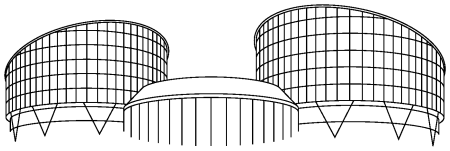

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

GRAND CHAMBER

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

(Application no. 2799/16 and 3 others – see appended list)

JUDGMENT

Art 8 • Correspondence • Transmission and use in competition law proceedings of data lawfully obtained through telephone tapping in criminal investigations • Transmission of intercept data for further use by another law-enforcement authority constituted a separate interference with Article 8 rights, distinct from original interception • Minimum safeguards set out by the Court for communicating intercept data to another law-enforcement authority to avoid arbitrariness and abuse • Transmissions to be limited to material collected in a Convention-compliant manner • Breadth of margin of appreciation depended on the content and nature of the data at issue and not on applicant's physical or legal nature or status • Minimum safeguards under Art 8 in principle the same for natural and legal persons • Impugned data transmission had legal basis in domestic law which fulfilled "foreseeability" requirements • Transmission authorisations by a non-judicial authority compatible with Art 8 • Art 8 not to be construed as guaranteeing prior notification of the transmission of intercept material or, by implication, to participate in any review prior to the transmission • In case-circumstances, absence of written reasoning in transmission authorisations and of prior notice of the transmissions compensated for by the effective *ex-post facto* judicial review conducting a *de novo* assessment and capable of affording the applicant companies appropriate redress • Redress in the form of the destruction of transmitted data or monetary compensation not necessarily required for a remedy concerning intercept data transmission • Restrictions on the use of such data might afford sufficient redress • Adequate safeguards against arbitrariness and abuse • Applicant companies afforded opportunity to effectively contest the transmissions • Adequate balancing exercise between interests at stake • Relevant and sufficient reasons justifying necessity and proportionality of interference for the purposes of enforcement of competition law
Art 13 (+ Art 8) • Effective remedy

STRASBOURG

1 April 2025

This judgment is final but it may be subject to editorial revision.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

TABLE OF CONTENTS

PROCEDURE **4**

INTRODUCTION **6**

THE FACTS **6**

THE CIRCUMSTANCES OF THE CASE 6

A. Ships Waste Oil Collector B.V., Burando Holding B.V. and Port Invest B.V. v. the Netherlands (nos. 2799/16, 3124/16 and 3205/16 – "the first group of applicant companies") 6

1. Criminal proceedings and data transmission 6
2. Administrative proceedings 8
   (a) The decision by the NMA to impose fines and the administrative review proceedings 8
   (b) Appeal proceedings before the Rotterdam Regional Court 9
   (c) Further appeal proceedings before the Supreme Administrative Court for Trade and Industry 10
3. Subsequent developments 14

B. Janssen de Jong Groep B.V. and Others v. the Netherlands ..... (no. 2800/16) 14

1. Criminal proceedings and data transmission 14
2. Civil proceedings 16
3. Administrative proceedings 18
   (a) The decision by the NMA to impose fines and the administrative review proceedings 18
   (b) Appeal proceedings before the Rotterdam Regional Court 18
   (c) Further appeal proceedings before the Supreme Administrative Court for Trade and Industry 20

4. Subsequent developments 20

RELEVANT LEGAL FRAMEWORK AND PRACTICE 21

I. DOMESTIC LAW AND PRACTICE 21

A. Constitution of the Kingdom of the Netherlands 21

B. The Judicial and Criminal Data Act 21

1. Relevant provisions 21

2. Legislative history 22

3. WJSG Instructions 25

4. Relevant domestic case-law 27

5. The Agreement between the Public Prosecution Service and the NMA 27

C. The Special Investigative Services Act 28

D. The Police Act 28

E. The Competition Act 28

F. The General Administrative Law Act 28

G. The Code of Criminal Procedure 29

H. The Decree on the retention and destruction of non-attached documents 30

I. The Civil Code 31

J. The Code of Civil Procedure 31

II. EUROPEAN UNION LAW 32

A. The ePrivacy Directive 32

B. The EIO Directive 32

C. Relevant case-law of the Court of Justice of the European Union (CJEU) 33

III. COMPARATIVE LAW MATERIAL 34

THE LAW 36

I. JOINDER OF THE APPLICATIONS 36

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION 36

A. The Chamber judgments 37

B. The parties' submissions 39

1. The applicant companies 39

(a) The legal basis for the interference and the "foreseeability" of the domestic law 39

(b) Safeguards against arbitrariness and abuse 40

(c) Legitimate aim and proportionality of the interference 42

2. The Government 43

(a) Existence of an interference 43

(b) The legal basis for the interference and the "foreseeability" of the domestic law 43

(c) Safeguards against arbitrariness and abuse 44
(d) Legitimate aim and proportionality of the interference 47
3. The third party 49
C. The Court's assessment 50
1. Existence of an interference and its scope 50
2. Justification for the interference 52
(a) Applicable general principles 52
(i) Lawfulness and necessity in a democratic society 52
(ii) The level of protection for legal persons and the margin of appreciation 55
(b) Application to the present case 56
(i) Preliminary considerations 56
(ii) Whether the interference was in accordance with the law 57
(α) Whether there was a legal basis in Dutch law 57
(β) Quality of the law 58
(iii) Whether the interference pursued a legitimate aim 61
(iv) Whether the interference was "necessary in a democratic society" 61
III. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION 67

OPERATIVE PROVISIONS 67

JOINT PARTLY DISSENTING, PARTLY CONCURRING OPINION OF JUDGES GUYOMAR AND RAVARANI 69

JOINT PARTLY DISSENTING OPINION OF JUDGES BOŠNJAK AND DERENČINOVIĆ 74

DISSENTING OPINION OF JUDGE SERGHIDES 77

JOINT DISSENTING OPINION OF JUDGES SERGHIDES AND ARNARDÓTTIR 90

DISSENTING OPINION OF JUDGE ARNARDÓTTIR, JOINED BY JUDGES SERGHIDES AND ŠIMÁČKOVÁ 91

APPENDIX 98

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

The European Court of Human Rights, sitting as a Grand Chamber composed of:

Marko Bošnjak,
Arnfinn Bårdsen,
Lado Chanturia,
Mattias Guyomar,
Georges Ravarani,
Carlo Ranzoni,
Georgios A. Serghides,
Tim Eicke,
Lətif Hüseynov,
Jovan Ilievski,
Jolien Schukking,
Raffaele Sabato,
Saadet Yüksel,
Lorraine Schembri Orland,
Kateřina Šimáčková,
Davor Derenčinović,
Oddný Mjöll Arnardóttir, *judges*,

and Johan Callewaert, *Deputy Grand Chamber Registrar*,

Having deliberated in private on 6 March 2024 and 15 January 2025,

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

PROCEDURE

1. The case originated in 4 applications (nos. 2799/16, 2800/16, 3124/16 and 3205/16) 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 six limited liability companies incorporated under Dutch law, whose details are listed in the appended table ("the applicant companies"), on 7 January 2016.

2. The applicant companies were represented by Ms M.C. van Heezik, a lawyer practising in Brussels, and Mr H.A. Bravenboer and Mr M. Bol, lawyers practising in Rotterdam. The Dutch Government ("the Government") were represented by their Agent, Ms B. Koopman, of the Ministry of Foreign Affairs.

3. The applicant companies complained that the transmission of intercept data lawfully obtained in a criminal investigation to competition authorities had constituted a violation of their rights under Article 8 of the Convention and that they had not had access to an effective domestic remedy in respect of that complaint, as required by Articles 8 and 13 of the Convention.

4. On 13 and 14 December 2018 the Government were given notice of the applications.

5. The applications were allocated to the Third Section of the Court, pursuant to Rule 52 § 1 of the Rules of Court. On 16 May 2023 a Chamber of that Section, composed of Pere Pastor Vilanova, Yonko Grozev, Jolien Schukking, Darian Pavli, Peeter Roosma, Ioannis Ktistakis and Andreas Zünd, judges, and Milan Blaško, Section Registrar, delivered three judgments in which it declared, unanimously, the applications admissible. It further held, by four votes to three, that there had been no violation of Article 8 of the Convention and, unanimously, that there had been no violation of Article 13 of the Convention in conjunction with Article 8. A joint dissenting opinion of Judges Grozev, Pavli and Ktistakis was appended to each of the judgments.

6. On 3 July and 9 and 10 August 2023 the applicant companies requested the referral of the case to the Grand Chamber in accordance with Article 43 of the Convention. On 25 September 2023 a panel of the Grand Chamber accepted the request.

7. The composition of the Grand Chamber was determined in accordance with the provisions of Article 26 §§ 4 and 5 of the Convention and Rule 24.

8. The applicant companies and the Government each filed observations on the merits of the case (Rule 59 § 1). In addition, third-party comments were received from the Government of the United Kingdom, who had been given leave by the President of the Grand Chamber to intervene in the written procedure (Article 36 § 2 of the Convention and Rules 71 § 1 and 44 § 3).

9. A hearing took place in public in the Human Rights Building, Strasbourg, on 6 March 2024.

There appeared before the Court:

(a) *for the Government*
Ms B. KOOPMAN, *Agent*,
Ms C. COERT, *Counsel*,
Ms E. ZIJLSTRA, *Adviser*;

(b) *for the applicant companies*
Ms M.C. VAN HEEZIK,
Mr H.A. BRAVENBOER,
Mr M. BOL, *Counsel*,
Ms C. CASTELEIN, *Adviser*.

The Court heard addresses by Ms van Heezik, Mr Bravenboer and Ms Koopman, as well as their replies to questions put by judges.

INTRODUCTION

10. The case concerns the transmission of intercept data lawfully obtained in a criminal investigation to another law-enforcement authority. The applicant companies complained that the transmission of the data to, and their use by, competition authorities had been neither "in accordance with the law" nor necessary in a democratic society on account, in particular, of the insufficiency of the procedural safeguards.

THE FACTS

THE CIRCUMSTANCES OF THE CASE

A. Ships Waste Oil Collector B.V., Burando Holding B.V. and Port Invest B.V. v. the Netherlands (nos. 2799/16, 3124/16 and 3205/16 – "the first group of applicant companies")

11. The first group of applicant companies are limited liability companies incorporated under Dutch law, engaged in the collection of waste liquids from ships in the Rotterdam port region. At the relevant time Burando Holding B.V. was the sole shareholder and a board member of Port Invest B.V., which was in turn the sole shareholder and a board member of the I. company.

1. Criminal proceedings and data transmission

12. 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* – "the VROM-IOD"), a special investigative service within the meaning of the Special Investigative Service Act (*Wet op de bijzondere opsporingsdiensten*; see paragraph 74 below) that operates under the authority of the public prosecutor (*officier van justitie*), began an investigation, under the codename "Toto", into the I. company. That company was suspected of the criminal offence of forgery of documents (Article 225 of the Criminal Code (*Wetboek van Strafrecht*)), and of involvement in the disposal of polluted waste, in contravention of environmental protection legislation (section 18.18 of the Environmental Management Act (*Wet Milieubeheer*)), amounting to a criminal offence.

13. 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. These included conversations between the employees of the I. company and of the Ships Waste Oil Collector B.V. company.

14. 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 that price-fixing was taking place. An official record (*proces-verbaal*) dated 21 April 2008 was drawn up by an official of the VROM-IOD, in which the evidence relating to the price-fixing was detailed and to which summary transcripts of some of the conversations were appended.

15. On 21 October 2008 the public prosecutor in charge of the investigation gave permission in accordance with section 39f of the Judicial and Criminal Data Act (*Wet Justitiële en Strafvorderlijke gegevens* – "the WJSG"; see paragraph 61 below) for the official record of 21 April 2008 and the appended transcripts to be transmitted to the NMA by writing "transmission to the NMA approved" on the document and dating and signing it by hand. They were transmitted to the NMA on 29 June 2009.

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

17. On 23 October 2009 the public prosecutor authorised the transmission of a further selection of transcripts and audio-recordings of telephone conversations intercepted in the "Toto" criminal investigation. In the authorisation for that transmission, the public prosecutor's approval was stated in the following terms, followed by his signature: "I have no objection to providing the above-described data requested by the NMA."

18. On 29 and 30 June 2010 the NMA inspectors visited the premises of the Ships Waste Oil Collector B.V. company and the I. company. They questioned members of the companies' management under caution, in the course of which they played back a sound-recording of an intercepted telephone conversation.

19. Meanwhile, the NMA provided the VROM-IOD with a list of search terms to examine the entire criminal file for relevant material. The transcripts of the telephone conversations found as a result of that search were transmitted to the NMA on several dates in 2010. The transmission authorisations of 30 June, 6 July and an unspecified date in August 2010 contained the mention "For approval", followed by the prosecutor's signature. The most recent transmission of data, approved by the prosecutor in August 2010, took place on 8 or 9 September 2010.

20. It further appears from the information in the case file that as a result of the "Toto" criminal investigation, the I. company and one of its employees were summoned to appear before the Rotterdam Regional Court (*Rechtbank*) on 19 December 2008 on suspicion of having committed, on several occasions, acts in breach of Article 225 of the Criminal Code and section 18.18 of the Environmental Management Act. On 11 March 2010 an agreement to settle the criminal case was reached between the I. company and the public prosecutor. On the same day a similar agreement to settle the criminal case was also reached between the I. company's employee and the

public prosecutor. The I. company was to pay 50,000 euros (EUR) to avoid further criminal proceedings related to the charges against it, while its employee was to pay EUR 4,000 for the same reason. The Regional Court, having heard the parties on 5 July 2010, gave judgment on that same date. Having established that a settlement had been reached, the Regional Court declared the Public Prosecution Service's case inadmissible (*het openbaar ministerie werd niet-ontvankelijk verklaard*), as had been requested by the prosecutor.

2. Administrative proceedings

(a) The decision by the NMA to impose fines and the administrative review proceedings

21. Based on the results of its investigation, the NMA concluded in a report of 28 December 2010 that during the period between 30 August 2005 and 31 July 2007 several companies, including the Ships Waste Oil Collector B.V. company and the I. company, had colluded with each other to allocate contracts and prevent or limit price competition in the field of ship-generated waste collection. The NMA held in its draft decisions that, in so doing, those companies had violated section 6 of the Competition Act (see paragraph 77 below). The report quoted extensively from the transcripts of the telephone conversations.

22. Following the submission of written comments (*zienswijze*) by counsel for the first group of applicant companies and a hearing held on 15 April 2011, the NMA gave its decisions on 16 November 2011. It found that the transcripts and recordings had been lawfully transmitted to it by decision of the public prosecutor. In terms of Article 8 of the Convention, the transmissions had been "in accordance with the law" in that they had had a statutory basis, had been foreseeable and had met a "pressing social need", namely, the enforcement of competition law. There was no suggestion that the interceptions themselves had been unlawful, or that the competing interests had been incorrectly weighed up by the public prosecutor. The NMA further found the companies liable for infringements of section 6(1) of the Competition Act. It imposed a fine on the Ships Waste Oil Collector B.V. company in the amount of EUR 834,000. It also imposed a fine in the amount of EUR 1,861,000 on the three companies jointly and severally: the I. company and Port Invest B.V. were liable for the entire amount, and Burando Holding B.V. was liable for the maximum amount of EUR 621,000. Because of their interconnectedness (see paragraph 11 above), the NMA assumed that Port Invest B.V. and Burando Holding B.V. had exercised decisive influence over the I. company's actions.

23. The first group of applicant companies lodged a written objection (*bezwaarschrift*) with the NMA arguing, *inter alia*, that the intercepted telephone conversations should not have been admitted as evidence because

they did not qualify as "criminal data" that could be transmitted on the basis of the WJSG (see paragraph 61 below), as the information had been irrelevant for the criminal investigation. They also protested about the lack of prior judicial review of the transmission of the data to the NMA. The Ships Waste Oil Collector B.V. company further submitted that it had never itself been suspected of any criminal offence. Moreover, as the criminal case had been settled by the I. company, no *ex post facto* judicial review of the lawfulness of the telephone tapping had taken place in the criminal proceedings. Also, intercept material could not be admitted in evidence because the NMA had no power to intercept communications. The NMA's use of intercept material in administrative proceedings amounted to a way of bypassing the legal requirements that restricted the power to intercept. Lastly, they submitted that there had been no legal basis for the contact between the NMA and the VROM-IOD prior to the official transmission of the criminal data.

24. The first group of applicant companies 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.

(b) Appeal proceedings before the Rotterdam Regional Court

25. The NMA submitted a defence statement (*verweerschrift*), explaining how the transmissions had been carried out and describing the contact it had had with the VROM-IOD in that connection (see paragraphs 13-19 above). The NMA had received the transcripts after the criminal investigation had been completed. It argued that the transmissions had complied with the requirements of the WJSG. In particular, the transmitted material had been part of the criminal file; it had therefore been criminal data within the meaning of the WJSG (see paragraph 61 below). The interference with the first group of applicant companies' rights under Article 8 of the Convention had been necessary and proportionate. The transmissions had concerned business-related telephone conversations that had taken place during the performance of their employees' duties. They had the possibility of fully contesting the authenticity and reliability of the evidence in the ongoing administrative proceedings. Furthermore, the companies should have used the civil remedy for retrospective and independent review by a civil court of the Public Prosecution Service's decision, which was classified as a "factual act" (*feitelijke gedraging*) in the domestic law.

26. 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 (see paragraph 53 below), it reiterated that the intercepted telephone data did qualify as "criminal data" within the meaning of the WJSG. Furthermore, it found no record of any weighing of interests to review, since the public prosecutor had merely given handwritten permission for the transmission of the official record of 21 April 2008 (see paragraphs 15 and 17 above) and, for the subsequent transmissions,

on pre-printed forms without any reasoning (see paragraph 19 above). It followed from that that the transcripts had to be excluded as evidence. Since the NMA's investigation and their decisions had mainly relied on this evidence, the Regional Court quashed the NMA's decisions.

(c) Further appeal proceedings before the Supreme Administrative Court for Trade and Industry

27. The Consumer and Market Authority (*Autoriteit Consument en Markt* – "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*). It argued that the transmission of criminal data by the Public Prosecution Service to another entity would only be incompatible with domestic law or Article 8 of the Convention if it could not be considered necessary in view of a compelling general interest or if it did not comply with the requirements of proportionality and subsidiarity. Under the WJSG, that assessment fell to the Public Prosecution Service and, subsequently, the civil courts in the form of an *ex post facto* judicial review. The transmission of criminal data to a third party 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* – "the AWB"), and therefore not amenable to judicial review by the administrative courts. Such a transmission by a public prosecutor required neither reasoning nor an *ex ante* review of its lawfulness. According to the ACM, the use in evidence of the criminal data received had been admissible as there were no indications that the data had been obtained unlawfully or, even if that were the case, that "the manner of that obtainment ran counter to the proper behaviour expected of authorities to such an extent that its use could not be considered permissible under any circumstances".

