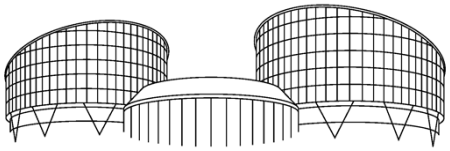

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

THIRD SECTION

CASE OF JANSSEN DE JONG GROEP B.V. AND OTHERS v. THE NETHERLANDS

(Application no. 2800/16)

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 Janssen de Jong Groep B.V. and Others 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. 2800/16) 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 three Dutch limited liability companies, Janssen de Jong Groep B.V., Janssen de Jong Infra B.V. and Janssen de Jong Infrastructuur Nederland B.V. (hereinafter also referred to as "the applicant companies"), on 6 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 companies complain 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 companies are limited liability companies engaged in construction, incorporated under Dutch law. Janssen de Jong Groep B.V. is the sole shareholder of Janssen de Jong Infrastructuur Nederland B.V., which is in turn the sole shareholder in Janssen de Jong Infra B.V. They were initially 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. Around 2007 suspicions arose that local government officials had been bribed by building contractors desirous of winning government contracts for infrastructure projects. The Public Prosecution Service (*Openbaar Ministerie*), assisted by the National Police Internal Investigations Department (*Rijksrecherche*), began an investigation under the codename "Cleveland", which implicated the applicant companies as suspects. In the context of this investigation, some of the applicant companies' employees were subjected to interception of their telephone conversations. The interception orders were authorised by an investigating judge (*rechter-commissaris*).

6. Certain intercepted telephone conversations were identified as being of potential interest to the Netherlands Competition Authority (*Nederlandse Mededingingsautoriteit* – "the NMA") because they contained indications of price-fixing. On various dates in July 2008 police officers gave NMA officials access, in strict confidence and on police premises, to a selection of written reports (*processen-verbaal*) of the intercepted communications. Upon request by the NMA, the police subsequently also gave access to other written reports that concerned the same companies and persons as in the initial selection. The NMA officials were allowed to make notes, which they had to leave with the police before they left. The NMA drew up reports of these meetings.

7. On 19 August 2008 the public prosecutor (*officier van justitie*) in charge provided a CD to the NMA with selected recordings of the intercepted telephone conversations for information purposes only and in strict confidence. He indicated in his accompanying letter that they could not be used for any other purpose except with his permission.

8. On 9 December 2008 the NMA started an official investigation into possible violations of the Competition Act (*Mededingingswet*) and requested the Public Prosecution Service permission to use the data.

9. On 16 December 2008 the public prosecutor wrote to the NMA in the following terms:

> "Having regard to your fax message of 15 December 2008 I give you permission to use the information gathered during the 'Cleveland' investigation (which was carried out by the National Police Internal Investigations Department under my supervision) for the purpose of your investigation(s) into violations of the Competition Act."

According to information submitted by the Government the data transmitted to the NMA amounted to approximately 2% of the total number of recordings of telephone conversations intercepted in the context of the "Cleveland" investigation.

10. On 27 and 28 January 2009 the NMA inspectors visited the business premises of one of the applicant companies and requested access to their books for their investigation and on 21 April 2009 the NMA inspectors questioned employees of the applicant companies under caution.

11. On 28 May 2009 the public prosecutor in charge wrote to the applicant companies' then counsel that information obtained in the course of the "Cleveland" investigation had been transmitted to the NMA in accordance with the Judicial and Criminal Data Act (*Wet Justitiële en Stravorderlijke gegevens* – "the WJSG"; see paragraph 22 below) and in accordance with 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*; see paragraphs 27-31 below).

II. CIVIL PROCEEDINGS

12. The applicant companies summoned the State before the provisional-measures judge (*voorzieningenrechter*) of the Regional Court (*rechtbank*) of The Hague, seeking a provisional order requiring the NMA to return the transmitted data to the Public Prosecution Service and to desist from making use of them, and seeking a provisional order prohibiting the Public Prosecution Service from the transmission of such data. They relied, *inter alia,* on Article 8 of the Convention.

