proceedings conducted by the Competition Authority in this case were even further removed from the original proceedings that gave rise to secret surveillance measures than they were in the circumstances of the case in *Janssen de Jong Groep B.V. and Others*. We conclude, therefore, that there has been a violation of Article 8 of the Convention.