28. As regards the transmission of the data, the ACM noted that it could be considered necessary for an important public interest: the economic well-being of the Netherlands. The data concerned possible price fixing which was among the most serious breaches of the prohibition on cartels. Moreover, between them, the first group of applicant companies had an 85-90% market share, so the potential damage was significant. The transmitted transcripts concerned strictly business-related conversations; only conversations that could be relevant to the ACM's investigation into a possible breach of the Competition Act had been included. The prior contact between VROM-IOD and ACM officials had been precisely aimed at ensuring the proportionality of the transmissions. As a specialised authority, the ACM could better assess which data could be relevant for ascertaining the existence of a competition-law violation and its seriousness. It was unlikely that the information regarding possible agreements on prices could have been obtained by the ACM in a less intrusive manner as the price-fixing agreements had not been documented in writing. The compelling public

interest in transmitting the data had therefore outweighed the interest in protecting the rights of the first group of applicant companies or their employees. Lastly, the ACM could lawfully receive intercept material, as the WJSG did not require recipients to have the power themselves to intercept communications. The ACM's further appeal was joined by the Board of Prosecutors-General.

29. The first group of applicant companies lodged a cross-appeal (*incidenteel hoger beroep*) on the grounds that the Regional Court should have found that, because the recordings of the intercepted telephone conversations were not included in any criminal file, they were therefore not "criminal data" that could be transmitted to another entity in accordance with section 39f(1) of the WJSG. Referring to Article 126cc of the Code of Criminal Procedure (see paragraph 82 below), the I. company, Port Invest B.V. and Burando Holding B.V. further argued that some of the data transmissions had been unlawful because they had taken place more than two months after the settlement agreement had been reached between the I. company and the public prosecutor, which, according to the first group of applicant companies, had marked the end of the criminal proceedings.

30. On 14 April 2014 the Supreme Administrative Court for Trade and Industry issued a decision (ECLI:NL:CBB:2014:151) in which it rejected the appeal of the Board of Prosecutors-General as inadmissible. It held that the interests entrusted to the Board of Prosecutors-General were not directly affected by the penalty decisions which were the subject of the judgment of the Regional Court being challenged, and concluded that the Board of Prosecutors-General had no legal interest of its own and hence no standing to bring proceedings.

31. 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 first group of applicant companies' 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 72 below]), in which it was considered, among other points, that a criminal file could relate to acts other than those for which the Public Prosecution Service had instituted a prosecution. The Supreme

Administrative Court for Trade and Industry cannot agree with the assertion ... that the telephone tap data (*tapgegevens*) have no relevance for the prosecution and qualify as by-catch, and therefore do not belong in the criminal file. Furthermore, as the ACM has stated, in this case it could not be ruled out that the telephone tap data would be relevant at some stage of the criminal proceedings ...

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 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 Convention], 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 collusion between companies. In view of the nature of the ban on cartels in section 6 of the Competition Act, the [Supreme Administrative Court of Trade and Industry] is of the opinion that in this case there exists a compelling general interest, namely the economic well-being of the country. In this regard, reference is also made to the judgment of 2 October 2014 [by the European Court of Human Rights] 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 for the purpose of the enforcement of legislation by the ACM.

4.4 With respect to the question 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 data relating to criminal records are transmitted.

However, the Supreme Administrative Court for Trade and Industry does not agree with 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 identifiable and can be assessed by the court – made at the time of the transmission and apparent at that time. The availability of written reasoning by 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 the legislative history suggests that the unavailability of written reasoning at the time of a 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 [Convention]. Under the second

paragraph of Article 8 of the [Convention], 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 has its statutory basis in the WJSG. Moreover, as to the lawfulness of this transmission, the law provides for judicial review procedures with sufficient safeguards, 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 those 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 reasonably 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 [see paragraph 46 below]), 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 transmission.

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 39f of the WJSG violates Article 8 of the [Convention] or any other treaty provision. ...

4.8 ... The circumstance that the ACM itself does not have the competence to intercept telephone conversations does not constitute a ground for 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 – , having [taken cognisance of transcripts and recordings of intercepted telephone conversations], made a selection from the large amount of data 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 in breach of the WJSG ...

4.10 The I. company, Port Invest B.V. and Burando Holding B.V. have also argued that the transmissions of 30 June, 7 July and 2 September 2010 were unlawful because the criminal case against them had ended with the conclusion of a settlement on 11 March 2010. The Supreme Administrative Court for Trade and Industry agrees with the ACM that the criminal case did not end until the court ruling of 5 July 2010 became

final, therefore on 19 July 2010. In view of the two-month period referred to in Article 126cc, paragraph 2, of the Dutch Code of Criminal Procedure [see paragraph 82 below], at the time of all the transmissions there did not yet exist a situation in which the data provided should have been destroyed."

3. Subsequent developments

32. On 20 October 2016 the Regional Court of Rotterdam found it proven that from 1 January 2006 to 31 July 2007 the first group of applicant companies had engaged in anti-competitive practices ("price-fixing") in violation of section 6 of the Competition Act. It reduced, however, the amount of the fines imposed, finding that the ACM had erroneously held that those practices had begun in 2005.

33. The first group of applicant companies and the ACM appealed against the judgment of the Regional Court of Rotterdam to the Supreme Administrative Court for Trade and Industry. On 30 October 2018 the Supreme Administrative Court for Trade and Industry quashed the Regional Court's judgment with regard to the amount of the fines and upheld the remainder of it. It held that the ACM had correctly established that the anti-competitive practices had begun on 30 August 2005. It therefore upheld the fines originally imposed by the ACM (see paragraph 22 above).

B. Janssen de Jong Groep B.V. and Others v. the Netherlands (no. 2800/16)

34. The application concerned 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. ("the Janssen companies").

1. Criminal proceedings and data transmission

35. Around 2007 suspicions arose that local government officials had been bribed by building contractors seeking to win 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 identified the Janssen companies as suspects.

36. In the context of this investigation, some of the telephone conversations of the Janssen companies' employees were intercepted. The interception orders were authorised by an investigating judge. The interception of telephone and internet communications was authorised under Article 126m of the Code of Criminal Procedure (see paragraph 81 below) on the basis of the suspicion that the criminal offences of bribery of an official, fraud and forgery of documents were being committed.

37. Certain intercepted telephone conversations were identified as being of potential interest to 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*) containing transcripts of the intercepted communications. Upon a request by the NMA, the police subsequently also gave it access to other written reports containing transcripts of telephone conversations of the same 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.

38. On 19 August 2008 the public prosecutor in charge of the investigation provided a CD to the NMA containing selected audio-recordings of about thirty 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.

39. On 9 December 2008 the NMA started an official investigation into possible violations of the Competition Act and requested the Public Prosecution Service's permission to use the data.

40. On 16 December 2008 the relevant 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."

41. On 22 December 2008 the NMA provided the police with a list of search terms to use to examine the criminal file for relevant material. The transcripts of telephone conversations found as a result of that search were transmitted to the NMA on 24 December 2008.

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

43. On 28 May 2009 the public prosecutor in charge of the investigation wrote to inform the Janssen companies' counsel at the time that information obtained in the course of the "Cleveland" investigation had been transmitted to the NMA in accordance with the WJSG (see paragraph 61 below) and the WJSG Instructions (see paragraphs 69-70 below).

44. On 1 November 2010 the public prosecutor decided not to pursue criminal charges (*voorwaardelijk sepot*) against Janssen de Jong Infra B.V., on condition that the company adhered to certain conditions throughout a probationary period set by the prosecutor. Subsequently three employees of the Janssen companies and six public officials were convicted of bribery. The latest judgments in the proceedings were issued on 19 May 2015.

2. Civil proceedings

45. The Janssen companies brought proceedings against the State – specifically, the Ministry of Justice (*Ministerie van Justitie*), as the party responsible in civil proceedings for the Board of Procurators-General and the Public Prosecution Service, and the Ministry for Economic Affairs (*Ministerie van Economische Zaken*), as the party responsible in civil proceedings for the NMA – 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 a provisional order prohibiting the Public Prosecution Service from transmitting data. They relied, *inter alia*, on Article 8 of the Convention. The Janssen companies submitted, in particular, that transmitting intercept data to the NMA had not been "in accordance with the law". They argued, first, that the wording of section 39f(1) of the WJSG was insufficiently precise for such transmission to be "foreseeable"; secondly, that the interception had been authorised in the context of investigating a criminal case rather than for the purpose of enforcing competition law; and, thirdly, that the NMA had no power under the domestic law to intercept communications.

46. In a judgment of 26 June 2009, the provisional-measures judge dismissed the Janssen companies' requests (ECLI:NL:RBSGR:2009:BJ0047). His reasoning included the following:

> "4.2. ... The crux of the dispute is whether the State [the Board of Prosecutors-General and the Public Prosecution Service] lawfully transmitted the intercepted telephone conversations to the NMA. To answer this question, it must first be assessed whether the WJSG is applicable ...
>
> 4.3. [The plaintiffs] argue in this regard that a distinction should be made between information ... that is relevant to the criminal investigation and by-catch information relating to potential price-fixing agreements. [The plaintiffs] contend that, unlike criminal data with criminal relevance, by-catch data are not included in the criminal file. According to [the plaintiffs], by-catch data do not qualify as criminal data within the meaning of section 1(b) of the WJSG since they are data obtained in the course of a criminal investigation but not included in a criminal file or processed by automated means.
>
> 4.4. Thus, the question arises whether the parts of the intercepted telephone conversations concerning potential price-fixing agreements were part of the criminal file. Provisionally, this question should be answered in the affirmative since the transcripts of intercepted telephone conversations as a whole are part of the criminal file. The Explanatory Memorandum ... states that the term 'case documents' is broadly interpreted in practice, and that the criminal file includes all documents that could reasonably be relevant for addressing the questions outlined in Articles 348 and 350 of the Code of Criminal Procedure [on whether a criminal offence has been committed and whether the suspect is liable for that offence] ... It cannot be ruled out that the transcripts of intercepted telephone conversations in their entirety may be relevant at some stage of the criminal proceedings to answer the questions set out in Articles 348 and 350 of the Code of Criminal Procedure. Parts of the transcripts concerning possible

price-fixing agreements might be so intertwined with parts of the transcripts related to the criminal investigation that it must be assumed that all the transcripts of the intercepted telephone conversations were part of the criminal file.

4.5. It follows from the foregoing that the transcripts of the intercepted telephone conversations, including those concerning possible price-fixing agreements, were part of the criminal file and should be considered criminal data within the meaning of section 1(b) of the WJSG. Consequently, the transmission of criminal data to the NMA falls within the scope of the WJSG.

4.6. The provisional-measures judge would now turn to the question whether the Public Prosecution Service complied with the conditions set out in the WJSG for transmitting the intercepted telephone conversations to the NMA. Section 39f of the WJSG provides a legal basis for the transmission of criminal data ... to third parties for non-criminal justice purposes. Under section 39f of the WJSG, transmission [of criminal data] to a third party is only justified if it is necessary in view of a compelling general interest. In the present case, it must be assessed whether the enforcement of section 6(1) of the Competition Act by the NMA constituted a compelling general interest within the meaning of section 39f(1) of the WJSG.

4.7. In this context, [the plaintiffs] argue that the interest of the NMA in the administrative enforcement of national competition law cannot be qualified as a compelling general interest within the meaning of section 39f(1) of the WJSG ... Since the NMA is tasked with, *inter alia*, the enforcement of the Competition Act, in particular with the oversight and investigation of cartel formation, prohibited price--fixing agreements, and other forms of collusion in public procurement, the provisional-measures judge provisionally finds, given the nature of section 6(1) of the Competition Act ..., that there was a compelling general interest at stake, namely the economic well-being of the Netherlands ... The foregoing leads to the conclusion that the State [the Board of Prosecutors-General and the Public Prosecution Service] lawfully transmitted the intercept data to the NMA in accordance with section 39f(1) of the WJSG.

4.8. [The plaintiffs] also argue that the transmission of the transcripts of the intercepted telephone conversations to the NMA violated Article 8 of the European Convention on Human Rights ...

4.9. [I]t is at present sufficiently established that ... the transmission of the intercepted telephone conversations to the NMA with a view to it carrying out further investigation and with a view to the enforcement of section 6(1) of the Competition Act, was necessary for the [protection of the] economic well-being of the Netherlands. This interest carries more weight than the interest of protecting the privacy of [the plaintiffs]. True, [the plaintiffs] have disputed whether the interference with their rights resulting from the transmission of the intercept material to the NMA was 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 intrusive way, given that such agreements tend as a rule not to be committed to paper. It follows from the above that the transmission of the intercept material by the Public Prosecution Service based on section 39f(1) of the WJSG was not incompatible with Article 8 of the Convention.

4.10. The conclusion of the foregoing is that, within the limited scope of these provisional-measures proceedings, it cannot be concluded with the required degree of probability that the transmission of the intercept material by the Board of

> Prosecutors-General and the Public Prosecution Service to the NMA constituted unlawful conduct towards [the plaintiffs]. Nor has the alleged violation of Article 8 of the [Convention] been sufficiently substantiated by [the plaintiffs]. This leads to the conclusion that the requests must be dismissed."

47. The Janssen companies did not appeal against this judgment.

3. Administrative proceedings

(a) The decision by the NMA to impose fines and the administrative review proceedings

48. In two reports of 17 December 2009 and 25 February 2010, the NMA found that the Janssen companies were responsible for an infringement of section 6(1) of the Competition Act. Those reports quoted extensively from the transcripts of the intercepted telephone conversations. The Janssen companies' counsel submitted written comments (*zienswijze*). As a preliminary issue, it was argued that the transmission, by the Public Prosecution Service to the NMA, of telephone conversations intercepted in the framework of the criminal investigation into corruption constituted a violation of Article 8 of the Convention. A hearing took place before the NMA on 21 June 2010 in which the Janssen companies and the other companies allegedly involved in the price-fixing were represented.

49. The NMA gave its decision on 29 October 2010. In response to the arguments raised by the Janssen companies' counsel, it contained reasoning similar to that set out in paragraph 22 above. Based on the results of its investigation, the NMA concluded that during the period from March to December 2008, one of the Janssen companies had colluded on bidding figures with other companies and exchanged information about their intended bidding behaviour prior to bidding on a number of tenders. In so doing, those companies had violated section 6 of the Competition Act. On 29 October 2010 the NMA imposed a fine on the Janssen companies jointly and severally in the amount of EUR 3,000,000.

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

(b) Appeal proceedings before the Rotterdam Regional Court

51. The Janssen companies subsequently lodged an appeal (*beroep*) with the Rotterdam Regional Court. They submitted that the transmission of the intercept material had been unlawful, arguing that the WJSG was not applicable because the transmitted data did not qualify as "criminal data". In that respect they argued that the recordings of the intercepted telephone conversations had not been included in the criminal file and that that information had been irrelevant for the criminal investigation. Furthermore, they argued, relying on Articles 8 and 13 of the Convention and on the Court's case-law, that the transmission of data obtained during the criminal

investigation to the NMA had not been "foreseeable" as it had no clear basis in domestic law, and complained about the lack of prior judicial review. They contended that the power to authorise the transmission of criminal data should be accorded to an independent tribunal rather than a prosecutor. The interception authorisation, granted by an investigating judge for the specific purpose of investigating a serious crime under ordinary criminal law, could not cover transmission of the intercept material to the NMA. In view of the above, the intercept material should not have been admitted in evidence. In any case, there had been no price-fixing.

52. The NMA submitted a defence statement. It explained how the transmissions had been carried out and described the contact it had had with the police and the prosecutor in that connection (see paragraphs 37-41 above). It argued, among other points, that the domestic law did not prohibit prior consultations in order to assess whether certain information might be relevant for the enforcement of the Competition Act. Once its relevance had been established, a formal transmission authorisation had been issued. It further submitted that the data had been "criminal data" within the meaning of the WJSG. The Janssen companies' argument that the intercept material had been by-catch data and, as such, could not be included in a criminal file, found no support in domestic law. The fact that the NMA did not itself have the competence to intercept telephone conversations had not rendered the transmission unlawful either, as none of the recipients mentioned in the WJSG Instructions had such competence. The NMA further argued that cartels and cartel-like collaborations were detrimental to the performance capacity of the country, and that dynamic and responsive markets were essential for an internationally interconnected market economy like the Dutch one. Therefore, enforcement of competition rules constituted a compelling general interest within the meaning of section 39f of the WJSG. Furthermore, the provisional-measures judge, in his ruling of 16 January 2008 (see paragraph 46 above), had also found that there had been a compelling general interest, namely the economic well-being of the country. It had been evident from the intercepted telephone conversations that the Janssen companies had participated in illegal bidding agreements in a structured and frequent manner. The NMA also stressed that the transmitted material represented approximately 2 to 3% of all the conversations that had been intercepted in the context of the "Cleveland" investigation. Lastly, it submitted that it was precisely the intention of the legislature to enable transmissions to authorities, like the NMA, involved in non-criminal enforcement of legislation.

53. The Regional Court gave judgment on 13 June 2013 (ECLI:NL:RBROT:2013:CA3079), declaring the Janssen companies' appeal well founded. Referring to the Explanatory Memorandum (see paragraph 63 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 transmission of data in issue. However, since the case

file did not contain an identifiable, reviewable weighing of interests by the public prosecutor, the Regional Court was of the view that the NMA had not been entitled in that case to use the intercepted telephone conversations as evidence. It considered that the NMA should, before making use of that information, have satisfied itself that the public prosecutor had established the existence of a compelling general interest and assessed whether the transmissions had been necessary for that purpose. Otherwise, the requirements of Article 8 of the Convention would not be adequately addressed, despite section 39f of the WJSG being specifically designed to ensure compliance with those requirements. Since, apart from the transmitted data, the NMA had not put forward sufficient alternative evidence, the Regional Court quashed the NMA's decision.

(c) Further appeal proceedings before the Supreme Administrative Court for Trade and Industry

54. The ACM lodged a further appeal (*hoger beroep*) with the Supreme Administrative Court for Trade and Industry. It advanced the same arguments as outlined in paragraph 27 above. The ACM's further appeal was joined by the Board of Prosecutors-General.

55. The Janssen companies lodged a cross-appeal on the grounds that the Regional Court should have found that, because the recordings of the intercepted telephone conversations were not included in any criminal file, they were therefore not "criminal data" that could be transmitted to another entity in accordance with section 39f(1) of the WJSG.

56. On 14 April 2014, the Supreme Administrative Court for Trade and Industry issued a decision (ECLI:NL:CBB:2014:151) rejecting the appeal of the Board of Prosecutors-General as inadmissible (see paragraph 30 above).

57. 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 Janssen companies' cross-appeal and referred the case back to the Regional Court. The judgment contained almost verbatim the same reasoning as that cited in paragraph 31 above. On the issue of the exploratory interactions between the Public Prosecution Service and the ACM, it held as follows:

> "Contrary to the argument made by [the Janssen companies], the circumstance that the ACM had access to the large amount of data 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 in breach of the WJSG."

4. Subsequent developments

58. On 23 June 2016 the Regional Court of Rotterdam found that the Janssen companies had colluded on bidding figures with other companies and exchanged information about their intended bidding behaviour prior to

bidding on public tenders. Their actions amounted to a violation of section 6(1) of the Competition Act. It carried out an assessment of the proportionality of the fine and reduced it to EUR 2,500,000.

59. The Janssen companies appealed against the judgment of the Regional Court of Rotterdam to the Supreme Administrative Court for Trade and Industry. On 8 May 2018 that court quashed the Regional Court's judgment in so far as it related to the amount of the fine and upheld the remainder of the judgment. It further reduced the fine to EUR 463,000, finding that the fine imposed by the Regional Court had been disproportionate to the violations found.