13. The provisional-measures judge gave judgment on 26 June 2009, dismissing the applicant companies' requests (ECLI: NL: RBSGR: 2009: BJ0047). His reasoning included the following:

> "In my provisional view, it is for the present sufficiently established that ... the transmission of the intercepted telephone conversations to the NMA with a view to further investigation by the NMA and with a view to the enforcement of section 6(1) of the Competition Act, is necessary for the [protection of the] economic well-being of the Netherlands. I consider that this interest carries more weight than the interest of protecting the privacy of [the applicant companies]. True, [the applicant companies] have disputed that the interference with their interest resulting from the transmission of the telephone conversations to the NMA is proportionate to the interest of the economic well-being of the Netherlands, but they have failed to make out a sufficiently well-reasoned case for the opposite view. Nor has a sufficiently convincing *prima facie* case been made out that the information concerning the alleged price-fixing among building contractors could reasonably have been obtained in a different, less disadvantageous way, given that such agreements tend as a rule not to be committed to paper. The above leads me to conclude that the transmission of the intercepted telephone conversations by the Public Prosecution Service based on section 39f(1) of the WJSG is not incompatible with Article 8 of the Convention."

14. The applicant companies did not appeal against this judgment and did not institute civil proceedings on the merits of the case.

III. ADMINISTRATIVE PROCEEDINGS

15. Based on the results of its investigation, the NMA concluded that during the period from March to December 2008, one of the applicant companies coordinated bidding figures with other companies and exchanged information about their intended bidding behaviour prior to bidding on a number of tenders. In doing so, these companies violated section 6 of the Competition Act (see paragraph 33 below). On 29 October 2010 the NMA imposed a fine on the applicant companies in the amount of 3,000,000 euros (EUR).

16. The applicant companies lodged a written objection (*bezwaarschrift*), which the NMA dismissed on 8 March 2012.

17. The applicant companies subsequently lodged an appeal (*beroep*) with the Rotterdam Regional Court. They submitted that the transmission of the data was unlawful, arguing that the WJSG was not applicable because the transmitted data did not qualify as 'criminal data'. In that respect they noted that the recordings of the intercepted telephone conversation had not been processed into the criminal file and that this information had been irrelevant for the criminal investigation. Further, they argued, relying on Articles 8 and 13 of the Convention, that in any event it had not been foreseeable on the basis of the applicable law that those data might be transmitted, and that no prior review by an independent court had taken place. The intercepted telephone conversations should therefore not be admitted as evidence. In any case, there had been no price-fixing.

18. The Regional Court gave judgment on 13 June 2013 (ECLI:NL:RBROT:2013:CA3079), declaring the applicant companies' appeal well-founded. Referring to the Explanatory Memorandum (see paragraph 24 below), it held that the transmitted data did qualify as 'criminal data' within the meaning of the WJSG and that section 39f(1) provided the statutory basis for the impugned transmission of data. However, since the case file did not contain a knowable, reviewable weighing of interests by the public prosecutor, the Regional Court was of the view that the NMA was not entitled in this case to use the intercepted telephone conversations as evidence. It considered that the NMA should, before making use of this information, have satisfied itself that the public prosecutor was of the view that there was a compelling general interest at stake, and why transmission was necessary for that purpose, because otherwise justice would not be done to the requirements of Article 8 of the Convention, which are precisely the requirements of which section 39f of the WJSG is intended to ensure compliance. Since the NMA, apart from the transmitted data, had not provided sufficient other evidence, the Regional Court quashed the NMA's decision.

19. 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, which had indeed taken place in the present case. 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 34 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.

20. The applicant companies 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.

21. The Supreme Administrative Court for Trade and Industry gave judgment on 9 July 2015 (ECLI:NL:CBB:2015:193). It quashed the Regional Court's judgment, dismissed the applicant companies' cross-appeal and referred the case back to the Regional Court. Its reasoning included the following:

> "3.4 ... 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 26 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. [..].

4.6 ... 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 for 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.

4.7 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.

4.8 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.

4.9 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 for 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 applicant companies], the circumstance that the ACM had access to a bulk of the data that were available and provisionally considered relevant by the public prosecution service, on the basis of which a selection was made, 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

22. 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

23. 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.

24. 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 34 below]. ... The act is aimed solely at the factual transmission of information relating to criminal data."

C. Relevant domestic case-law

25. In his advisory opinion to the Supreme Court of 3 February 2012 in the *Trafigura* case (ECLI:NL:PHR:2012:BV3436 – see paragraph 21 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."

26. 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

27. 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.

28. 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.

29. 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.

30. 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 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.

31. 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 COMPETITION ACT

32. 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.

33. 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).

III. THE GENERAL ADMINISTRATIVE LAW ACT

34. 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

35. The applicant companies complained that the transmission to the NMA of data that were irrelevant to the criminal investigation had constituted a violation of their 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

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

37. 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 companies

38. The applicant companies submitted that the transmission of the tapped information to the NMA had not been in accordance with the law. They 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, they 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. They 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. They considered their case to be comparable to that in

Dragojević v. Croatia (no. 68955/11, 15 January 2015). Lastly, they argued that it had not been foreseeable on the basis of the applicable domestic law that the NMA could gain confidential access to the data before the official transmission. In their 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.

39. The applicant companies 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), they 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, they 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. They further argued 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

40. 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.

41. 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 22 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.

42. 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 27-30 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

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

44. 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).

45. Turning to the present case, the Court accepts that the transmission to the NMA of data obtained in the "Cleveland" criminal investigation against the applicant companies through tapping of their employees' telephones constituted an interference with those companies' rights under Article 8 of the Convention.

(b) Whether the interference was justified

(i) Introductory remarks

46. 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 companies have raised Convention issues on the transmission of data in the context of competition law proceedings (see paragraphs 15-21 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 companies would not have been able to effectively challenge the telephone tapping if they 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.

47. It remains, however, a fact that the subsequent transmission of the data took place without the applicant companies' 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.

48. 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).

49. 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).

50. 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).

51. 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

52. The applicant companies argued that the transmission of data which had no relevance to the criminal investigation had been insufficiently foreseeable (see paragraph 38 above). The Government contested that argument (see paragraphs 40-42 above).

53. The Court notes that the interference had a legal basis under Dutch law, namely section 39f of the WJSG **(**see paragraph 22 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 applicant companies (and its employees) was still underway at the time of the transmission of the relevant data (see paragraphs 5-9 above). Notification could thus have compromised the criminal investigation, its deployment of covert investigative measures, and an investigation of the applicant companies 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 companies' prior knowledge. Similar to what the Court has held with regard to secret surveillance measures such as interception of communications (see paragraph 48 above), the requirement of foreseeability in the context at issue cannot be taken to mean that the authorities were obliged to notify the applicant companies that they were going to transmit criminal data to the NMA.

54. The Court notes that there is also a difference between the situation of covert investigative measures in the case-law mentioned (see paragraphs 48-50 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 46 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 companies as to the scope and manner of exercise of the authorities' discretion to transmit the data.

55. 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 22 above).

56. Further, in addressing the arguments raised by applicant companies in support of their complaint that the impugned data transmission had not been sufficiently foreseeable (see paragraph 38 above), the Court notes the following.

57. On the basis of section 39f of the WJSG (see paragraph 22 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 32 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 companies seem 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 21 above).

58. 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 22 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 24 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 26 above).

59. Next, the Court observes that, while the text of section 39f of the WJSG (see paragraph 22 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 23, 25-26, 31 and 34 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 21 above). This

approach also follows from the Supreme Court's case-law (see paragraphs 25 and 26 above).

60. Given the foregoing, the Court finds that the applicable law gave the applicant companies 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 the Public Prosecution Service 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 Public Prosecution Service 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.

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

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

62. 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.

63. 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

64**.** The applicant companies 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 39 above). The Government contested that argument (see paragraph 42 above).

65. 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.

66. 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 59 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 23 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 27-31 above).

67. 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 companies 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 companies' complaints could thus be redressed.

68. 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 companies, 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 23 and 31 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 companies submitted that in practice civil proceedings would not provide for a sufficiently thorough review, but they have not provided any substantiation or examples of this.

69. The present case is not comparable to that in *Sanoma Uitgevers B.V.*, cited by the applicant companies (see paragraph 39 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.

70. 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.

71. 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 companies and the authorities' interests to protect

the economic well-being of the country (see paragraphs 13 and 21 above). In that connection the Court also takes account of the fact that it transpires from the Government's submissions that the transmission concerned only 2% of the intercepted telephone conversations (see paragraph 9 above), about which the applicant companies have not made any submissions in reply, and that the applicant companies have 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.