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. DOMESTIC LAW AND PRACTICE

A. Constitution of the Kingdom of the Netherlands

60. Article 93 of the Constitution provides that the Convention forms part of domestic law. Under Article 94 of the Constitution, the provisions of the Convention take precedence over domestic statutory rules in the event of a conflict.

B. The Judicial and Criminal Data Act

1. Relevant provisions

61. The relevant parts of the Judicial and Criminal Data Act (*Wet Justitiële en Strafvorderlijke gegevens* – "the WJSG") provided as follows at the material time:

Section 1

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

...

(b) criminal data (*strafvorderlijke gegevens*): personal data or data concerning a legal person obtained in the context of a criminal investigation and processed by the public prosecutor in a criminal file (*strafdossier*) or by automated means;

..."

Section 39b(1)

"The Board of Prosecutors-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 39c(2)

"The Board of Prosecutors-General may only process criminal data if it is appropriate, relevant, and not excessive, considering the purposes for which the data are being processed."

Section 39f

"(1) The Board of Prosecutors-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:

(a) preventing and identifying criminal offences;

(b) maintaining order and safety;

(c) the enforcement of legislation;

(d) making decisions under administrative law;

(e) evaluating the necessity of taking a measure related to legal status or disciplinary action;

(f) providing assistance to victims and others affected by criminal offences; or

(g) the carrying out of a private-law legal act by a person or entity assigned a public task.

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

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

(b) provided in a manner that reasonably prevents the identification of persons other than the individual concerned.

..."

Section 39j(1)

"Every transmission of criminal procedural data in accordance with sections 39e and 39f shall be recorded and the record retained for at least one year."

2. Legislative history

62. 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.

63. 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):

"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 (*processtukken*) and processed in a criminal file (*strafdossier*), [the Public Prosecution Service's automated case management system] or the higher appeal systems. The Code of Criminal Procedure does not contain a

definition of the term ‘case documents’. In practice, the concept is broadly interpreted. ... The criminal file comprises all documents that could reasonably be relevant for addressing the questions outlined in Articles 348 and 350 of the Code of Criminal Procedure [on whether a criminal offence has been committed and whether the suspect is liable for that offence] ...

The proposed sections 39e and 39f require the transmission of criminal data to third parties to be ‘necessary in view of a compelling general interest’. ... This requirement draws inspiration from the principles stated in [the Dutch Personal Data Protection Act] ... This requirement is justified by the potential threat posed by sensitive data, such as criminal data, to the data subject’s privacy. The intention is to restrict the sharing of such data.

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. ...

... A public prosecutor is deemed to be well-placed for weighing up the interests of the suspect against the compelling general interest. Based on this assessment, the prosecutor determines whether it is necessary for the Public Prosecution Service to transmit criminal data to a third party and, if so, which third party has a legitimate interest ...

Section 39f further defines the purposes for which the Public Prosecution Service can transmit criminal data to third parties not directly involved in the criminal justice system. Those purposes provide a specific explanation of [what constitutes] ‘necessity in view of a compelling general interest’ ... They have been defined in such a way and formulated so broadly that all transmissions currently carried out by the Public Prosecution Service for non-criminal justice purposes can be included ...

In practice, the Public Prosecution Service must weigh the compelling general interest against the right to privacy of the person affected by the criminal investigation. When weighing these interests, the Public Prosecution Service must also consider the necessity of the transmission, which it must be able to demonstrate, and take into account the principles of proportionality and subsidiarity. In addition to weighing these interests, the Public Prosecution Service must ensure that the requested data transmission, as a form of further processing of the requested data, is not incompatible with the aim for which they were included in the criminal file at the time, namely the prosecution of one or more criminal acts. Finally, the recipient of the data must have a legal basis for receiving them. This legal basis is laid down in section 39f(2)(a). It states that transmitted criminal data must be necessary in view of a compelling general interest or the determination, exercise or defence of a right in law. These requirements are derived from [the Personal Data Protection Act].

As stated above, the public prosecutor is deemed to be well-placed for the assessment whether a compelling general interest requires the transmission of criminal data to a third party. For this reason, unlike in section 39e, the choice was made not to include a list of recipients of criminal data in the law ... Instead, it is left to the discretion of the public prosecutor to decide whether the transmission of criminal data to a third party is appropriate. This is in line with the current practice of the Public Prosecution Service”.

64. As regards applicable remedies, the Explanatory Memorandum reads as follows:

"... The decision of the Public Prosecution Service to transmit criminal data concerning the person in question 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 78 below]. The rationale for this lies in the fact that it lacks certain elements required by the definition of the term 'decision', since it does not constitute a legal act. Indeed, it cannot be regarded as an act intended for legal effect. While it may produce a legal effect, that is not its primary purpose. The act is aimed solely at the factual transmission of information relating to criminal data.

Consequently, [the administrative remedies] are not available to the third party seeking data or to the data subject. Furthermore, there is no right for the individual concerned to be heard with respect to an intention by the public prosecutor to disclose their data to a third party.

Establishing the right to be heard for the data-requesting third party and the data subject is deemed unnecessary. The rationale is that a transmission by the prosecutor to a third party aligns with the purpose for which the data were collected by the Public Prosecution Service, and the data subject is aware of the fact that the public prosecutor, with the aim of serving a compelling general interest, may inform a third party about the offences [he, she or it] has committed, either of [his, her or its] own motion or at the request of a third party. However, this does not preclude the possibility that, as part of the weighing-up of interests, the public prosecutor may find it appropriate to afford the person concerned an opportunity to express [his, her or its] views on a proposed transmission. The public prosecutor should evaluate this on a case-by-case basis."

65. The Note on the report (*Nota naar aanleiding van het verslag*) on the WJSG (Lower House of Parliament, parliamentary year 2002-03, 28 886, no. 5, pp. 5 and 16), which contains responses to questions raised by members of parliament, reads as follows:

"Data transmissions are subject to procedural requirements. These are not established in the bill but follow either indirectly from the bill or from principles of good administration. One such requirement is that the Public Prosecution Service is obliged to state the reasons for its decision on a request for information. This stems from the fact that a transmission by the prosecution under the bill is only admissible if it is necessary in view of a compelling general interest and passes the above-mentioned necessity test. This implies a duty for the prosecution to state reasons. In its decision, it must provide insight into the nature of the interests taken into consideration and the standards that played a role in the weighing-up so that this decision can...be reviewed by the courts ... The bill contains no obligation for the Public Prosecution Service to inform the data subject prior to or after the transmission of [his, her or its] data to a third party of that transmission. The reason for this is that a transmission by the Public Prosecution Service to a third party is compatible with the purpose for which the data were collected by the Public Prosecution Service and the data subject knows or ought to have known that the Public Prosecution Service, in view of a compelling public interest, on its own initiative or on a request, may inform a third party about the criminal offences in which [he, she or it] is involved.

...

The members of the Labour Party asked the government to explain once again ... how legal protection is or will be regulated and in which cases objections and appeals can or cannot be lodged, and with which court, by both data subjects and third parties.

> In response to the previous questions from the members of the Labour Party, I have indicated that data subjects and others can bring a civil claim before a civil court against a decision of the Public Prosecution Service to transmit data. ... In that framework, I explained that bringing the processing of criminal data under the WJSG does not mean any changes in legal protection compared to the Personal Data Protection Act. Also, I indicated in that context that, after the entry into force of this Act, no objection and appeal will be available against a decision of the Public Prosecution Service to transmit, under the proposed sections 39e or 39f, criminal data to a third party, and the reasons therefor."

3. WJSG Instructions

66. The Judiciary Organisation Act (*Wet op de Rechterlijke Organisatie*) provides the legal basis for the Board of Prosecutors-General to give instructions (*aanwijzing verstrekking)* to the Public Prosecution Service on the performance of its tasks and the exercise of its powers.

67. The relevant version of the Instructions on the transmission of criminal data for purposes not related to the administration of criminal justice (*Aanwijzing verstrekking strafvorderlijke gegevens voor buiten de strafrechtspleging gelegen doeleinden*, "the WJSG Instructions") was adopted on 6 August 2007 by the Board of Prosecutors-General and published in Official Gazette (*Staatscourant*) no. 19 of 28 January 2008.

68. The WJSG Instructions provided that the Board of Prosecutors-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.

69. The WJSG Instructions contained further principles and instructions, including a flowchart, for the exercise of the power to transmit data. They read, in so far as relevant, as follows:

> "IV. Transmission of information to third parties for purposes not related to the administration of criminal justice.
>
> ...
>
> *2. Principles applicable to the transmission of data*
>
> A number of general principles and assumptions apply to the assessment of any transmission of data to third parties, except for cases where there is a statutory obligation to transmit data ...
>
> *Not an obligation, but a power*
>
> The WJSG does not create an obligation to transmit criminal data to third parties, but confers the power to do so. The limits of that power are set out in [the WJSG] and these Instructions. This means that a requesting person or body who belongs to one of the categories of recipients referred to in these Instructions (chapter IV § 4) can never derive a right to receive data from these Instructions. A balancing exercise will always have to be conducted ...

Not a service

Criminal data can only be transmitted for purposes that fall outside the administration of criminal justice if this is compatible with the performance of the duties of the Public Prosecutor/Advocate-General and in so far as this is necessary in the light of a compelling general interest ... This means that criminal data may not be transmitted solely on the basis of the third party's interest in obtaining it.

More certainty regarding criminal prosecution

As a basic principle, criminal data may only be transmitted after the delivery of a relevant judgment by a criminal court. They may only be transmitted prior to that if urgent reasons for doing so become apparent to the Public Prosecution Service and the criminal case has been examined (in terms of criminal procedure) by the Public Prosecution Service.

Passive/active transmission

It follows from the WJSG that the Public Prosecutor/Advocate-General can transmit information for purposes that fall outside the administration of criminal justice both actively (on their own initiative) and passively (on request).

Whatever form the transmission of criminal data takes, grounds must exist not only for the Public Prosecution Service to transmit the data, but also for the recipient to receive them. The question as to whether grounds exist for the recipient to receive the data is also for the Public Prosecution Service to answer (section 39f(2), introduction, and (a) of the WJSG).

Subsidiarity, necessity and proportionality

In the assessment of whether and, if so, in what form, data can be transmitted, the principles of necessity, proportionality and subsidiarity are closely interrelated. If the recipient's objective can be achieved in a different manner entailing less interference with privacy than the transmission of criminal data by the Public Prosecution Service, the information in question will not be transmitted (subsidiarity criterion). ...

The transmission of data that is not necessary to pursue one of the objectives mentioned in section 39f of the WJSG must be avoided at all times (necessity criterion). ... The starting-point must in any case remain the selection of the information, so that no more is transmitted than is necessary to achieve the purpose of the transmission. Under the WJSG it is for the Public Prosecution Service, and not the recipient, to determine what criminal data the recipient needs.

The form in which data are transmitted is also important. If the manner of transmitting the data unnecessarily or disproportionately interferes with the privacy of a person concerned, the data will not be transmitted in that manner, unless it is possible to provide them in a form that causes no interference or no disproportionate interference, for example by means of anonymisation, by omitting parts, by providing a summary or simply providing a statement regarding the relevant data.

...

4. The recipients

Under section 39f(1) of the WJSG, criminal data may be transmitted to the following persons and bodies, for the purposes mentioned therein.

Categories marked with an <S>, are standard transmissions

...

c. the enforcement of legislation;

For the purposes of the enforcement of legislation, criminal data may be transmitted to:

<S> Administrative bodies (including the Tax Authority, business associations, benefit agencies, grant providers, inspectorates, special investigation services, De Nederlandse Bank, Stichting Autoriteit Financiële Markten, the Pension and Insurance Chamber) ..."

70. As regards applicable remedies, the WJSG Instructions read as follows:

"The decision to transmit criminal data to third parties, as outlined in sections 39e and f of the WJSG, does not qualify as a decision within the meaning of the AWB. Consequently, the affected party cannot raise objections (*bezwaar*) or lodge applications for judicial review (*beroep*) under the AWB [see paragraph 80 below] in respect of such a decision.

There are two forms of legal protection available to the affected party. If the data subject believes that unlawful processing is occurring, [he, she or it] can hold the State liable under Article 6:162 of the Dutch Civil Code for a wrongful act (*onrechtmatige daad*) [see paragraph 87 below] ...

4. Relevant domestic case-law

71. In his advisory opinion to the Supreme Court of 3 February 2012 in the *Trafigura* case (ECLI:NL:PHR:2012:BV3436), 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 AWB]. With regard to the claim made, 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 a court afterwards and independently."

72. In its judgment of 20 April 2012 in the same 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."

5. The Agreement between the Public Prosecution Service and the NMA

73. On 17 February 2003 the Public Prosecution Service and the NMA entered into an agreement (*Convenant Openbaar Ministerie en Nederlandse Mededingingsautoriteit*), which was published in Official Gazette no. 73 of

14 April 2003, p. 8. The primary objective of this agreement was to facilitate the exchange of information, within the bounds of the law, to enhance the effective execution of their respective duties. The agreement did not affect the exchange of data pursuant to other statutory obligations. The agreement specifically defined the information to be exchanged as data and intelligence obtained by either the Public Prosecution Service or the NMA in the execution of their statutory duties, particularly in the context of investigating and detecting potential criminal offences in the construction sector. The exchanged data were to be treated with strict confidentiality and could only be used for the designated purpose. The agreement was set to expire on 31 December 2003.

C. The Special Investigative Services Act

74. At the relevant time the VROM-IOD was listed under the Special Investigative Services Act as one of the special investigation services which, under the authority of the public prosecutor, were charged with the enforcement of criminal law (sections 2 and 3).

D. The Police Act

75. Section 13 of the Police Act, as in force at the material time, provided that, in the context of criminal law enforcement and justice, the police acted under the authority of the public prosecutor, unless another law provided otherwise. The public prosecutor had the power to issue instructions to police officers for carrying out the tasks mentioned above.

E. The Competition Act

76. At the material time, section 5 of the Competition Act provided that the NMA was charged with the enforcement of that Act.

77. Section 6(1) of the Competition Act prohibited agreements between companies, decisions by associations of companies and concerted practices aimed at or with the effect of the prevention, restriction or distortion of competition within the Netherlands market (price-fixing).

F. The General Administrative Law Act

78. Section 1:3 of the General Administrative Law Act (*Algemene wet bestuursrecht* – "the AWB") defines a "decision" as a written decision by an administrative body, constituting a legal act under public law. Section 3:46 of the AWB provides that a decision must be based on proper reasoning.

79. The AWB provides for the following "principles of good administration" (*algemene beginselen van behoorlijk bestuur*):

Section 3:1(2)

"The provisions of sections 3.2 to 3.4 apply, *mutatis mutandis*, to acts of administrative authorities other than decisions to the extent that the nature of the act permits it."

Section 3:2

"When preparing a decision, an administrative authority shall collect the necessary information concerning the relevant facts and interests to be taken into consideration."

Section 3:3

"An administrative authority shall not use the power to take a decision for a purpose other than that for which it was conferred."

Section 3:4

"(1) An administrative authority shall weigh up the interests directly affected by a decision, subject to any limitations following from a provision of law or the nature of the power to be exercised.

(2) The adverse consequences of a decision for one or more interested parties may not be disproportionate to the objectives pursued by the decision."

80. The AWB contains the following relevant provisions on administrative remedies:

Section 3:15(1)

"Interested parties may express their views on a draft decision to the administrative authority either in writing or orally, at their discretion."

Section 6:4(1)

"To raise an objection (*bezwaar*), one must submit a notice of objection to the administrative authority that issued the order."

Section 7:1(1)

"Before lodging an application for judicial review (*beroep*) against an order with an administrative court, the party must first raise an objection against the order ..."

Section 8:1(1)

"An interested party has the right to lodge an application for judicial review with the district court against an order ..."

G. The Code of Criminal Procedure

81. Article 126m § 1 of the Code of Criminal Procedure in conjunction with Article 67 § 1 provides that the interception of communications can be authorised on suspicion of a serious criminal offence, that is, an offence for

which the Criminal Code prescribes a penalty of at least four years' imprisonment.

82. At the relevant time, Article 126cc provided as follows:

> "1. The public prosecutor shall retain the official records and other objects from which data can be derived, which have been obtained through surveillance by means of a technical device which records signals, the recording of confidential communications, the recording of telecommunications or the requesting of data on a user and the telecommunication traffic data pertaining to that user, in so far as said records or objects have not been attached to the case documents (*processtuken*), and shall make them available for the investigation until the conclusion of the case.
>
> 2. Upon expiry of two months after the conclusion of the case ..., the public prosecutor shall order the destruction of the official records and other objects referred to in paragraph 1. An official record of the destruction shall be prepared."

83. Article 126dd provided:

> "1. The public prosecutor may use data obtained through surveillance by means of a technical device which records signals, the recording of confidential communications, the recording of telecommunications or the requesting of data on a user and the telecommunication traffic data pertaining to that user, for the following purposes:
>
> (a) A criminal investigation other than the one for which the authorisation was originally given;
>
> (b) Processing to gain insights into individuals' involvement in crimes and actions as outlined in [the Police Data Act].
>
> 2. In the event of the application of sub-paragraph 1 (a), there is no requirement to destroy the data, in contrast to what is stated in Article 126cc § 2, until the conclusion of the other investigation. In the event of the application of sub-paragraph 1 (b), there is no requirement to destroy the data until such time as the Police Data Act no longer permits its storage."

84. In its judgment of 6 March 2012 (ECLI:NL:HR:2012:BQ8596), the Supreme Court held as follows:

> "3.5 In the light of the legislature's intention ... to protect from destruction – under Article 126cc of the Code of Criminal Procedure – material from which information could be derived that could be used in another case, and having regard to the legislature's intentionally broad interpretation of the term 'other criminal investigation' as referred to in Article 126dd of the Code of Criminal Procedure, it must be concluded that the legislature did not intend to limit the possibility of applying Article 126dd of the Code of Criminal Procedure, as put forward in the statement of grounds for appeal. It should be noted in this regard that Article 126dd of the Code of Criminal Procedure is not intended to regulate the processing of data obtained in the course of a criminal investigation; this purpose is served by the provisions of the WJSG."

H. The Decree on the retention and destruction of non-attached documents

85. The Decree on the retention and destruction of non-attached documents (*Besluit bewaren en vernietigen niet-gevoegde stukken*), which was in force at the material time, established the procedure for the retention

and destruction of the documents referred to in Article 126cc of the Code of Criminal Procedure (see paragraph 82 above). Section 2(1) provided, in particular, that the official reports and other material referred to in Article 126cc § 1 of the Code of Criminal Procedure should be kept in a secure place designated by the public prosecutor.

86. The Explanatory Note to that Decree read as follows:

> "An important difference between the collection of information by such technical means [including for the purpose of recording confidential communications] and the collection of information by other means is that, using technical means, a large amount of information about persons is collected and recorded in a relatively indiscriminate manner. This means that not only information relevant to the investigation is recorded, but also non-relevant information about persons who have nothing to do with the offence. It is for this reason that the new Article 126cc of the Code of Criminal Procedure lays down rules on the preservation and destruction of official reports and other material that contain information recorded using such technical devices and that are not attached to the case documents. On the one hand, it is important that this information be preserved for a certain period of time so that the defence can take note of it in view of it being potentially exculpatory evidence. On the other hand, the protection of privacy requires that this retention period be no longer than is strictly necessary and that, in principle, at the end of this period the data must be destroyed."