72. 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

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

II. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

74. The applicant companies complained that in respect of their complaint under Article 8 they 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

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

76. 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

77. The applicant companies complained that they had been deprived of an effective remedy because they had not been notified of the transmission beforehand, and that they had not had access to *ex ante* judicial oversight. Relying on *Čonka v. Belgium* (no. 51564/99, § 79, ECHR 2002-I), they 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.

78. The Government argued that the applicant companies 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.

79. In the light of its considerations and findings under Article 8 of the Convention (see paragraphs 46-73 above), the Court finds that the applicant companies had an effective remedy at their disposal to raise their complaints under that provision.

80. 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 Registrar	Pere Pastor Vilanova 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

1. The present case involves the transfer and use of data obtained through secret surveillance, initially authorised by a judge for the purposes of a criminal investigation, to an administrative authority for the purposes of a separate and unrelated investigation into the applicant company. We regret that we are unable to follow the majority in finding that there has been no violation of Article 8 of the Convention in this case. In our view, the applicant company's right to respect for its correspondence was violated as a result of certain structural flaws in the national legal framework, combined with a lack of sufficient safeguards and adequate reasoning provided by the national authorities in the specific circumstances of the present case.

I. A NEED FOR FURTHER JURISPRUDENTIAL DEVELOPMENT

2. We consider that the present case raises a number of serious and novel questions of Article 8 interpretation. We find ourselves in agreement with the principled objections put forward by Judge Koskelo in her partially dissenting opinion in the judgment in *Adomaitis v. Lithuania* (no. 14833/18, 18 January 2022), decided by the Second Section of the Court in January 2022. Beyond that, we note that the approach followed by the respective majorities in these two cases differed in significant respects, including as to the lines of case-law applied to similar matters.

3. Among other aspects calling for a more consistent interpretation, the present case also raises a methodological question: should the same or at least similar standards apply in this context to physical persons (such as the applicant in *Adomaitis*) versus legal persons (such as the applicant company in the present case)? In our view, the confidentiality interests protected by Article 8 in a secret surveillance context require similar safeguards in both scenarios. While our case-law may permit a somewhat "wider margin of appreciation" when it comes to interferences with the Article 8 rights of legal persons (see paragraph 51 of the present judgment, and the cases cited therein), this is a matter of balancing in the final proportionality analysis, rather than a paradigmatic difference of approach.

4. The response to this preliminary question is also relevant for determining the legal standards and lines of case-law that may be invoked, under both the Convention and European comparative law more generally. While personal data protection regimes typically apply to physical persons alone, they can provide helpful guidance in determining the general standards that ought to apply to the confidentiality interests of legal persons in a secret surveillance context in respect of secondary processing or transfers of such data to additional public authorities, also because such information could contain the personal data of individuals, including of a sensitive nature. It is

for this reason that we refer in our analysis to certain European Union data protection standards that we consider to be of relevance. Conversely, today's judgment relies exclusively on the secret surveillance line of case-law and includes no references to general data protection principles, even on a *mutatis mutandis* basis.

II. THE NATURE OF THE INTERFERENCE AND THE APPLICABLE TEST

5. The first challenge posed by this case relates to the proper characterisation of the interference with the applicant company's confidentiality interests in a context where lawfully obtained surveillance data, authorised for a given purpose, were transferred to a different authority for the purposes of a separate and unrelated investigation of the same company concerning alleged infractions of a less serious gravity. The majority placed a good deal of emphasis on the fact that the original surveillance had been lawfully authorised (see paragraph 54 of the judgment), as did the majority in *Adomaitis* (cited above). In our view, this is neither sufficient, nor entirely pertinent. The original judicial authorisation was granted for the purposes of an unrelated criminal investigation on the basis of reasonable suspicion of a certain criminal activity (bribery of government officials); the authorising judge could not have been aware that "by-catch" from that surveillance would subsequently reveal indications of a different kind of violation of the law (namely, anti-competitive behaviour). As such, the original authorisation cannot be considered to have justified further use and transfer of any by-catch data for possible administrative investigations that might come in many different forms and levels of gravity. The power to authorise transfers of criminal data belongs in the Dutch system to a public prosecutor, a matter to which we come back below. Secondly, it is also relevant that the secondary investigation was not of a criminal nature or such that would have been capable of justifying secret surveillance measures on its own.

6. In these circumstances, the further transfer and processing of by-catch data for unrelated purposes constitutes an additional and serious interference with the privacy and confidentiality interests protected by Article 8. As such, it must be accompanied by robust safeguards, which must also ensure that such an arrangement cannot be abused to *circumvent* the rather stringent conditions for authorising secret surveillance in the first place. This position is consistent with that adopted by the Grand Chamber of the Court in *Big Brother Watch and Others v. the United Kingdom* ([GC], nos. 58170/13 and 2 others, 25 May 2021) in which it held that the transmission of bulk interception data to foreign States and international organisations "should be limited to such material as has been collected and stored in a Convention-compliant manner *and should be subject to certain additional*

specific safeguards pertaining to the transfer itself" (ibid., § 362, emphasis added; see also *Centrum för Rättvisa v. Sweden* [GC], no. 35252/08, §§ 317-30, 25 May 2021).

7. The next question in the analysis relates to the precise nature of those additional transfer-specific safeguards. The Court's long-standing case-law holds that, in the context of secret surveillance, the minimum safeguards that must be set out in domestic law should include "precautions to be taken when communicating the data ... to other parties" (see paragraph 49 of the present judgment). However, the case-law is relatively scarce on the precise nature of these guarantees, depending also on the identity of those third-party recipients (for example, domestic versus foreign recipients). It was only relatively recently, in the *Big Brother Watch and Others* and *Centrum för Rättvisa* cases (both cited above), that the Court provided some additional guidance, in the context of transfers of data obtained through bulk surveillance to foreign States or international organisations. Of the four safeguards identified in those judgments, two appear to be most pertinent to the present case and more generally to a context of *domestic* transfers between two or more national authorities: that the circumstances in which such a transfer may take place must be set out clearly in domestic law; and that the transfer should also be subject to independent control (see *Big Brother Watch and Others*, cited above, § 362, and paragraph 49 of the present judgment). No further guidance has been provided on the nature of such "independent control" – in particular whether it should be *ex ante*, *ex post facto* or a combination of both.

8. With respect to the first criterion – the circumstances that can justify further sharing, for unrelated secondary purposes, of criminal investigation data obtained through secret surveillance – we believe that the Court's case-law needs to be developed beyond the mere legality requirement by addressing also the quality of those secondary purposes. In particular, national law should set a certain minimum *level of gravity* of potential breaches of the law the investigation of which can justify the further transfer of criminal investigation data, especially if such non-criminal infringements are not capable of triggering the use of secret surveillance measures on their own. Such an approach is necessary to avoid circumvention of the strict safeguards around secret surveillance and "fishing expeditions" by law-enforcement authorities more generally. To put it plainly, data obtained for the investigation of serious crime should not be used to enforce traffic regulations. Furthermore, the principle of data minimisation should apply, requiring the transferring authority to share no more than is necessary for the secondary investigative purpose.[1] Finally, the proportionality of the further

[1] See, *mutatis mutandis*, the judgment of the Court of Justice of the European Union (CJEU) of 2 March 2023 in *Norra Stockholm Bygg AB* (C-268/21, ECLI:EU:C:2023:145), involving a private contractual dispute in which the claimant sought to obtain the staff register data of the defendant company (held for tax-law purposes), which included staff's personal data.

transmission of intercepted information should be assessed, weighing the character of the personal (or otherwise protected) data contained therein and its sensitivity against the gravity of the suspected illegal conduct.

9. Secondly, while some form of *ex post facto* judicial protection is essential, robust safeguards should also be provided *prior* to the transfer of secret surveillance data to another public authority, especially if such a transfer is made for a purpose other than the legitimate aim that justified the original collection and if the subject matters, or the identified suspects or investigation targets, in the two sets of proceedings are not linked or closely related. This follows from two sets of considerations: the highly intrusive nature of secret surveillance and the fact that any further unlawful sharing of such data within the government is likely to produce some degree of irreparable harm; and, secondly, general principles of data protection law requiring that protected data should only be processed for purposes other than those for which the data were collected subject to stringent conditions (known as the principle of purpose limitation).[2]