I. The Civil Code

87. Article 6:162 of the Civil Code reads as follows:

> "1. Anyone who commits a wrongful act (*onrechtmatige daad*) against another for which he, she or it is responsible, must remedy the resulting damage suffered by the other person.
>
> 2. Unless justified by valid reasons, the following actions are considered wrongful: the infringement of a right, and an act or omission that breaches a duty imposed by law or an unwritten rule governing appropriate social behaviour.
>
> 3. The wrongdoer is held accountable for the commission of a wrongful act if it was the wrongdoer's fault or if it arises from a cause for which he, she or it is liable in accordance with the law or generally accepted principles (*de in het verkeer geldende opvatting*)."

J. The Code of Civil Procedure

88. The relevant part of Article 254 § 1 of the Code of Civil Procedure reads as follows:

> "In situations of urgency where immediate provisional measures are deemed necessary in the interests of the parties, the provisional-measures judge has the authority to grant such measures ..."

II. EUROPEAN UNION LAW

A. The ePrivacy Directive

89. Directive 2002/58/EC (as amended by Directives 2006/24/EC and 2009/136/EC) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ 2002 L 201) ("the ePrivacy Directive") explicitly states that its provisions provide for protection of the legitimate interests of subscribers who are legal persons (Article 1(2)).

90. Article 5(1) of the Directive provides that Member States shall ensure the confidentiality of communications and related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they will prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1).

91. Under Article 15(1) of the Directive, Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in a number of its Articles when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in that paragraph. All the measures referred to in that paragraph must be in accordance with the general principles of Community law.

B. The EIO Directive

92. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ 2014 L 130) ("the EIO Directive") defines the EIO as a judicial decision which has been issued or validated by a judicial authority of a Member State ("the issuing State") to have one or several specific investigative measure(s) carried out in another Member State ("the executing State") to obtain evidence in accordance with that Directive. The EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State (Article 1(1)).

93. The "issuing authority" means a judge, a court, an investigating judge or a public prosecutor competent in the case concerned (Article 2(c)(i)).

94. An EIO may be issued with respect to criminal proceedings that are brought by, or that may be brought before, a judicial authority in respect of a criminal offence under the national law of the issuing State; in proceedings brought by administrative or judicial authorities in respect of acts which are punishable under the national law of the issuing State by virtue of being infringements of the rules of law and where the decision may give rise to proceedings before a court having jurisdiction, in particular, in criminal matters; and in connection with proceedings referred to above which relate to offences or infringements for which a legal person may be held liable or punished in the issuing State (Article 4).

95. The issuing authority may only issue an EIO after assessing whether (a) it is necessary and proportionate for the purpose of the proceedings referred to in Article 4 taking into account the rights of the suspected or accused person; and (b) the investigative measures indicated in the EIO could have been ordered under the same conditions in a similar domestic case (Article 6(1) and (2)).

96. Member States are to ensure that legal remedies equivalent to those available in a similar domestic case, are applicable to the investigative measures indicated in the EIO (Article 14(1)).

C. Relevant case-law of the Court of Justice of the European Union (CJEU)

97. In *Lietuvos Respublikos generalinė prokuratūra* (judgment of 7 September 2023, C-162/22, EU:C:2023:631) the CJEU addressed the issue of the use of data relating to electronic communications (traffic data and the content of electronic communications) retained by providers of electronic communications services, which had originally been made available to the competent authorities for the purpose of combating serious crime, in an administrative investigation into misconduct in office of a public prosecutor, resulting in the latter's dismissal. The CJEU found that the list of objectives capable of justifying a limitation of the right to confidentiality of communications set out in the first sentence of Article 15(1) of the ePrivacy Directive (see paragraph 91 above) was exhaustive. The objectives were enumerated in a hierarchical order and the importance of the objective pursued by the limitation had to be proportionate to the seriousness of the interference (see paragraphs 34-35 of the CJEU's judgment). It held that once data had been retained and made available to the competent authorities for the purpose of combating serious crime, such data could not be transmitted to other authorities and used in order to achieve objectives, such as, in that case, combating corruption-related misconduct in office, which were of lesser importance in the hierarchy of objectives of public interest than the objective of combating serious crime and preventing serious threats to public security (see paragraphs 41-44 of the CJEU's judgment).

98. In *M.N. (EncroChat)* (judgment of 30 April 2024, C-670/22, EU:C:2024:372), the Grand Chamber of the CJEU interpreted the EIO Directive (see paragraphs 92-96 above), which deals with judicial cooperation in criminal matters. It held that it had to be interpreted as meaning that an EIO for the transmission of evidence already in the possession of the competent authorities of the executing State did not necessarily have to be issued by a judge. In so far as, under the law of the issuing State, a public prosecutor was competent, in a purely domestic situation in that State, to order the transmission of evidence already in the possession of the competent national authorities, that public prosecutor was competent to issue an EIO for the transmission of evidence that was already in the possession of the competent authorities of the executing State (see paragraphs 69-77 of the CJEU's judgment). The CJEU further held that the lawfulness under Article 6(1)(b) of the Directive of an EIO seeking the transmission of data already in the possession of the competent authorities of the executing State was subject to the same conditions as those applicable to the transmission of such data in the issuing State and not those applicable to the gathering of the evidence (see paragraphs 94 and 96 of the CJEU's judgment).

III. COMPARATIVE LAW MATERIAL

99. The Court conducted a comparative study of the legislation of thirty-seven member States of the Council of Europe (Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, the Republic of Moldova, Montenegro, North Macedonia, Poland, Portugal, Romania, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom).

100. The legislation of several States (Albania, Bosnia and Herzegovina, Croatia, Finland, Georgia, Latvia, Luxembourg, the Republic of Moldova, North Macedonia, Portugal, Romania, Serbia, Slovakia and Slovenia) does not provide for a possibility to transmit data collected in a criminal investigation, in particular through secret-surveillance measures, to another public authority for non-criminal purposes. Two more States do not provide for a specific legal framework governing transmission of data collected in a criminal investigation, in particular through secret-surveillance measures, to another public authority for non-criminal purposes, but it could not be excluded that transmissions would be possible under general data protection law (Cyprus and Montenegro).

101. In some States it is permitted to transmit data collected during criminal investigations for use in specifically designated non-criminal proceedings, such as competition proceedings (Armenia, Austria, Belgium, the Czech Republic, France, Greece, Iceland, Italy and Switzerland),

disciplinary proceedings (Italy – disciplinary proceedings against judges, employees of public entities and police officers, Lithuania – corruption-related proceedings, Poland – disciplinary proceedings against judges and assessors, San Marino – disciplinary proceedings against judges, and the Czech Republic, in exceptional circumstances), tax proceedings (France, Germany, Italy and Poland), anti-doping proceedings (Spain), for security vetting (the Czech Republic and Estonia) or for the supervision of financial markets (Iceland, Liechtenstein and Switzerland).

102. Some States provide for more general transmission conditions, either instead of specifically designating the proceedings for the purposes of which the data may be transmitted (Cyprus, Denmark, Hungary, Malta, Montenegro, Sweden and the United Kingdom), or together with such specifically defined proceedings (Austria, Belgium, the Czech Republic, Estonia, France, Germany, Greece, Italy, Liechtenstein, Poland and San Marino).

103. By way of example, the States under examination provide for the following conditions for transmissions: (a) an explicit legal basis or authorisation (for example, Austria, the Czech Republic, France, Germany, Hungary, Liechtenstein, Sweden, Switzerland and the United Kingdom); (b) the lawfulness of the collection of information through secret-surveillance measures in the criminal proceedings (for example, Estonia, Germany, Italy, Hungary, Poland and San Marino); (c) the transmitted data must be necessary for the fulfilment of a specified purpose, such as the duties of the requesting/receiving authority (for example, Cyprus, Denmark, Germany, France, Liechtenstein, Switzerland and the United Kingdom); (d) transmission of data is permitted only for a limited set of purposes (for example, Malta and the United Kingdom); (e) respect for the defence rights of the person concerned by securing access to the transmitted information (for example, Belgium, France, Hungary and Italy); (f) consideration of the privacy interests of the person concerned when deciding on transmission of data (for example, Austria, Belgium, Cyprus, Montenegro and Sweden); (g) availability of a remedy before an administrative and/or judicial authority (for example, Austria, the Czech Republic and Germany); and (h) compliance with the principle of proportionality (for example, Germany, Greece and Sweden). In Germany, the transmission of data obtained by intrusive surveillance and investigative measures is permissible only if it would hypothetically be permissible, under constitutional law, to collect the relevant data again for the alternative purpose using comparably intrusive methods; if the information is obtained through covert access to information technology systems, each new use of such data is subject to the same justification requirements as the original data collection. In Austria the recipient must be explicitly allowed to process data for the purpose for which they are transmitted. Greek legislation requires that the criminal proceedings in which the data have been collected and the competition proceedings in which they

will be used be closely related in substance and procedure. In Montenegro it is prohibited to transfer by-catch intercept data.

104. In a majority of States allowing the transmission of data, the transmission authorisation is issued by the public authority possessing the data in question, most often a prosecutor or other investigative authorities. The transmission must be authorised by a judge in Liechtenstein and Spain. In France, transmissions are authorised by an investigative judge, a trial judge or a prosecutor.

105. In general, the above conditions and safeguards apply to the transmission of data regardless of whether they concern individuals or legal persons, but different safeguards apply to natural and legal persons in Denmark. In certain States (for example, Germany, Hungary, Poland), criminal proceedings and/or secret-surveillance measures can be carried out against individuals only. National data protection laws are generally limited to natural persons only, except to a certain extent in Austria and Italy. Legal entities can have their confidentiality and secrecy interests protected under different laws and regulations, which may not reach the level provided under the personal data protection laws (for example, Cyprus, Germany, Iceland, Luxembourg and Romania).

THE LAW

I. JOINDER OF THE APPLICATIONS

106. Having regard to the similar subject matter of the applications, the Court finds it appropriate to examine them jointly in a single judgment.

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

107. The applicant companies complained that the transmission to the Netherlands Competition Authority (*Nederlandse Mededingingsautoriteit* – "the NMA") of intercept data that were irrelevant to the criminal investigation had constituted a violation of their rights under Article 8 of the Convention. In addition, they complained that the exploratory interactions between the officials of the NMA and those involved in the criminal investigations had not been in accordance with the law. Article 8 reads as follows:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

A. The Chamber judgments

108. The Chamber accepted that the transmission to the NMA of data obtained in the criminal investigations against the applicant companies through the tapping of their employees' telephones had constituted an interference with those companies' rights under Article 8 of the Convention. In its assessment of whether the interference had been justified, the Chamber, in the absence of the applicant companies' arguments to the contrary, proceeded on the basis that the intercept data had been lawfully obtained through methods compatible with Article 8 of the Convention. It further took into account that the transmissions had taken place without the applicant companies' knowledge and considered that the standards developed in the context of secret-surveillance measures were relevant to the cases.

109. As regards the lawfulness of the interference, the Chamber found that it had had a legal basis under Dutch law. It further found that the domestic law met the requirement of "foreseeability". In that connection, it concluded as follows. First, that that requirement could not be taken to mean that the authorities had been obliged to give a prior notification to the applicant companies about the data transmissions. Secondly, that differences between the original covert investigative measure and the transmission of the data resulting therefrom had to be taken into account. The transmission of the data had derived from the interception, which had already benefited from safeguards against arbitrariness. The power to transmit the intercept data lawfully obtained in accordance with the requirements of Article 8 had not therefore been "unfettered". Thirdly, that the applicable domestic law had provided adequate indication as to the circumstances and conditions under which the Public Prosecution Service was empowered to transmit data and as to the scope and manner of exercise of its discretion in the matter. In particular, Dutch law set out the limits of and the conditions for the transmission of data by the Public Prosecution Service and provided clear instructions on the exercise of the power to transmit. Fourthly, that it had been sufficiently foreseeable that the NMA was an authority charged with the enforcement of legislation and therefore authorised to receive criminal data. The possibility to transmit intercept data to public authorities that did not themselves have the power to use such coercive measures was clearly provided for in the domestic law, as confirmed by the domestic courts. It had also been sufficiently foreseeable on the basis of the law as interpreted by the domestic courts that data not used for the criminal prosecution could be considered "criminal data" within the meaning of the Judicial and Criminal Data Act (*Wet Justitiële en Strafvorderlijke gegevens* – "the WJSG") and could therefore be transmitted. Furthermore, the Chamber noted that, while the text of section 39f of the WJSG contained strict conditions for the transmission of criminal data, it did not specify the form in which the balancing test required under the domestic law was to be carried out.

However, it clearly followed from the Explanatory Memorandum to the bill, as well as from the WJSG Instructions, that the decision to transmit criminal data was qualified under the domestic legal framework as a "factual act", not as a "decision" under the General Administrative Law Act (*Algemene wet bestuursrecht* – "the AWB"). Lastly, the Chamber found that the exploratory interactions between the officials of the Public Prosecution Service and 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* – "the VROM-IOD"), on the one hand, and the NMA, on the other, had been sufficiently foreseeable, as cooperation between them was needed in order to identify the data relevant for the required compelling general interest and there was no indication that anyone other than the Public Prosecution Service and the VROM-IOD had been responsible for the selection of data. The Chamber concluded from the above that the interference had been "in accordance with the law". The existence of adequate safeguards against arbitrariness and abuse was to be examined as part of the question whether the interference had been "necessary in a democratic society".

110. The Chamber accepted that the data transmission had served the legitimate aim of protecting the economic well-being of the country. It further held that the domestic law contained adequate safeguards against abuse, as it set out the limits of and the conditions for the transmission of criminal data. In particular, the statutory requirement of a "compelling general interest" was explicitly linked in the legislative history to the legitimate aims set out in Article 8 § 2 of the Convention. Additional conditions were outlined in the WJSG Instructions, including the requirement for the receiving authority to have a legal basis to receive the data, the inability for that authority to obtain the information by less intrusive methods and the requirement that the data be necessary for a purpose defined in section 39f of the WJSG. Furthermore, there was extensive *ex post facto* judicial oversight in place, including administrative proceedings concerning the NMA's decision to impose fines on the applicant companies and proceedings before the civil courts. The courts in both sets of proceedings had been competent to rule on the lawfulness and Convention-compliance of the transmissions and had been able to afford redress. The civil courts could have prevented the data from being used by the NMA, if the transmission had been found to have been unlawful. Lastly, the Chamber found that the interference had been proportionate to the legitimate aim pursued. The domestic courts had conducted an adequate balancing exercise between the interests of the applicant companies and the public interest in protecting the economic well-being of the country.

B. The parties' submissions

1. The applicant companies

(a) The legal basis for the interference and the "foreseeability" of the domestic law

111. The applicant companies submitted that the interference with their Article 8 rights had had no basis in the domestic law and that the domestic law did not meet the "foreseeability" requirements. First, the broad interpretation of "criminal data" (see paragraph 61 above) as including "by-catch" data had been unforeseeable. In the applicant companies' opinion, only information which was reasonably relevant to the prosecution of the criminal case was to be included in a criminal file and therefore considered as falling under the definition of "criminal data". Not all information collected in the context of a criminal investigation could be processed under the WJSG: under section 39b of the WJSG and the Explanatory Memorandum (see paragraphs 61 and 63 above), only information necessary for the proper discharge of the duties of the Public Prosecution Service – that is, the prosecution of criminal offences – could thereby be processed. Data that had no relevance to the criminal investigation could not therefore be processed under the WJSG. Instead, such data were to be handled according to a distinct legal framework outlined in Article 126cc of the Code of Criminal Procedure and the Decree on the retention and destruction of non-attached documents (see paragraphs 82 and 85-86 above). The fact that by-catch data were temporarily digitally stored and archived could not alter that conclusion. Significantly, Ships Waste Oil Collector B.V. had never been under investigation and the by-catch intercept data in respect of it had not been covered by the interception authorisation. Therefore, the transmission of those data had been incompatible with the purposes for which they had been collected. The applicant companies also argued that the Supreme Court's judgment of 20 April 2012 (see paragraph 72 above) was not relevant to their situation and, in any event, did not support the interpretation of "criminal data" as including data that were irrelevant to the subject of the prosecution from the outset.

112. Secondly, it had not been foreseeable that intercept data could be transmitted to the NMA. The NMA had no power to intercept communications, as telephone tapping was only allowed for a limited list of serious crimes (see paragraph 81 above). Furthermore, neither the legislation nor the WJSG Instructions explicitly mentioned it as a permitted recipient of criminal data.

113. Thirdly, the applicant companies submitted that the conditions for transmitting criminal data under section 39f of the WJSG had not been fulfilled. Transmission of criminal data under that provision was permissible only in so far as it was necessary in view of a compelling general interest. It could not be assumed that every violation of section 6 of the Competition Act

would give rise to the existence of a compelling general interest; the legislature had clearly intended to allow the transmission of data in only exceptional circumstances. In any event, data transmissions for the enforcement of section 6 of the Competition Act were not specifically provided for and were therefore not foreseeable. The applicants also relied on the WJSG Instructions (see paragraph 69 above), which stated that the transmission of criminal data could occur only after the delivery of a relevant judgment by a criminal court; transmissions prior to that were allowed only in urgent cases after the criminal case had been examined by the Public Prosecution Service. That requirement had not been complied with in their case. The applicant companies further submitted that under section 39f of the WJSG, the Public Prosecution Service had the procedural duty to state the reasons for its decision to transmit data, so that its balancing of interests could be verified (see paragraph 65 above). This obligation had not been respected.

114. Lastly, the WJSG did not provide a legal basis for the disclosure of criminal data prior to their official transmission. Nor had there been a legal basis for the NMA to provide a list of search terms on the basis of which the prosecutor could search for additional information for transmission. The WJSG Instructions explicitly stated that it was for the Public Prosecution Service, and not the recipient, to determine what criminal data the recipient needed (see paragraph 69 above). The NMA's access to the data prior to their official transmission had undermined the legislature's intention to limit transmissions to what was necessary in view of a compelling general interest. Even if the prosecutor had ultimately refused to transmit the data, the NMA had already taken cognisance of them and, on the basis of that knowledge, could have used its own investigative powers to collect evidence against the applicant companies. In such a case, the applicant companies would have been unable to learn about, and demonstrate, the illegal origin of the NMA's knowledge.

(b) Safeguards against arbitrariness and abuse

115. The applicant companies submitted that the domestic law did not set out with sufficient clarity the circumstances and conditions under which the transmission of criminal data to other authorities was authorised. As a result, the discretion granted to the Public Prosecution Service was barely restricted, leading to almost unfettered power, which was incompatible with the Court's case-law. First, the term "compelling general interest" lacked a precise definition. The WJSG Instructions only provided a broad reference to interests that could be encompassed by this concept. Secondly, the aims justifying the transmission of criminal data were formulated in a very broad and vague manner such as, in so far as relevant for the present case, the "enforcement of legislation" under section 39f(1)(c) of the WJSG. The WJSG Instructions (see paragraph 69 above) did not list or specify the minimum level of gravity of violations of legislation that could justify the transmission

of data under that provision. The assessment of whether the suspected violation of legislation was serious enough to justify the transmission of data was therefore left to the prosecutor's discretion.