III. THE QUALITY OF THE STRUCTURAL SAFEGUARDS IN THE DUTCH SYSTEM

10. We turn now to the structural safeguards contained in the national legal system, as relevant and applied by the national authorities in the present case. It is worth recalling that the case involved the transfer of criminal investigation data, obtained through judicially authorised secret surveillance, for the purposes of an administrative investigation that was (a) entirely unrelated to the subject matter of the original criminal investigation ("by-catch" data), and (b) of a nature that would not be capable of authorising secret surveillance measures on its own. In fact, the Competition Authority

---

[2] See, for example, Article 4 § 2 of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, which provides as follows:
"Processing by the same or another controller for any of the purposes set out in Article 1(1) [other enumerated law-enforcement purposes] other than that for which the personal data are collected shall be permitted in so far as: (a) the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and (b) processing is necessary and proportionate to that other purpose in accordance with Union or Member State law."
See also the opinion of Advocate-General Campos Sanchez-Bordona delivered on 30 March 2023 in *Lietuvos Respublikos generalinė prokuratūra* (Case C-162/22, ECLI:EU:C:2023:266), currently pending before the CJEU (concerning a request for a preliminary ruling as to whether personal data obtained in a criminal investigation may subsequently be used in "linked" disciplinary proceedings of an administrative nature against a public official).

enjoys no powers under national law to request surveillance measures in the exercise of its administrative law enforcement functions. It is, therefore, a context that requires that any sharing of criminal investigation data be subject to particularly stringent safeguards.

11. The transfer of "criminal data" to other public authorities is possible under Dutch law for the purposes of "enforcement of legislation" and to the extent that those data are "necessary in view of a compelling general interest or the determination, exercise or defence of a right in law" (see section 39f of the Judicial and Criminal Data Act, as reproduced in paragraph 22 of the present judgment). The decision to transfer the criminal data to another public authority is made by a public prosecutor, without any further checks at that stage. The Board of Prosecutors General provided further instructions on the transmission of criminal data "for purposes other than criminal law enforcement" through a 2008 Order (see paragraph 28 of the judgment).

12. In our view, the necessity requirement tied to "a compelling general interest", at least as construed in the present case, is generally adequate as a statutory threshold that limits the further transmission of criminal data obtained through secret surveillance.[3] We agree with the Chamber majority that the investigation and sanctioning of anti-competitive practices is, in principle, a sufficiently compelling public interest, which corresponds to protection of "the economic well-being of the country" under the second paragraph of Article 8 of the Convention.

13. At the same time, it would have been preferable for the prosecutorial instructions to have provided more detailed and specific guidance as to the level of gravity of non-criminal infractions capable of meeting the threshold for transmission. The same can be said about the apparent lack of guidance on procedures and criteria for further data minimisation. Such criteria could refer, in addition to the gravity of the suspected non-criminal infraction, to the reliability of the evidence supporting those suspicions and the sensitivity of the data at stake, among others.

14. More importantly, we disagree with the majority that the public prosecutor's decision-making process in transferring the criminal data to the Competition Authority met the "independent control" requirement or was otherwise compliant with Article 8 standards. To begin with, it is rather questionable whether a public prosecutor, as the only authority to provide any *ex ante* control in the Dutch system, can be deemed capable of ensuring "independent control" prior to the actual transfer.[4] We do not, however, need

[3] The same cannot be said, however, of the second limb of section 39f(2)(a): "the determination, exercise or defence of a right in law" appears to be an extremely open-ended and loose threshold, capable of justifying transfers in relation to virtually any breach of the law irrespective of its level of gravity. That notwithstanding, this second limb appears to have played no role in the present case.

[4] See, *mutatis mutandis*, the judgment of the CJEU of 2 March 2021 in *H.K.* (C-746/18, ECLI:EU:C:2021:152), addressing, *inter alia*, the question as to whether the Estonian public

to take a firm position on this aspect, as the decision-making process suffers, in our view, from a more serious flaw. While prosecutors are required, in principle, to undertake a balancing of interests and to assess the necessity and proportionality of the transfer, they are not required to record the outcome of that process in a properly reasoned decision. Such a transfer is treated under national law merely as a "physical act", rather than as a legal measure constituting a serious and additional interference with the fundamental privacy interests of natural and legal persons. Providing a properly reasoned decision for such an interference would appear to be the minimum required by Article 8 by way of *ex ante* independent control; on this point, we are in agreement with the view of the Rotterdam Regional Court that the case file did not contain "a knowable, reviewable weighing of interests" (see paragraph 18 of the present judgment).