116. The applicant companies also argued that prosecutors who had the authority to authorise transmissions of criminal data were part of the executive and could not therefore be deemed an independent body within the meaning of the Court's case-law.

117. The WJSG and the WJSG Instructions did not contain any requirements relating to the content of the transmission authorisations. The legislature had clearly intended that they should contain an identifiable and verifiable statement of reasons (see paragraph 65 above). No statement of reasons had, however, been provided in the applicant companies' cases (see paragraphs 15, 17, 19 and 40 above). The applicant companies had therefore been unable to ascertain whether the balancing of conflicting interests, having regard to the principles of necessity, proportionality and subsidiarity, as required by the domestic law, had been performed prior to the transmission of the data. The absence of a reasoned decision, coupled with the wide discretion afforded to public prosecutors, meant that the extent to which the applicant companies' interests had been taken into account remained unknown and rendered the *ex ante* decision-making process incapable of providing sufficient safeguards against arbitrariness and abuse. Given the highly intrusive nature of telephone tapping and large amounts of data irrelevant for the investigation thereby collected, the absence of sufficient safeguards for the further processing of such data raised serious concerns.

118. In the applicant companies' view, the absence of an identifiable and verifiable *ex ante* reasoning could not be remedied by *ex post facto* judicial review. The WJSG did not provide for an obligation to give notice of the data transmission. The applicant companies had, for example, learned about the transmissions months after they had taken place. The NMA had therefore had ample time to investigate the data before the applicants had had an opportunity to oppose their transmission. The information obtained by the NMA as a result could not be unlearnt.

119. Furthermore, the fact that the transmission of criminal data under section 39f of the WJSG was deemed a "factual act" (*feitelijke handling*) rather than a "decision" (*besluit*) within the meaning of the AWB limited the possibilities for a judicial review. In particular, it was not possible to use administrative legal remedies against the transmission itself (see paragraph 70 above), such as an objection (*bezwaar*) and an application for judicial review (*beroep*) under the AWB. The only available remedy had been before the civil courts under Article 6:162 of the Civil Code (see paragraph 87 above). The scope of the civil courts' review was, however, insufficient. Because the legislature frequently granted administrative authorities a certain amount of discretion, civil courts typically conducted a limited review of the legality of their actions. Thus, the

transmission authorisation could be deemed a wrongful act under Article 6:162 of the Civil Code only if the civil court found that the administrative authority could not have reasonably approved the transmission. Furthermore, considering that civil proceedings typically took eighteen to twenty-four months, it seemed improbable that they could result in a judgment before the NMA imposed an administrative fine. Civil courts were reluctant to rule on the lawfulness of the data transmission if it could be examined subsequently on judicial review in administrative proceedings challenging any fine imposed.

120. As regards the judicial review of the NMA's decision to impose a fine, the present case showed that its scope was also limited. Evidence unlawfully obtained under criminal law could be used in administrative proceedings unless it violated the "*zozeer-indruist*" criterion. That criterion, established in the case-law, dictated that evidence obtained unlawfully could only be excluded in administrative proceedings if its acquisition conflicted with "what could be expected from a government acting appropriately" to the extent that its use was impermissible in all circumstances. The review of the lawfulness of a data transmission to the NMA by the Supreme Administrative Court for Trade and Industry was limited to that criterion. It was, moreover, influenced by the Supreme Court's position that the NMA was not obliged to verify the legitimacy of receiving criminal data. As a result, an administrative judicial review could not provide a comprehensive judicial review of the legality of a data transmission.

(c) Legitimate aim and proportionality of the interference

121. The applicant companies conceded that the interference with their Article 8 rights had pursued a legitimate aim, although that legitimate aim had not been sufficiently established in the domestic proceedings.

122. They further submitted that the transmission of by-catch data had not been proportionate to the legitimate aim, for the same reasons they had submitted that the transmission had not had a foreseeable basis in law. The transmission of data had led to very serious consequences for the applicant companies, such as heavy fines and exclusion from public procurement procedures. The reasons advanced by the domestic authorities to justify such a serious interference with the applicant companies' Article 8 rights had been insufficient. In particular, the domestic authorities had considered that the transmission of data had constituted a limited interference, which had been less serious than the original telephone tapping. Furthermore, the NMA could have investigated the violations of the Competition Act by using investigative powers accorded to it by the legislature. The transmission of the by-catch data had not therefore complied with the statutory principles of necessity, proportionality and subsidiarity.

2. The Government

(a) Existence of an interference

123. The Government accepted that the transmission of the criminal data by the Public Prosecution Service to the NMA had enlarged the group of persons with knowledge of the intercepted data. The transmission of the criminal data had therefore amounted to an interference with the applicant companies' rights under Article 8 the Convention.

(b) The legal basis for the interference and the "foreseeability" of the domestic law

124. The Government submitted that in all the cases the transmitted criminal data had been lawfully obtained in the framework of criminal investigations concerning serious criminal offences. The criminal data had been lawfully transmitted to the NMA under section 39f(1)(c) of the WJSG, the WJSG Instructions and section 6(1) of the Competition Act (see paragraphs 61, 69 and 77 above). The applicant companies had challenged the transmission of the criminal data in the administrative proceedings concerning the fines and, in the Janssen companies' case, also in civil proceedings. The domestic courts had found that the data transmission had been lawful.

125. The data transmitted to the NMA in the present cases had been "criminal data" within the meaning of section 1(b) of the WJSG (see paragraph 61 above), as confirmed by the domestic courts. They had been obtained in the framework of criminal proceedings on the basis of a judicial authorisation. The intercepted communications had been stored digitally and processed by automated means. The Government disagreed with the applicants' argument that the transmitted data had been "by-catch" data obtained incidentally. The fact that the data had proved to be irrelevant to the criminal investigations had not affected their classification as "criminal data".

126. Nor did the Government agree with the applicant companies' argument that the data in question should have been destroyed pursuant to Article 126cc of the Code of Criminal Procedure (see paragraph 82 above). They relied in this respect on Article 126dd of that Code (see paragraphs 83-84 above). They found it illogical that lawfully transmitted criminal data should be destroyed before the administrative proceedings had been concluded simply because the criminal case in the framework of which the data had been collected had been closed.

127. As regards the provision of search terms and the NMA's access to the intercept data prior to the transmissions, the Government considered it logical and reasonable that the Public Prosecution Service should be able to contact the recipient for preliminary consultations to assess the necessity of the transmission. A degree of insight into the data in question by the receiving public authority might be needed to assist the prosecutor in understanding

whether there were sufficient reasons for that authority to carry out an investigation or take supervisory measures. Such prior consultations could help ensure more targeted and proportionate transmissions of data by limiting them to what was necessary and relevant. The Government stressed that the NMA had not had access to the entirety of the intercept material and had not been allowed to select intercept material for transmission. The fact that the NMA had supplied digital search terms to the Public Prosecution Service to facilitate selection of relevant data had permitted the latter to work in a more targeted manner. However, the public prosecutor had at all times been in charge of the process and had decided which material was to be transmitted, based on his assessment of the necessity and proportionality of the transmission. Such prior consultations were not prohibited under domestic law and served an important objective of ensuring compliance with the statutory requirements of necessity, subsidiarity and proportionality.

(c) Safeguards against arbitrariness and abuse

128. The Government submitted at the outset that the safeguards for the transmission of intercept material developed in *Big Brother Watch and Others v. the United Kingdom* ([GC], nos. 58170/13 and 2 others, 25 May 2021) concerned the international transmission of data obtained as a result of the bulk interception of communications. They were not applicable to the present case, which concerned the domestic transmission of data obtained as a result of the targeted interception of communications on the basis of a valid judicial authorisation. Furthermore, the transmission of a selection of lawfully obtained data was a less serious interference compared to the actual interception of communications. Although they agreed that adequate and effective safeguards had to be in place, they argued that such safeguards did not necessarily have to be identical to those applied to the authorisation of interception measures. States Parties enjoyed a wider margin of appreciation in determining the statutory safeguards applicable to the transmission of lawfully intercepted data.

129. In the alternative, they argued that the domestic law contained the safeguards required by the *Big Brother Watch and Others* case (cited above), which ensured that the discretion granted to the public prosecutor did not result in an unfettered power. The domestic law gave a clear indication as to the circumstances and the conditions under which prosecutors were empowered to transmit data to third parties under section 39f of the WJSG. First, only "criminal data" could be transmitted. The definition of "criminal data" was deliberately broad. The crucial criteria were that the information had been acquired within the framework of a criminal investigation and had undergone automated processing. Secondly, data could only be transmitted for one of the purposes exhaustively listed in section 39f(1) of the WJSG, including, in so far as relevant for the present case, the enforcement of legislation. Thirdly, data could be transmitted only if necessary in view of a

compelling general interest. It appeared from the legislative history that "compelling general interest" was intended to reflect the exhaustive list of purposes set out in paragraph 2 of Article 8 of the Convention, including the protection of the economic well-being of the country. By listing permissible purposes for transmission, section 39f of the WJSG gave concrete expression to what was meant by "compelling general interest".

130. Furthermore, the WJSG Instructions contained a list of recipients to which data could be transmitted. In particular, they specified that "administrative bodies" were permitted to receive data transmitted for the purpose of the enforcement of legislation. The NMA was such an administrative body, responsible for enforcing the Competition Act. The Agreement between the Public Prosecution Service and the NMA, officially published on 14 April 2003, contained arrangements on data sharing between the Public Prosecution Service and the NMA (see paragraph 73 above). It had therefore been foreseeable that the NMA was one of the administrative bodies which could lawfully receive criminal data, despite the fact that it was not explicitly mentioned in the WJSG Instructions. It had been a deliberate choice by the legislature to make the list of potential recipients non-exhaustive, leaving it to the discretion of the Public Prosecution Service to decide who had an interest in receiving those data. The aim had been to avoid a situation where the Public Prosecution Service was not permitted to share data necessary for the performance of a crucial task by an authority not mentioned on the list. In the Government's opinion, that did not mean that the domestic law failed to satisfy the requirement of "foreseeability": it was essential to allow room for interpreting the WJSG requirements.

131. Data transmissions were also subject to the principles of proportionality and subsidiarity. The legislature recognised the interest of the data subject in protecting his, her or its privacy and required the prosecutor to carefully weigh the conflicting interests before transmitting criminal data to third parties. In so doing, the prosecutor was required to take into account the fact that the data had been obtained by covert investigative measures without the knowledge of the person concerned. In particular, the prosecutor had to assess whether the data transmission was compatible with the purpose for which they had been collected, namely the prosecution of one or more criminal offences. He or she also had to verify whether the recipient had a legal basis for receiving that data. Furthermore, he or she had to evaluate whether it was possible for the recipient to obtain the information in a less intrusive way (see paragraph 63 above). It also followed from the WJSG Instructions that no more information than was necessary for the purpose of the transmission could be transmitted to the recipient. This meant that the prosecutor had to assess what information was necessary for the recipient to exercise its tasks.

132. As regards the second requirement outlined in the *Big Brother Watch and Others* case (cited above), namely that the transmission of intercept

material should be subject to independent control, the Government stressed that the Court had not yet explained by whom and at what point such control should be exercised. They argued that in the Netherlands, the transmission of data was subject to independent control, first, through the weighing-up of interests by the public prosecutor and, secondly, through judicial review.

133. The legislature considered that the Public Prosecution Service was well suited to weigh up the interests of the data subject against the compelling general interest and to decide whether it was necessary to transmit criminal data to a third party. The Public Prosecution Service was independent from the NMA, as there were no hierarchical links between the two bodies. Furthermore, the Public Prosecution Service had no vested interest in transmitting data to the NMA, as the data were transmitted for non-criminal justice purposes. Public prosecutors were therefore capable of impartially weighing up the interests of the person concerned against the compelling general interest.

134. The Government further explained that the transmission of criminal data under section 39f of the WJSG was not intended to have legal effect. Therefore, such a transmission was not a "decision" (*besluit*) within the meaning of the AWB (see paragraph 78 above). It was a "factual act" (*feitelijke handeling*). A prosecutor was accordingly not required to state his or her reasoning in writing, since the requirement to provide written reasoning applied only to "decisions". By the same token, he or she was not required to notify the person concerned of the transmission of data. Indeed, such a notification could obstruct the investigation conducted by the administrative authority and would thereby defeat the intended purpose of the data transmission. However, the so-called "general principles of good administration" (*algemene beginselen van behoorlijk bestuur*), including the principle of proportionality, applied, *mutatis mutandis*, to "factual acts" (see paragraph 79 above). In addition, there were a number of unwritten principles of good administration, which included the principles of legal certainty, equality and protection of legitimate expectations. Moreover, every transmission of criminal data was recorded, and the record was kept for at least one year (see paragraph 61 above). In other words, although a prosecutor was not required to state his or her reasoning in writing, the domestic law contained sufficient safeguards against arbitrariness and abuse, in particular, by requiring the prosecutor to weigh up the competing interests before taking a decision to transmit criminal data to third parties.

135. The Government argued that the present case differed from *Dragojević v. Croatia* (no. 68955/11, 15 January 2015), in which the obligation to provide written reasoning had been set out in the domestic law and had not been complied with. By contrast, Dutch law did not require the prosecutor to provide written reasoning; the procedure prescribed by the domestic law had been complied with in the present case. In their view, the absence of prior written reasoning was not incompatible with the Convention

as such and did not undermine the effectiveness of the available *ex post facto* judicial review. The courts could still examine, on the basis of information in the case file, whether the data transmission had complied with the general principles of good administration and with the requirements of the WJSG and the WJSG Instructions, including whether the statutory principles of necessity and proportionality had been satisfied. The conflicting interests involved were evident and all pertinent information was presented to the courts for them to weigh those interests retrospectively and independently against each other, even in the absence of written reasoning from the prosecutor. If necessary, the public prosecutor could, at the request of the judge, provide an insight into the underlying weighing-up of interests. For example, in the applicant companies' cases, the Public Prosecution Service had intervened as a third party in the proceedings before the Supreme Administrative Court for Trade and Industry and had explained the reasoning behind the transmission of the data (see paragraphs 28 and 54 above). In any event, the courts had to assess the lawfulness of the transmission itself rather than the prosecutor's reasoning.

136. The applicants had had the possibility of lodging an action before a civil court under Article 6:162 of the Civil Code (see paragraph 87 above) to claim compensation for the damage suffered as a result of the disclosure of criminal data. It had also been possible to institute provisional-measures proceedings under Article 254 of the Code of Civil Procedure (see paragraph 88 above). Those procedures provided for the possibility of a full review of the lawfulness of the data transmission, including its compatibility with Article 8 of the Convention. In addition, if an administrative authority had imposed a fine on the basis of the information in the transmitted criminal data – as in the applicant companies' case – the person concerned could lodge an objection against the decision imposing the fine with the administrative authority that had made it (sections 6:4 and 7:1 of the AWB, see paragraph 80 above). The decision on such an objection was subject to judicial review under the AWB (see paragraph 80 above). The administrative courts had competence to examine whether the evidence used to make the decision to impose a fine had been obtained in a lawful manner. They could therefore examine whether the transmission of the criminal data had been compatible with Article 8 of the Convention.

(d) Legitimate aim and proportionality of the interference

137. The Government submitted that the information provided to the NMA in the present case had contained indications of price fixing. The investigation of such anti-competitive practices was in the general interest. The transmission of the data in question to the NMA had therefore served the legitimate aim of protecting the economic well-being of the country.

138. They further argued that they should be afforded a margin of appreciation in assessing whether the contested measures were "necessary in

a democratic society". Given that they concerned legal persons, a wider margin of appreciation was to be applied than would have been the case had they concerned an individual (they referred to *Bernh Larsen Holding AS and Others v. Norway*, no. 24117/08, §§ 158-59, 14 March 2013, and *Naumenko and SIA Rix Shipping v. Latvia*, no. 50805/14, § 51, 23 June 2022). The fact that only a limited amount of relevant targeted information had been transmitted further widened the margin of appreciation.

139. In their opinion, the fact that the NMA itself had no power to intercept communications had no relevance for the question whether the transmission of intercept material to, and its subsequent use by, the NMA had been proportionate to the legitimate aim pursued. None of the third parties to which criminal data could be transmitted under section 39f of the WJSG possessed such a power. Only the Public Prosecution Service could intercept communications, after receiving an authorisation from an investigating judge. There was a significant difference between granting a public authority the power to intercept communications, thus causing a serious interference with the right to privacy, on the one hand, and, on the other, allowing the use, under specific conditions and based on statutory provisions, of information uncovered incidentally by another public authority during the lawful interception of communications for other purposes. Furthermore, the Government rejected the applicant companies' allegations that, by benefiting from the transmitted intercept material, the NMA had indirectly misappropriated the power to intercept communications that were not granted to it by the legislation. The applicant companies had not contested that the transmitted information had been lawfully obtained in the framework of criminal investigations into serious crimes.

140. Furthermore, the fact that the original interception authorisations had been limited to the criminal investigation was irrelevant, as was the question whether the authorising judge could have foreseen that the intercept material thereby obtained would be transmitted to the NMA. In the course of criminal investigations, there were sometimes instances where more information than had originally been sought was obtained. Such information could be transmitted to third parties under the WJSG if the Public Prosecution Service considered it necessary in view of a compelling general interest and after weighing up the interests at stake.

141. The Government submitted that in the present cases the domestic courts had advanced relevant and sufficient reasons for the data transmissions. The intercept material had disclosed indications of anti-competitive agreements. The Court had previously acknowledged the strong public interest involved in the effective enforcement of competition law (referring to *SA-Capital Oy v. Finland*, no. 5556/10, § 78, 14 February 2019). That public interest had outweighed the applicant companies' interests. It was unlikely that the NMA could have learned about the anti-competitive agreements through other means, as such agreements were

not as a rule made in writing. There had therefore been no less intrusive alternatives to obtain the information. Furthermore, the prosecutor had taken care to transmit only information that might be relevant for the NMA's investigations, which had amounted to a very small part of the total intercept material. The interference had therefore been proportionate to the legitimate aim pursued.

3. The third party

142. The United Kingdom Government submitted that there was no requirement for *ex ante* authorisation, whether by a court or other independent body, for the transmission of intercept data to a third party in the Court's existing case-law. Introducing such a requirement would not be consistent with the conclusion in *Big Brother Watch and Others* (cited above), in which the Grand Chamber of the Court had specifically examined the British system which required no *ex ante* authorisation at all (let alone independent authorisation), prior to onward transmission of intercepted material to foreign intelligence partners, and had found it consistent with Article 8. The Grand Chamber had held that the transmission of intercept data to third parties had to be "subject to supervision by an independent authority" and "subject to independent control". Furthermore, it had found that the *ex post facto* oversight and review mechanisms in place in the United Kingdom satisfied those tests (ibid., §§ 356, 362, 398, 411-12 and 414-15). If, as the Court had held in *Big Brother Watch and Others*, there was no need for intelligence agencies to have *ex ante* independent authorisation before onward transmission to foreign intelligence partners, it was very difficult to see how it could possibly be justified as a requirement before transmitting intercept data to domestic authorities.

143. Furthermore, developing the Court's case-law to introduce a requirement of *ex ante* independent authorisation would not be in the public interest. A requirement to apply to a judge for authorisation to transmit intercept data to another body would likely involve substantial additional resources and administrative burden. However, there would likely be little or no incentive for any intercepting agency to expend those resources and incur that burden, as the purpose of transmitting the intercept data would relate to the functions of the recipient public body and it would not further the intercepting agency's own aims. Such a requirement would thus act as a great disincentive to the police or any other intercepting authority to transmit data, even if such transmission was strongly in the public interest. The requirement for independent authorisation would also likely involve substantial additional delay. Moreover, such further independent authorisation was in any event unnecessary. Where the interception of the data had itself already been independently authorised, ensuring that its collection was necessary and proportionate, its onward transmission to another domestic public body would be sufficiently safeguarded by (i) the existence of clear conditions for

transmission, set out in domestic law; (ii) the need for the intercepting agency to satisfy itself that the recipient had adequate protections in place for the data; and (iii) the existence of independent oversight over the transmission of data, including the availability of judicial review.

144. The United Kingdom Government also submitted that it was unnecessary for the public prosecutor to have given a reasoned decision for the transmission, in circumstances where relevant and sufficient reasons for the same were given in the course of an *ex post facto* judicial review. The Court's existing case-law did not require a "properly reasoned decision" for the proposed transmission. In particular, there was no reference to any such requirement in *Big Brother Watch and Others* (cited above). Secondly, a requirement for a "properly reasoned decision" would risk imposing far too onerous a burden on an authorising body; it would be a significant disincentive to data transmission. Thirdly, it was unnecessary. Although the authority transmitting the intercept data to a third party should make a sufficient record of the basis of the decision to do so, to enable effective *ex post facto* independent oversight and/or judicial review, that did not connote any need for a quasi-judicial "reasoned decision".

C. The Court's assessment

1. Existence of an interference and its scope

145. It was not disputed between the parties that there had been an interference with the applicant companies' Article 8 rights.

146. The Court has previously accepted that legal entities are entitled to the protection afforded by Article 8, and can thus claim to be victims of an interference with their Article 8 rights. In particular, the business premises of legal persons are covered by the notion of "home" under Article 8 § 1 of the Convention (see, among others, *Société Canal Plus and Others v. France*, no. 29408/08, § 52, 21 December 2010; *Société Colas Est and Others v. France*, no. 37971/97, §§ 41-42, ECHR 2002-III; *Saint-Paul Luxembourg S.A. v. Luxembourg*, no. 26419/10, §§ 37 and 39, 18 April 2013; and *UAB Kesko Senukai Lithuania v. Lithuania*, no. 19162/19, §§ 109-10, 4 April 2023), and the communications of legal persons are covered by the notion of "correspondence" under that Article (see, for example, in the context of secret-surveillance activities, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 60, 28 June 2007; *Liblik and Others v. Estonia*, nos. 173/15 and 5 others, § 110, 28 May 2019; and *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, § 374, 11 January 2022). Article 8 thus provides protection for the confidentiality of legal persons' communications.

147. In the present case, the telephones of some of the employees of the Janssen companies and of the I. company were tapped in the framework of criminal investigations. Among the conversations thus intercepted were

telephone conversations between the employees of the I. company and the employees of the Ships Waste Oil Collector B.V. company. A selection of the information obtained was transmitted to the NMA and used as a basis for fining the applicant companies in competition proceedings. The interception measures, and subsequent data transmissions for use in the competition proceedings directly affected the applicant companies and therefore interfered with their right to respect for their correspondence under Article 8 (compare *Liblik and Others*, cited above, §§ 111-12).

148. The Court notes that neither the Ships Waste Oil Collector B.V. company nor its employees were targeted by the interception measures and that its employees' conversations were intercepted incidentally as a result of the tapping of the telephones of the I. company's employees. It has previously found that telephone tapping carried out on the line of a third party as a result of which an applicant's conversations with that third party were intercepted, and the use of those data in criminal or disciplinary proceedings against the applicant amounted to an interference with that person's Article 8 rights (see, among others, *Lambert v. France*, 24 August 1998, § 21, *Reports of Judgments and Decisions* 1998-V; *Pruteanu v. Romania*, no. 30181/05, § 41, 3 February 2015; *Versini-Campinchi and Crasnianski v. France*, no. 49176/11, § 49, 16 June 2016; and *Terrazzoni v. France*, no. 33242/12, § 43, 29 June 2017). The Court does not see any reason to reach a different conclusion in the present case.

149. It must further be examined whether in the present case the interception of communications and the transmission of the data thereby obtained for use in the competition proceedings are aspects of a single interference or constitute separate interferences. The Court has found in some cases that the interception and transmission of intercept data were aspects of the same interference (see *Versini-Campinchi and Crasnianski*, cited above, § 49; *Terrazzoni*, cited above, § 43; and *Adomaitis v. Lithuania*, no. 14833/18, § 81, 18 January 2022), while in other cases it regarded them as two distinct interferences (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 79, ECHR 2006-XI, and *Karabeyoğlu v. Turkey*, no. 30083/10, §§ 74, 112 and 119, 7 June 2016). Given that the transmission of data to other authorities enlarges the group of persons with knowledge of the intercept data and can lead to investigations or other action being instituted against the data subject (see *Weber and Saravia*, cited above, § 79), the Court considers that the transmission of intercept data for further use by another law-enforcement authority constitutes a separate interference with Article 8 rights, distinct from, albeit related to, the original interception of communications.

150. In view of the above considerations, the Court considers that the transmissions of intercept data for use in the competition proceedings amounted to an interference with the applicant companies' right to respect for their correspondence under Article 8.

2. Justification for the interference

(a) Applicable general principles

(i) Lawfulness and necessity in a democratic society

151. The confidentiality of communications is an essential element of the right to respect for private life and correspondence, as enshrined in Article 8. Users of telecommunications and internet services must have a guarantee that their own privacy and freedom of expression will be respected, although such a guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others (see *K.U. v. Finland*, no. 2872/02, § 49, ECHR 2008, and *Delfi AS v. Estonia* [GC], no. 64569/09, § 149, ECHR 2015).

152. Any interference with Article 8 rights can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which that paragraph refers and is necessary in a democratic society in order to achieve any such aim. The wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 228, ECHR 2015). An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient" (see *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 101, ECHR 2008).

153. When intercept data, obtained in a Convention-compliant manner, is transmitted from one law-enforcement agency to another without the knowledge of the data subject, the Grand Chamber, like the Chamber, considers that the standards developed in the context of secret-surveillance measures are relevant to its assessment. At the same time, owing to the difference in the extent of the interference between the original interception and the subsequent transmission of data, these standards cannot be directly transposed to cases such as the present one. The interception of communications is a very intrusive measure because, by its very nature, it is likely to result in the collection and examination of a large volume of a targeted person's communications. By contrast, data transmissions such as that in the present case involve, as a rule, only a limited amount of selected intercept material that has been lawfully obtained and are in that sense usually less intrusive.

154. The Court also notes that the transmitted data are usually the product of legally regulated interception procedures to which all relevant safeguards against arbitrariness and abuse apply. This includes procedural safeguards, such as those relating to authorisation procedures, and substantive safeguards, such as those regarding the grounds on which the interception can be ordered. Therefore, the safeguards applicable to the process of obtaining intercept data that may subsequently be transmitted to another law-enforcement authority also limit, at least to a certain extent, the risk of arbitrariness and abuse related to the transmission (see, *mutatis mutandis*, *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, § 324, 25 May 2021).

155. Accordingly, the Court considers that while the standards developed in the context of secret-surveillance measures provide a useful framework for its assessment, they will have to be adapted to reflect the specific features of transmissions of intercept data from one law-enforcement agency to another. In this respect, the Court will also have regard to the standards developed in the context of data protection.

156. The Court reiterates that it is essential, in the context of data protection – as in the context of telephone tapping, secret surveillance and covert intelligence-gathering – to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient safeguards against arbitrariness and abuse (compare *S. and Marper*, cited above, § 99, with further references).

157. While being, as a rule, less intrusive than the original interception of communications, the transmission of intercept data for use in pursuit of a new purpose is a significant interference with the rights of the data subject, which must be justified in accordance with the requirements of Article 8 § 2. The Court has therefore held that the transmission of data for use beyond the original criminal context for their collection must have a basis in law and be foreseeable to the data subject (see *Versini-Campinchi and Crasnianski*, cited above, § 55; *Terrazzoni*, cited above, §§ 49-50; and *Starkevič v. Lithuania*, no. 7512/18, § 87, 29 March 2022). The importance of sufficiently circumscribing in law the scope of possible new uses of the data has also been noted by the Court as a safeguard against arbitrariness and abuse (see, for example, *Weber and Saravia*, cited above, §§ 125-26; *Karabeyoğlu*, cited above, §§ 117-18; *Ekimdzhiev and Others*, cited above, § 327; and *Adomaitis*, cited above, § 87). The Court has, furthermore, required that such transmission and use be convincingly justified in the circumstances of the case by reference, *inter alia*, to the importance of the aim pursued by the transmission (see *Drakšas v. Lithuania*, no. 36662/04, § 61, 31 July 2012; *Adomaitis*, cited above, § 87; and *Starkevič*, cited above, § 91). Finally, in its assessment of the necessity in a democratic society of data transmissions in

pursuit of purposes beyond the original criminal context for their collection, the Court took into account that the transmission was subject to effective judicial review (see *Versini-Campinchi and Crasnianski*, cited above, § 74; *Terrazzoni*, cited above, §§ 60-61; and *Adomaitis*, cited above, § 87).

158. The Court also notes that the lawfulness of the interference resulting from the transmission of intercept data is closely connected to the question whether the interference was "necessary in a democratic society". It may therefore be appropriate for the Court to address the two requirements jointly. In this context, "the quality of law" implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that the transmission of intercept data takes place only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards against arbitrariness and abuse (compare *Roman Zakharov*, cited above, § 236). Regardless of whether it is addressed separately or jointly with the lawfulness requirement, this assessment depends on all the circumstances of the case, such as the nature and scope of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law (compare *Roman Zakharov*, cited above, 232, and *Liblik and Others*, cited above, §§ 130-31).

159. It follows from the Court's well-established case-law that the law must provide for "precautions to be taken when communicating [intercept] data to other parties" (see *Roman Zakharov*, cited above, § 231). They should ensure, *inter alia*, that the transmissions do not become an instrument for circumventing the strict safeguards applicable to the interception of communications. To date the Court has not yet provided guidance regarding such precautions, except in the very specific context of the international transmission of data collected through the bulk interception of communications (see *Big Brother Watch and Others*, cited above, §§ 362 and 392). The Court considers that, outside that context, the precautions to be taken when communicating intercept material to another law-enforcement authority should include the following minimum requirements, which should be set out in law in order to avoid arbitrariness and abuse.

160. First, the Court considers that the transmission of intercept material beyond the original criminal context for its collection should be limited to such material as has been collected in a Convention-compliant manner. Secondly, the circumstances in which such a transmission may take place must be set out clearly in domestic law. In this respect, the Court notes that where a power vested in the executive is exercised in secret, the risks of arbitrariness and abuse are evident. It is therefore essential to have sufficiently clear rules on when the transmission of intercept data can take place without the knowledge of those concerned. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances and conditions under which public authorities are empowered

to resort to any such measures. Moreover, since the implementation in practice of such measures is not open to scrutiny by the individuals concerned or the public at large, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (compare, in the context of secret surveillance, *Roman Zakharov*, cited above, §§ 229-30). Thirdly, the law must provide for safeguards concerning the examination, storage, use, onward transmission and destruction of the data transmitted. Finally, the transmission and use of intercept data for a purpose beyond the original criminal context for their collection must be subject to effective review by a judicial or otherwise independent body (see *Versini-Campinchi and Crasnianski*, cited above, § 74; *Terrazzoni*, cited above, §§ 60-61; and *Adomaitis*, cited above, § 87).

161. The Court must also assess whether the interference arising out of the data transmission can, in the circumstances of the case, be considered "necessary in a democratic society" in pursuit of a legitimate aim (see paragraph 152 above). In this assessment, the Court will take into account the nature of the data, the importance of the aim pursued by their transmission, and the resulting consequences for the applicant, as well as the quality of the authorisation procedures and the effectiveness of available remedies.

(ii) The level of protection for legal persons and the margin of appreciation

162. The Court reiterates that the breadth of the margin of appreciation to be enjoyed by the State in any case under Article 8 depends on a number of factors, including the nature of the Convention right in issue, its importance for the person concerned, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights. Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted (see *S. and Marper*, cited above, § 102, with further references). A heightened level of protection is also required for sensitive personal data (see *Catt v. the United Kingdom*, no. 43514/15, § 112, 24 January 2019, and *Glukhin v. Russia*, no. 11519/20, § 76, 4 July 2023).

163. The Court is aware of the different approaches to the margin of appreciation applicable to measures which interfere with the Article 8 rights of legal persons. In some cases the Court has held that the fact that the measure was aimed at legal persons meant that a wider margin of appreciation could be applied than would have been the case had it concerned an individual (see, in the context of searches and seizures conducted at business premises, *Bernh Larsen Holding AS and Others*, cited above, § 159; *DELTA PEKÁRNY a.s. v. the Czech Republic*, no. 97/11, § 82, 2 October 2014; *Erduran and Em Export Dış Tic A.Ş. v. Turkey*, nos. 25707/05 and 28614/06, § 99, 20 November 2018; and *Naumenko and SIA Rix Shipping*, cited above, § 51).

On the other hand, in a number of cases the Court did not refer to a wider margin of appreciation in respect of legal entities and applied the same level of scrutiny and safeguards to them as to natural persons (see, in the context of searches and seizures, *Vinci Construction and GTM Génie Civil et Services v. France*, nos. 63629/10 and 60567/10, 2 April 2015; *Société Canal Plus and Others*, cited above; *Lindstrand Partners Advokatbyrå AB v. Sweden*, no. 18700/09, 20 December 2016; and *UAB Kesko Senukai Lithuania*, cited above; see also, in the context of the interception of communications, *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008; *Association for European Integration and Human Rights and Ekimdzhiev*, cited above; *Liblik and Others*, cited above; *Big Brother Watch and Others*, cited above; and *Ekimdzhiev and Others*, cited above). It considers it useful to clarify its approach, before applying it to the present case.

164. The Court finds that the breadth of the margin of appreciation should depend in each case on the content and nature of the data in question rather than on the applicants' physical or legal nature or their status. It will be wider in respect of the collection and processing of business-related data of both companies and individuals (see, *mutatis mutandis*, *Niemietz v. Germany*, 16 December 1992, § 31 *in fine*, Series A no. 251-B), than in the case of the collection and processing of data concerning an individual's intimate sphere or a particularly important facet of an individual's existence or identity (see paragraph 162 above). The breadth of the margin of appreciation will also depend on the gravity of the interference (see, for example, *Big Brother Watch and Others*, cited above, § 339; and *Naumenko and SIA Rix Shipping*, cited above, § 51) and the object pursued by it (see, for example, *Weber and Saravia*, cited above, § 106, and *Big Brother Watch and Others*, cited above, § 338).

165. As regards the applicable safeguards against arbitrariness and abuse, while being mindful of differences that might arise between cases concerning natural and legal persons as a result of the application of data protection laws to the former and the function of the margin of appreciation, the Court finds that the minimum safeguards under Article 8 should in principle be the same.

(b) Application to the present case

(i) Preliminary considerations

166. The Court would begin by noting that the applicant companies have not complained about the lack of legal safeguards concerning the examination, storage, use, onward transmission and destruction of the data after their transmission. Furthermore, they have not complained about the telephone tapping as such. It is not in dispute between the parties that the data were lawfully obtained in the framework of criminal proceedings in which the interception orders had been authorised by the investigating judge. The

Court will accordingly proceed on the basis that the data were lawfully obtained in a manner compatible with Article 8 of the Convention.

167. The Court further observes that in the present case the applicant companies' complaints were based on specific and undisputed instances of transmissions of data obtained through telephone tapping. Therefore, the Court's assessment of the applicable safeguards, although it necessarily entails some degree of abstraction, cannot be of the same level of generality as in cases concerning general complaints about a law permitting the secret surveillance of communications and in which the Court must, of necessity and by way of exception to its normal approach, carry out an abstract assessment of such a law. 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 applicants in the particular circumstances (see *Goranova-Karaeneva v. Bulgaria*, no. 12739/05, § 48, 8 March 2011; *Dragojević*, cited above, § 86; and *Zubkov and Others v. Russia*, nos. 29431/05 and 2 others, § 126, 7 November 2017).

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

(α) Whether there was a legal basis in Dutch law

168. Despite a disagreement between the parties as to the existence of a legal basis for the impugned interference, the Court finds no reason to call into question the view taken by the domestic courts in the instant case that the transmissions of data had a legal basis in section 39f of the WJSG (see paragraphs 31, 46 and 57 above). It reiterates in this connection that its power to review compliance with domestic law is limited, as it is primarily for the national authorities, notably the courts, to interpret and apply domestic law (see *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13, §§ 144 and 147, 27 June 2017).

169. The Court also observes that the present case is to be distinguished from *Dragojević* (cited above) and *Liblik and Others* (cited above), in which the interferences were not "in accordance with the law" because the domestic authorities had not complied with the explicit requirement under domestic law that authorisations be duly reasoned. In the present case, while prosecutors were required by Article 3:4 of the AWB and the WJSG Instructions to assess the necessity and proportionality of the transmissions (see paragraphs 69 and 79 above), they were not required under Dutch law to record their assessment in a written reasoned decision, as data transmission was qualified under domestic law as a "factual act", not as a "decision" within the meaning of the AWB (see paragraphs 64, 70 and 78 above). That interpretation of the domestic law was confirmed by the Supreme Administrative Court for Trade and Industry (see paragraph 31 above). The Court is therefore not convinced by the applicant companies' argument that

the absence of written reasoning in transmission authorisations rendered them unlawful under the domestic law.

(β) Quality of the law

170. For an interference to be "in accordance with the law" it must not only have some basis in domestic law, it must also meet quality requirements: the law must be accessible to the person concerned and foreseeable as to its effects (see paragraph 152 above) The first of these two requirements – the accessibility of the law – does not raise any problem in the instant case.

171. The Court will next examine whether the Dutch law applicable at the material time met the criteria of foreseeability, and in particular whether it sufficiently clearly defined the circumstances in which a transmission of lawfully obtained intercept material to another law-enforcement authority could be authorised (see paragraph 160 above).

172. The transmission of data collected in the framework of a criminal investigation to persons or public authorities for non-criminal justice purposes was governed by the WJSG, and in particular by its section 39f, as in force at the material time (see paragraph 61 above). In so far as relevant to the instant case, it set out the following conditions for transmitting data: (i) the transmission had to concern "criminal data" within the meaning of section 1(b) of the WJSG; (ii) it was permitted for an exhaustive list of purposes, including the "enforcement of legislation"; (iii) the transmission had to be necessary in view of a compelling general interest.

173. Additional information regarding the application of section 39f of the WJSG could be found in the WJSG Instructions (see paragraphs 67-70 above). The WJSG Instructions in force at the material time provided, among other points, guidance as to the application of a necessity and proportionality test, an open-ended list of potential recipients of data and information about applicable remedies. Furthermore, the legislative history provides guidance regarding the interpretation of the concept of "criminal data" and the requirement of "a compelling general interest", linking it to the legitimate aims listed in Article 8 § 2 of the Convention, and indicates which factors the Public Prosecution Service must take into account when assessing whether the compelling general interest requires the transmission of data (see paragraph 63 above).