15. We consider this to be a significant structural flaw in the national legal framework, which weighed heavily in our conclusion in favour of finding a violation of Article 8. For the reasons we have already posited above as to the importance of robust *ex ante* controls, we consider that the various forms of *ex post facto* judicial review that were available and used by the applicant company were not sufficient to remedy the shortcomings of the initial prosecutorial decision-making. We are of the view that the applicant company was correct in relying on the Court's established position that the absence or insufficiency of reasons at the original stage of authorisation of secret surveillance measures cannot be remedied retroactively, for example, on appeal (see *Dragojević v. Croatia*, no. 68955/11, 15 January 2015, and *Liblik and Others v. Estonia*, nos. 173/15 and 5 others, 28 May 2019). The same rationale is applicable in the present context as the further sharing of criminal data, which had not, as such, been authorised by the investigating judge, should be treated as an additional and potentially equally serious interference with the applicant company's Article 8 rights.

IV. OTHER NECESSITY CONSIDERATIONS

16. In addition to the foreseeability of the legal framework and the quality of the general safeguards contained therein (as addressed above) – and even though the two branches of the analysis are closely interlinked in this context – it is necessary to also assess the reasons provided by the national authorities as to the necessity and proportionality of the interference in the concrete circumstances of the case.

17. The 2008 Transmission (Designation) Order included a number of instructions for public prosecutors in making transmission decisions: they should ensure that there is a legal basis for the receiving authority to receive

---

prosecutor's office could be regarded as an independent administrative authority capable of authorising access of the investigating authority to data relating to electronic communications.

such data; that there is no other way for that authority to obtain the information in a less intrusive way (the *ultima ratio* rationale); and that the transfer is actually necessary for a lawful purpose, such as enforcement of legislation. At the same time, as already noted, there appears to have been no explicit guidance on the proportionality assessment and on data minimisation criteria and procedures. Be that as it may, the absence of any reasoned decision by the prosecutor in the present case means that neither the national authorities, nor this Court are in a position to carry out a reliable and intelligent assessment as to the quality of the balancing exercise carried out by the public prosecutor. The *ex post facto* assessment by the national courts is not capable of remedying this omission retroactively.

18. While the preceding analysis would be sufficient for a finding of a violation of Article 8, we would also add that we are not persuaded that the *ex post facto* judicial review conducted by the Supreme Administrative Court for Trade and Industry was in line with Article 8 standards either. The Chamber majority concludes, within a brief paragraph, that the domestic courts "conducted an adequate balancing exercise under Article 8" – an assertion that is rather striking in its lack of any further substantiation (see paragraph 71 of the present judgment).

19. An important element of the proportionality analysis, under both national and Convention standards, is whether the use of secret surveillance methods can be justified on *ultima ratio* grounds. In this respect, the national court found, in rather summary fashion, that the condition had been met because price-fixing agreements "[were] not, as a rule, put in writing" (see point 4.9 of the judgment of the Supreme Administrative Court for Trade and Industry, as cited in paragraph 21 of the present judgment). With respect, we do not find such reasoning to be persuasive. To begin with, the absence of a written agreement to commit illegal acts would seem to us to be the norm rather than an exception providing justification for special measures. Secondly, the fact that the Competition Authority has no legal powers to request secret surveillance measures suggests that it is normally considered to be capable of fulfilling its competition law enforcement functions without resorting to surveillance – and that exceptional circumstances would be needed to justify such use. Finally, unlike the alleged instances of criminal bribery that gave rise to the original surveillance authorisation, price-fixing practices tend to have above-the-surface aspects that can serve as a starting-point for administrative investigations.

20. In the light of the above considerations, we conclude that the national courts did not provide sufficient reasons for the necessity in a democratic society of the interference with the applicant company's Article 8 rights.

APPENDIX

List of applicant companies:

1. JANSSEN DE JONG GROEP B.V. is a limited liability company incorporated under Netherlands law having its statutory seat in Son en Breugel.
2. JANSSEN DE JONG INFRA B.V is a limited liability company incorporated under Netherlands law having its statutory seat in Roermond.
3. JANSSEN DE JONG INFRASTRUCTUUR NEDERLAND B.V. is a limited liability company incorporated under Netherlands law having its statutory seat in Son en Breugel.