174. The Court considers that the relevant domestic law applicable in the applicant companies' case defined with sufficient clarity the circumstances in which a transmission of lawfully obtained intercept material to another law-enforcement authority could be authorised. It is true that the WSJG and the WSJG Instructions did not specify the minimum level of gravity of violations of legislation that could justify data transmission. The Court notes, however, that the requirement of the "foreseeability" of a law does not go so far as to compel States to enact legal provisions listing in detail all circumstances that may prompt a decision to transmit data (see,

mutatis mutandis, *Kennedy v. the United Kingdom*, no. 26839/05, § 159, 18 May 2010). Dutch law defined the data which could be transmitted ("criminal data") as well as the permissible purpose (the "enforcement of legislation") and the group of potential recipients. Furthermore, it required a necessity and proportionality assessment linked to a "compelling general interest". It therefore sufficiently clearly defined the nature of the situations in which transmissions could be authorised.

175. The applicant companies argued that the domestic courts' interpretation of the term "criminal data" as covering by-catch data had been unforeseeable. The Court is not persuaded by this argument. It reiterates that the wording of statutes is not always precise, and that the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague. The role of adjudication vested in the national courts is precisely to dissipate such interpretational doubts as may remain. Unless their interpretation is arbitrary or manifestly unreasonable, the Court's role is confined to ascertaining whether the effects of that interpretation are compatible with the Convention (see *NIT S.R.L. v. the Republic of Moldova* [GC], no. 28470/12, §§ 159-60, 5 April 2022, with further references).

176. In the Court's view, it seems reasonably foreseeable from the wording of section 1(b) of the WJSG (see paragraph 61 above) and the legislative history cited by the domestic courts (see paragraphs 31 and 46 above) that by-catch data could be considered criminal data within the meaning of the WJSG. The main criteria for defining "criminal data" under section 1(b) of the WJSG were that the data were (i) obtained in the context of a criminal investigation, and (ii) included in a criminal file or processed by automated means. The domestic courts explained that the transcripts of all the intercepted telephone conversations were considered to be part of the criminal file as they could become relevant at some stage of the criminal proceedings. The courts added that, in any event, they were stored digitally and in that sense were processed by automated means within the meaning of section 1(b) of the WJSG. It also appears from the available evidence that the national courts were consistent in interpreting and applying the relevant term (see paragraph 72 above). In view of the above, the domestic courts' interpretation of the term "criminal data" as covering by-catch data does not appear to have been arbitrary or manifestly unreasonable.

177. As regards the applicant companies' argument that it had not been foreseeable that the NMA could be a recipient of criminal data, it follows from the legislative history that it was the legislature's choice not to include an exhaustive list of recipients in section 39f of the WJSG and to leave the matter to the discretion of the public prosecutor (see paragraph 63 above). The WJSG Instructions indicated that criminal data required for the purpose of the enforcement of legislation could be transmitted to "administrative

bodies". Several examples of such bodies were mentioned (see paragraph 69 above). It is true that the list of examples did not explicitly mention the NMA. It is, however, clear that the NMA was an administrative body charged with the enforcement of the Competition Act. The Court also agrees with the Chamber that, contrary to what the applicant companies suggested, the authorisation to receive criminal data was not made dependent in the domestic law on the investigative powers of the receiving entity. As pointed out by the Supreme Administrative Court for Trade and Industry, the WJSG precisely provided for the possibility, under certain conditions, that data obtained through coercive measures in criminal proceedings could be transmitted to other public authorities that did not themselves have the power to use such coercive measures (see paragraph 31 above). In view of the above, the Court is satisfied that the domestic legal provisions made it reasonably foreseeable that the NMA could lawfully receive criminal data.

178. In view of the foregoing, the Court finds that the domestic law sufficiently clearly defined the circumstances in which the transmission of lawfully obtained intercept material to another law-enforcement authority could be authorised.

179. Lastly, the applicant companies complained that the NMA's prior access to certain data and its provision of search terms in order to select data had been unforeseeable. In this respect, the Court observes that in the Janssen companies' case, prior to the prosecutor's transmission authorisation, the NMA was given access, on police premises and in strict confidence, to a selection of transcripts of intercepted telephone conversations. A CD was also sent to the NMA containing selected audio-recordings of about thirty conversations for information purposes only and in strict confidence, with an explicit ban on their use for any other purpose, before the transmission of data was authorised (see paragraphs 37-38 above). Furthermore, in the cases of all the applicant companies, the NMA provided the police and the VROM-IOD with lists of search terms to examine the entire criminal files, as a result of which additional material was transmitted to the NMA (see paragraphs 19 and 41 above). The Court notes in this connection that the domestic law required the prosecutor to assess the necessity and proportionality of the envisaged transmission (see paragraph 69 above). The Court considers that it was reasonably foreseeable that, in order to assess the necessity and proportionality of the transmission as required by law, the prosecutor might need to consult with the authority competent to enforce competition law, that is the NMA, in order to identify the relevant data. There is no indication that any entity other than the Public Prosecution Service had control over the selection of the data which the NMA accessed or that the NMA accessed more information than was necessary for the authorised purpose. By helping to ensure that the transmissions of data were more targeted and that only the amount of information needed for the recipient to perform its duties was transmitted, prior consultation could therefore be considered as a reasonable

and foreseeable stage of the proportionality and necessity assessment required by the domestic law. Moreover, as established by the Supreme Administrative Court for Trade and Industry in the Janssen companies' case (see paragraph 57 above), those consultations did not affect the lawfulness of the transmission of data that took place on a later date in conformity with the requirements set out in the WJSG and the WJSG Instructions.

180. In the light of the above, the Court concludes that the relevant domestic law applicable in the applicant companies' cases fulfilled the requirements of "foreseeability" under Article 8 § 2 of the Convention.

(iii) Whether the interference pursued a legitimate aim

181. The Government argued that the data transmissions had served the legitimate aim of protecting the economic well-being of the country, which the applicant companies did not dispute. 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"

182. The Court will first assess whether the authorisation procedures and available remedies afforded the applicant companies adequate and effective safeguards against arbitrariness and abuse (see paragraphs 158 and 161 above).

183. The Court is not convinced by the applicant companies' argument that the authorisation procedures were deficient because the transmission authorisations had been granted by a prosecutor who could not be deemed an independent body. An independent *ex ante* authorisation for transmissions of intercept material lawfully obtained in a Convention-compliant manner to another law-enforcement authority is not required by Article 8. Authorisation of such transmissions by a non-judicial authority may be compatible with the Convention. Where there is extensive *post factum* judicial or otherwise independent oversight, this may counterbalance the absence of an independent authorisation (see, in the context of secret surveillance, *Szabó and Vissy v. Hungary*, no. 37138/14, § 77, 12 January 2016).

184. The Court notes in this connection that it has previously found no violation of Article 8 in cases where transmissions of intercept data had been authorised by prosecutors (see *Versini-Campinchi and Crasnianski*, cited above, § 12; *Drakšas*, cited above, § 61; *Adomaitis*, cited above, § 10; and *Starkevič*, cited above, § 21; see also *Terrazzoni*, cited above, § 22, in which the transmission was authorised by the Minister of Justice (*le garde des Sceaux*); see also the comparative-law material summarised in paragraph 104 above).

185. Given that the intercept material in the present case had been collected on the basis of a judicial authorisation and in a Convention-compliant manner, it was not incompatible with the Convention for the authorisation to transmit that material to another law-enforcement authority to be granted by the prosecutor. What is more important is whether the domestic system of review of data transmissions as a whole provided the applicant companies with adequate safeguards against arbitrariness and abuse and was capable of restricting the contested transmissions to what was "necessary in a democratic society".

186. As regards the applicant companies' complaint about the absence of prior notice for the data transmission, the Court has previously held, in the context of telephone tapping, that when the secret-surveillance measures are first ordered and while they are being carried out, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. In that sense, Article 8 of the Convention does not guarantee the right to a prior notification about secret surveillance (see *Klass and Others v. Germany*, 6 September 1978, §§ 55 and 68, Series A no. 28, and *Roman Zakharov*, cited above, § 286). The same applies to the transmission of intercept material when the secrecy of the transmitted data is of importance for the original criminal proceedings or for the new proceedings for the purposes of which the data are being transmitted. Article 8 cannot be construed as guaranteeing prior notification about the transmission of intercept material (see, *mutatis mutandis*, *Othymia Investments B.V. v. the Netherlands* (dec.), no. 75292/10, § 44, 16 June 2015, in the context of the transmission of tax-related information to another State) or, by implication, the possibility to participate in any review prior to the data being transmitted.

187. The Court observes that the "Cleveland" criminal investigation was still ongoing at the time of the contested data transmissions and the telephone tapping was apparently still being kept secret from the persons concerned. Notifications could thus have undermined the criminal investigation, the success of covert investigative measures and an investigation of the Janssen companies by the NMA. Therefore, the Court accepts that, in the circumstances of the present case, the transmissions of the data had to take place without the Janssen companies' prior knowledge. The fact that the Janssen companies were unable to take part in the authorisation proceedings or apply for a preventive remedy in another form did not therefore, in the circumstances of the case, entail a breach of Article 8.

188. As regards the "Toto" investigation, the suspects learned about the criminal proceedings against them and presumably about the use of telephone tapping on 19 December 2008 (see paragraph 20 above). Any prior notifications about transmissions that took place after that date would no longer have undermined the criminal investigation or the success of the covert investigative measures. Moreover, on 29 June 2010 the Ships Waste Oil

Collector B.V. company and the I. company learned about the competition proceedings and the previous transmissions of data (see paragraph 18 above). It is unclear why the subsequent data transmissions were carried out in secret and in what way prior notice about them would have hampered the competition proceedings. The Court finds it regrettable that Ships Waste Oil Collector B.V., Burando Holding B.V. and Port Invest B.V. were not given prior notice about the transmissions that took place after 29 June 2010 and were therefore unable to have their arguments against those transmissions heard in the framework of an *ex ante* review. However, the Court will ascertain below whether they were given a sufficient opportunity to have their arguments heard during the *ex post facto* review.

189. The Court notes the absence of any reasoning in the transmission authorisations, which did not contain any verifiable assessment of whether the transmissions were "necessary in a democratic society", including whether they were proportionate to the legitimate aim pursued. The Court considers that written reasoning, even if a succinct one, is desirable to ensure that the authorising authority has properly assessed the necessity and proportionality of the interference with Article 8 rights (see, in the context of interception of communications, *Ekimdzhiev and Others*, cited above, § 313) and to facilitate an effective review of the transmission for the purposes of Article 8 § 2 of the Convention (see, also in the context of interception of communications, *Potoczká and Adamčo v. Slovakia*, no. 7286/16, § 76, 12 January 2023). Nevertheless, as the transmitted material was the product of lawful telephone tapping authorised by a court, the safeguards applicable to the process of obtaining the intercept data limited the risk of arbitrariness and abuse related to the transmissions of those data (see paragraph 154 above). In such circumstances the lack of reasoning may be compensated for by *ex post facto* review.

190. It is important to note that the applicant companies eventually learned about the data transmissions and were able to use judicial *ex post facto* remedies. It follows that, in the specific circumstances of the case, the assessment of the effectiveness of the remedies available under domestic law must be carried out without taking into account the initially secret nature of the transmissions (compare *Gernelle and S.A. Société d'Exploitation de l'Hebdomadaire Le Point v. France* (dec.), no. 18536/18, § 49, 9 April 2024).

191. The applicant companies challenged the lawfulness and Convention-compliance of the data transmissions in the administrative proceedings concerning the NMA's decisions to impose fines on them. The scope of review of the domestic courts in those proceedings was not limited to the admissibility of the intercept material in evidence. The courts examined whether the transmissions had been lawful – which included the necessity and proportionality test as part of the lawfulness assessment – and also whether they complied with Article 8 of the Convention (see paragraphs 31 and 57 above). The remedy used by the applicant companies was therefore

able to deal with the substance of the Convention complaint that the interference was not "in accordance with the law" or "necessary in a democratic society" (compare *Capriotti v. Italy* (dec.), no. 28819/12, §§ 56-57, 23 February 2016, and *Gernelle and S.A. Société d'Exploitation de l'Hebdomadaire Le Point*, cited above, §§ 44 and 51; contrast *Zubkov and Others*, cited above, §§ 88 and 95-98, with further references; *Potoczká and Adamčo*, cited above, § 61; and *Plechlo v. Slovakia*, no. 18593/19, § 46, 26 October 2023; see also, in the context of Article 13, *Khan v. the United Kingdom*, no. 35394/97, § 44, ECHR 2000-V, and *P.G. and J.H. v. the United Kingdom*, no. 44787/98, § 86, ECHR 2001-IX).

192. As follows from the Dutch Supreme Court's case-law in civil proceedings, the lawfulness of the "factual act" of transmission did not depend on the reasons given by the prosecutor at the time. The assessment of the lawfulness of a "factual act" could be carried out by the reviewing court retrospectively and independently (see paragraphs 71-72 above). In the present case, the Supreme Administrative Court for Trade and Industry applied the same approach, finding that it was not necessary to have the prosecutor's reasoning and carrying out its own *de novo* assessment of whether the transmissions had been lawful and compatible with the Convention (see paragraph 31 and 57 above). The Court concludes that in the circumstances of the present case, the absence of written reasoned transmission authorisations was compensated for by an *ex post facto* review in the judicial proceedings challenging the administrative fines in which the applicant companies were given an opportunity to effectively contest the transmission of data.

193. Furthermore, the Court has no reason to doubt that those proceedings were capable of affording the applicant companies appropriate redress. It reiterates that it has generally considered the appropriateness of the redress to be dependent on all the circumstances of the case, having regard, in particular, to the nature of the Convention violation at stake (see *Gäfgen v. Germany* [GC], no. 22978/05, § 116, ECHR 2010). In previous cases concerning the transmission of intercept material, the Court found that applicants who had been able to contest the admissibility of the transmitted material as evidence in disciplinary proceedings had obtained an effective judicial review. It thereby implicitly accepted that the exclusion of evidence resulting from an inadmissibility challenge could afford adequate redress (see *Versini-Campinchi and Crasnianski*, cited above, §§ 71-74; *Terrazzoni*, cited above, §§ 60-61; and *Adomaitis*, cited above, §§ 87-88). In the Court's view, redress in the form of the destruction of transmitted data or monetary compensation is not necessarily required for a remedy concerning the transmission of intercept data; restrictions on their use, such as a declaration of inadmissibility as evidence, may afford sufficient redress for such transmissions.

194. The Court further observes that it was also open to the applicant companies to challenge the transmissions in civil proceedings under Article 6:162 of the Civil Code (see paragraph 87 above), either in substantive proceedings (*bodemprocedure*) or in proceedings under Article 254 of the Code of Civil Procedure before the provisional-measures judge (see paragraph 88 above). It is clear from the WJSG Instructions that the civil courts were designated and entrusted with the competence to rule on the lawfulness of data transmissions in tort proceedings (see paragraph 70 above). This also follows from the legislative history of the WJSG (see paragraph 65 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 Court is not convinced by the applicant companies' arguments that the civil proceedings could not have provided a sufficiently thorough review and is therefore not satisfied by their explanation of why they did not use this remedy. In the provisional-measures proceedings initiated by the Janssen companies – which they did not however pursue on appeal – the judge assessed both the domestic lawfulness of the transmissions and their compliance with Article 8 of the Convention, in particular by verifying the existence of a compelling general interest and by balancing it against the applicant companies' rights (see paragraph 46 above). The Court therefore has no reason to doubt that the civil remedy, if it had been pursued by the applicant companies, would have been capable of dealing with the substance of their Convention complaint by examining whether the interference had been lawful and proportionate to a compelling general interest, and of providing redress in the form of damages or injunctions. For the reasons explained in paragraph 192 above, the lack of written reasoning in the transmission authorisations could not undermine the effectiveness of the civil remedy in the circumstances of the case (see the Supreme Court's case-law in civil proceedings in paragraphs 71-72 above). In that connection, the Court notes that the Convention forms part of domestic law and that it takes precedence over domestic statutory rules in the event of a conflict (see paragraph 60 above).

195. In view of the above, while the transmission authorisations did not contain any reasons, the Court considers that this was compensated for by a *de novo* assessment of the transmissions' lawfulness and their "necessity in a democratic society" by the courts which carried out the *ex post facto* review (see paragraph 192 above). The applicant companies have not convincingly shown that that review was ineffective. The domestic system of review of data transmissions as a whole therefore afforded the applicant companies adequate safeguards against arbitrariness and abuse, providing for an opportunity to effectively contest the transmissions of intercept material and safeguarding their rights.

196. Lastly, as regards the existence of relevant and sufficient reasons justifying the data transmissions in the present case, the Court reiterates that,

in accordance with the principle of subsidiarity, the national authorities have the primary responsibility to secure the rights and freedoms defined in the Convention, and that in so doing they enjoy a margin of appreciation, subject to the Court's supervisory jurisdiction (see, for example, *Verein KlimaSeniorinnen Schweiz and Others v. Switzerland* [GC], no. 53600/20, § 541, 9 April 2024). In assessing whether the national authorities remained within their margin of appreciation in this respect, the Court will take into account the nature of the data, the importance of the aim pursued by their transmission and the resulting consequences for the applicants (see paragraphs 161 and 164 above).

197. The Court agrees with the domestic courts that there is strong public interest involved in the effective enforcement of competition law (see *SA-Capital Oy*, cited above, § 78). Given the potential negative impact of cartels on market competition and the difficulties involved in detecting and investigating them, it is important that competition authorities and other law-enforcement agencies be able to cooperate in their efforts to uncover and punish such anti-competitive practices. The enforcement of competition law is crucial to safeguarding the performance capacity and fairness of market economies, and, consequently, the economic well-being of the country.

198. The Court notes that the violations of competition law revealed by the intercept material were undoubtedly serious and, in view of the applicant companies' high market share and the systematic and repeated nature of those violations, could lead to significant damage (see paragraphs 28 and 52 above). The Court has previously classified similar administrative competition proceedings as "criminal" within the autonomous meaning of Article 6 of the Convention, in view of the nature of the offence and the nature and severity of the sanction (see, for example, *A. Menarini Diagnostics S.R.L. v. Italy*, no. 43509/08, §§ 39-45, 27 September 2011).

199. Furthermore, as regards the intrusiveness of the interference, while the sanctions imposed on the applicants were serious, there is no reason to doubt, and it was not contested by the applicant companies, that the data transmissions were limited to material relevant for the competition proceedings. Furthermore, the transmitted material exclusively concerned the business activities of legal persons; it did not contain any data which could be considered sensitive.

200. In view of the above, and noting that domestic authorities carefully assessed the lawfulness of the transmission under the WJSG 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 31, 46 and 57 above), the Court is satisfied that the domestic authorities advanced relevant and sufficient reasons to justify the necessity and proportionality of the data transmission for the purposes of enforcement of competition law.

The respondent State thus remained within the margin of appreciation afforded to it.

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

III. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

202. The applicant companies complained that they had not had access to an effective remedy for their complaint under Article 8. They relied on 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."

203. Relying on its findings under Article 8, the Chamber found that the applicant companies had had effective remedies at their disposal for their complaints under that Convention provision.

204. The applicant companies complained that they had been deprived of an effective remedy because they had not been notified of the data transmissions beforehand, and that they had not had access to *ex ante* judicial review. The available *ex post facto* judicial review had also proved to be ineffective.

205. The Government submitted that Article 13 of the Convention did not guarantee a right to be notified or a right to a preventive remedy. The applicant companies had had effective remedies at their disposal in civil and administrative proceedings.

206. In the light of its considerations and findings under Article 8 of the Convention (see paragraphs 186-195 above), the Court finds that the applicant companies had an effective remedy at their disposal to raise their complaints under that provision.

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

FOR THIS REASON, THE COURT

1. *Decides*, unanimously, to join the applications;

2. *Holds*, by twelve votes to five, that there has been no violation of Article 8 of the Convention in respect of Ships Waste Oil Collector B.V., Burando Holding B.V. and Port Invest B.V.;

3. *Holds*, by ten votes to seven, that there has been no violation of Article 8 of the Convention in respect of Janssen de Jong Groep B.V., Janssen de Jong Infra B.V. and Janssen de Jong Infrastructuur Nederland B.V;

4. *Holds*, by fifteen votes to two, that there has been no violation of Article 13 of the Convention in respect of all applicant companies.

Done in English and in French, and delivered at a public hearing in the Human Rights Building, Strasbourg, on 1 April 2025, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Johan Callewaert	Marko Bošnjak
Deputy to the Registrar	President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

(a) Joint partly dissenting, partly concurring opinion of Judges Guyomar and Ravarani;
(b) Joint partly dissenting opinion of Judges Bosnjak and Derenčinović;
(c) Dissenting opinion of Judge Serghides;
(d) Joint dissenting opinion of Judges Serghides and Arnardóttir;
(e) Dissenting opinion of Judge Arnardóttir, joined by judges Serghides and Šimáčková.

M.B.
J.C.

JOINT PARTLY DISSENTING, PARTLY CONCURRING OPINION OF JUDGES GUYOMAR AND RAVARANI

(Translation)

1. The present judgment examines several applications jointly, having regard to their similar subject matter (see paragraph 106 of the judgment).

2. With regard to the companies Ships Waste Oil Collector B.V., Burando Holding B.V. and Port Invest B. V., we voted with the majority in the Grand Chamber in finding that there had been no violation of Article 8 of the Convention (see point 2 of the operative part of the judgment). Our views are accurately reflected in the three steps of the judgment's reasoning leading to that conclusion: whether the impugned interference was in accordance with the law, whether it pursued a legitimate aim and whether it was "necessary in a democratic society".

3. However, regarding the companies Janssen de Jong Groep B.V., Janssen de Jong Infra B.V. and Janssen de Jong Infrastructuur B. V., we were unable to vote with the majority, since we consider that there has been a violation of Article 8 of the Convention (see point 3 of the operative part of the judgment).

4. We feel it is necessary to explain our position briefly. It is rooted in the circumstances of the case, which differ from one set of applications to the other. Thus, as paragraph 167 of the judgment saliently points out, the Court's examination in the present case concerned "specific ... instances of transmissions of data obtained through telephone tapping", which did not involve an abstract assessment of the applicable legislation but rather an examination of the "manner in which it was applied to the applicants in the particular circumstances".

5. The judgment rightly presents the circumstances of the case successively, starting with the "first group of applicant companies" followed by the other applicant companies (application no. 2800/16). Regarding the latter, the initial situation was similar to that of the first group: in the context of a criminal investigation, some of the telephone conversations of the Janssen companies' employees were intercepted in accordance with interception orders authorised by an investigating judge (see paragraphs 35-36). Some of the intercept data, which contained indications of price-fixing, were identified as being of potential interest to the Netherlands Competition Authority ("NMA", succeeded by the Consumer Market Authority, or "ACM"), which, on 9 December 2008, opened an official investigation into suspected violations of the Competition Act and requested authorisation to use the data. Authorisation was granted by the public prosecutor in charge of the criminal investigation on 16 December 2008 (see paragraphs 39-40). The particularity of this case lies in the events

that unfolded prior to this authorisation, which are set out in paragraphs 37-38 of the judgment: in July 2008 police officers gave NMA officials access, in confidence, to a selection of transcripts of the intercepted communications; the police also granted the NMA's request for access to other transcripts; in August 2008 the public prosecutor in charge of the investigation provided a CD to the NMA containing audio recordings of about thirty of the intercepted telephone conversations "for information purposes only and in strict confidence", indicating that they should not "be used for any other purpose except with his permission".

6. In our view, the granting of such access, prior to any authorisation for the transmission and use of the intercept data, was clearly devoid of any legal basis and irreparably vitiated the remainder of the proceedings in question. In other words, we respectfully but resolutely disagree with the majority's assessment concerning the first step of the examination (lawfulness of the interference). Such a finding is a necessary and sufficient condition for the conclusion that there has been a violation of Article 8 of the Convention in respect of the Janssen companies, leaving intact the next two steps of the reasoning, which are common to both sets of applications (legitimate aim and necessity of the interference).

7. When exercising its scrutiny of the "quality of law" requirement, the Court normally proceeds by seeking to ascertain whether the interference complained of was "in accordance with the law", in other words, whether it had a basis in domestic law and, if so, whether this basis was accessible to the applicant and foreseeable in its effects.

8. Like the majority, we are of the view that "the domestic law sufficiently clearly defined the circumstances in which the transmission of lawfully obtained intercept material to another law-enforcement authority could be authorised" (see paragraph 178), which explains our vote with regard to the first group of applicant companies.

9. However, we reject this conclusion as regards the NMA's access to some of the intercept data concerning the Janssen companies prior to the transmission authorisation by the Public Prosecution Service.

10. This particular issue is expressly dealt with in paragraph 179 of the judgment, as follows:

> "...The Court notes in this connection that the domestic law required the prosecutor to assess the necessity and proportionality of the envisaged transmission (see paragraph 69 above). The Court considers that it was reasonably foreseeable that, in order to assess the necessity and proportionality of the transmission as required by law, the prosecutor might need to consult with the authority competent to enforce competition law, that is the NMA, in order to identify the relevant data. There is no indication that any entity other than the Public Prosecution Service had control over the selection of the data which the NMA accessed or that the NMA accessed more information than was necessary for the authorised purpose. By helping to ensure that the transmissions of data were more targeted and that only the amount of information needed for the recipient to perform its duties was transmitted, prior consultation could

> therefore be considered as a reasonable and foreseeable stage of the proportionality and necessity assessment required by the domestic law. Moreover, as established by the Supreme Administrative Court for Trade and Industry in the Janssen companies' case (see paragraph 57 above), those consultations did not affect the lawfulness of the transmission of data that took place on a later date in conformity with the requirements set out in the WJSG and the WJSG Instructions."

11. In our view, none of the reasons advanced in that paragraph to set aside the complaint that the prior consultations were not "in accordance with the law" is convincing.

12. Firstly, as much as we endorse the reasoning contained in paragraphs 172-174 of the judgment leading to the conclusion, concerning section 39f of the WJSG, that "the domestic legal provisions made it reasonably foreseeable that the NMA could lawfully receive criminal data" (see paragraph 177), we are not prepared to accept that there existed a form of "cascading foreseeability", on which the following step of the argument relies.

13. Indeed, the majority infer from the foreseeability of the transmission of criminal data that exploratory interactions prior to any transmission authorisation were themselves foreseeable, based on the fact that the Public Prosecution Service – the authority empowered to give such authorisation – was required to assess the necessity and proportionality of the transmission. Even though the principle of such prior access is not laid down in any provision of domestic law, the judgment accepts that it was foreseeable on the sole ground that it supposedly contributed to a more rigorous and therefore more reasonable selection of data for transmission. It seems to us that, in turning a duty (obligation to ensure the necessity and proportionality of the transmission of data) into a prerogative (power to give unauthorised access to intercept data), the judgment strays from the Court's previous case-law on the "quality of law" requirements. While the prior consultations could be regarded as "reasonable" in the light of their purpose, it was not "foreseeable" that the authorisation of any transmission of data would, implicitly but necessarily, be coupled with prior access to the data in question. The fact that certain measures might generally be useful and reasonable is not sufficient to render them *ipso facto* lawful. The argument verges on paradox by accepting the principle of informal, unlimited access to intercept data by the NMA on the ground that such access might then help to restrict the scope of the data which the very same NMA is to be formally authorised to access. As to there being "no indication that any entity other than the Public Prosecution Service had control over the selection of the data which the NMA accessed", this is completely irrelevant to the issue under consideration.

14. The obligation to assess the proportionality and necessity of the transmission of data, a requirement provided for by law, cannot, in our view, lead us to accept that the exploratory interactions in question constitute a "reasonable and foreseeable" stage of that assessment. The principle of minimising transmitted data is essential to ensuring compliance with Article 8

of the Convention. In our view, however, it should apply after formal authorisation by the Public Prosecution Service rather than serving to justify prior access afforded in practice, outside of any legal framework and any safeguards.

15. Nor are we persuaded by the second reason given in the judgment. Relying on the findings reached by the Supreme Administrative Court for Trade and Industry in its judgment of 9 July 2015, the majority in the Grand Chamber note that the exploratory interactions did not affect the lawfulness of the transmission of data that took place on a later date. We would note in passing that, in the light of the first line of argument, it would have been more consistent to go so far as to assert that this prior access, being a "reasonable" measure, had actually contributed to the lawfulness of the transmission in question. Be that as it may, let us return to the reasoning of the judgment of 9 July 2015, endorsed by the Court (see paragraph 57):

> "Contrary to the argument made by [the Janssen companies], the circumstance that the ACM had access to the large amount of data 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 in breach of the WJSG."

In our view, the fact that the NMA was given prior access to vast swathes of intercept data irreparably vitiated the proceedings in question to the extent that they relied on the use of the data thereby accessed; that their use was subsequently authorised is neither here nor there. Once it is established that the NMA gained prior access to the data, with no basis in law and no procedural safeguards as to their use at that stage, the Public Prosecution Service's subsequent transmission authorisation for part of the data cannot be regarded as having expunged the infringement of Article 8 earlier in the proceedings, which tainted their outcome. On this point we are very largely in agreement with the arguments made in paragraphs 10 and 11 of the dissenting opinion of our colleague Judge Arnardóttir, joined by Judges Serghides and Šimáčková.

16. The NMA enjoyed access to the intercept data from July and August 2008, well before an official investigation was opened, on 9 December 2008, into possible violations of the Competition Act, suspicion of which was fuelled by the telephone conversations thereby brought to its attention, followed by the request for authorisation to use part of them. Having regard to the potential impact on the ensuing proceedings that followed and absent any procedural safeguards surrounding such informal access, the authorisation subsequently granted by the Public Prosecution Service could not remedy, by a kind of retroactive neutralisation, the resulting interference with Article 8 of the Convention, which was not in accordance with the law.

17. We are convinced of the importance of cooperation between the various public authorities when it comes to the legitimate protection of the States' economic well-being and the need to safeguard the effectiveness of

that protection, in particular in the context of competition law and in the face of powerful private economic interests. Taking account of these considerations may justify substantial interference with the rights of companies under Article 8 of the Convention, provided it is regulated in such a manner that it remains compatible with the requirements that the Court's case-law has attached to effective compliance with that Article. This was the case, in our opinion, regarding the first group of applicant companies. But the same considerations cannot lead us to accept that informal, unsupervised and unverifiable practices should be allowed to piggy-back on procedures that are in accordance with the law and surrounded by adequate and effective safeguards against abuse and arbitrariness. For this reason, we voted in favour of finding a violation of Article 8 of the Convention in respect of the second group, the Janssen companies.

JOINT PARTLY DISSENTING OPINION OF JUDGES BOŠNJAK AND DERENČINOVIĆ

1. We agree with the conclusion that there had been no violation of Article 13 in this case. However, we respectfully disagree with the majority finding that there has been no violation of Article 8 of the Convention and also agree with most of the well-structured views and conclusions expressed in the dissenting opinion of Judge Arnardóttir, joined by Judges Serghides and Šimačkova. They are right about the shortcomings of the majority's decision with regard to the proportionality assessment. We share their view that "the transmission of intercept criminal data for purposes unrelated to the original purpose of the interception can only be justified in pursuit of weighty interests" (see paragraph 3 of the Dissenting Opinion of Judge Arnardóttir, joined by Judges Serghides and Šimačkova) and that "the discretion conferred by Dutch law on the competent authorities to transmit intercept criminal data for use in pursuit of unrelated purposes is too broad to guard against arbitrary interference and abuse of power" (ibid., paragraph 8). We also support their critique of the lack of reasoned decisions on the transmission of data, data-sharing prior to official transmission and the insufficiency of ex post facto or retrospective judicial authorisation. However, there are additional elements – for instance, the purpose-based approach, the question of lawfulness and the rights of those who were not formally subject to interception in the criminal proceedings – which we would like to develop further from the perspective of the most fundamental principles of contemporary criminal law and procedural guarantees. We believe that these elements were not sufficiently taken into account by the majority when identifying safeguards against abuse.

2. At the outset, we wish to emphasise the general importance of data-sharing arrangements between law-enforcement agencies. Such an arrangement is not only to be regarded as best practice but also as a practical imperative in the context of combatting the most serious forms of organised crime and terrorism. There should be no doubt whatsoever that preventing terrorism, for instance, will certainly require a prompt and smooth exchange of relevant data in the form of their transmission not only between law-enforcement agencies but also between the latter and the intelligence services. It would be difficult not to justify the transmission of such data for the purposes of preventing an imminent terrorist attack in "ticking time-bomb" scenarios, for instance. However, such data-sharing arrangements should be subject to strict procedural and substantive safeguards. This is particularly relevant in the context of interference with the rights and freedoms protected by both the Dutch Constitution and the Convention. In this regard, we note that phone-tapping is considered a special means of obtaining evidence in the case of serious crimes. The threshold for

applying such measures in the Dutch legal system is based on the severity of the penalty that can be imposed on the perpetrator in the event of conviction (four years' imprisonment; see paragraph 81 of the judgment). Given the intrinsic nature of such measures, which seriously interfere with constitutional and Convention rights and freedoms (intrusiveness), their application in most legal systems is subject to strict judicial scrutiny (oversight). In comparative legal systems such measures should always be subsidiary in nature and applied only if relevant information cannot be obtained in any other way (subsidiarity). Likewise, their application should be limited in time, be subject to periodic review and be based on a reasoned decision.

3. As a consequence of strict formal requirements and conditions for the interception of criminal data, the domestic legislation should also provide for effective safeguards – drafted and interpreted in a clear and unequivocal manner – against any circumvention, through their subsequent transmission, of the purpose and procedures pertaining to the initial collection (interception) of data. The absence of such safeguards would undermine otherwise robust guarantees as applied in the context of criminal proceedings, to the detriment of the protected human rights of data subjects. The domestic legislation in the present case is couched in vague language and allows for the transmission of data for some purposes/objectives that are prima facie incompatible with those required for their interception. In our view, effective safeguards against abuse should include, at the legislative level, a clear delineation of the purposes for which the transmission of intercept data may be authorised, ensuring that any such purpose will necessarily involve particularly weighty interests, thereby reflecting the seriousness of the resulting interference. In this regard, we consider that it should be next to impossible to justify, for instance, the transmission of criminal data for the purposes of disciplinary proceedings, or the carrying out of a private-law legal act by a person or entity assigned a public task, as the domestic legislation currently provides (see paragraph 61 of the judgment). This defective piece of legislation is coupled with broad discretionary powers conferred on the prosecution authorities, who are not asked to provide even succinct reasoning in their decisions to transmit data to other law-enforcement authorities. The combination of vague and overly broad legislation with wide discretion in its application creates a real risk of arbitrariness – a risk which was materialised in this case.

4. The absence of necessary safeguards becomes particularly problematic when one considers those data subjects which were not targeted by the initial interference but whose rights were subsequently interfered with when their data was transmitted as "by-catch information". This is what happened in the case of the Ships Waste Oil Collector B.V. company, which was not suspected of committing any criminal offence in the "Toto" investigation but ultimately was heavily fined in another set of proceedings, namely for

price-fixing. Given that the potential scope of the second interference is, in fact, unlimited, there is a genuine risk that the circumvention of lawful purposes and procedures could affect even those legal and natural persons that were not in any way targeted by the primary interference. This risk is exacerbated by the fact that, in accordance with the Dutch legislation and its application in the present case, the transmission of intercept data is allowed for purposes that have nothing to do with the very high, purpose-based threshold required for the primary interference.

5. Finally, we can agree with the majority that the market competition infringements "revealed by the intercept material were undoubtedly serious and, in view of the applicant companies' high market share and the systematic and repeated nature of those violations, could lead to significant damage" (see paragraph 198 of the judgment). However, we are strongly opposed to using the argument "that the Court has previously classified similar administrative competition proceedings as 'criminal' within the autonomous meaning of Article 6 of the Convention, in view of the nature of the offence and the nature and severity of the sanction" (ibid.), to the detriment of the applicants. This is in clear contradiction with the very purpose of subsuming the facts of the case under the "protective" ambit of the criminal limb of Article 6. The purpose of this exercise is not to convert certain conduct on the part of an applicant into a criminal offence and/or to prove its criminal character but rather to provide for the protection of procedural rights enshrined in fair trial guarantees in the context of criminal proceedings. The way it has been done in this case is obviously mistaken and contradicts the logic of the protection afforded by Article 6 of the Convention.

DISSENTING OPINION OF JUDGE SERGHIDES

I. INTRODUCTION

1. The applicant companies complained under Articles 8 and 13 of the Convention about the transmission to the Competition Authority of the 'by-catch' data obtained when lawfully intercepting data in the context of a criminal investigation. They contended that the transmission of these data for use by the Competition Authority in administrative proceedings concerning price-fixing had not been foreseeable and that the existing safeguards were insufficient. The main issues raised by this case are the level of protection of legal persons, compared with that of natural persons, and the safeguards called for under Article 8 in respect of the *transmission* of such data, as opposed to their *interception*. In particular, as regards the former, the issues raised are: the required level of detail of provisions authorising the transmission of intercepted data, including on the purposes for which such a transmission may be justified; whether an *ex ante* authorisation of such a transmission is required, in addition to an *ex post facto* judicial review on the merits, and, if so, whether that authorisation should be reasoned and given in writing; whether there is a legal basis for the prior access to the intercepted data which was given to the administrative authority by the public prosecutor before the transmission of the data; and whether the *ex post facto* review has to be of a judicial nature to be effective.

2. While I agree with point 1 of the operative provisions of the judgment to join the applications, I respectfully disagree with all the other points (namely points 2-4) of the operative provisions of the judgment, that is, the substantive ones. In particular, I disagree with point 2 that there has been no violation of Article 8 of the Convention in respect of Ships Waste Oil Collector B.V., Burando Holding B.V. and Port Invest B.V.; with point 3 that there has been no violation of Article 8 of the Convention in respect of Janssen de Jong Groep B.V., Janssen de Jong Infra B.V. and Janssen de Jong Infrastructuur Nederland B.V; and, lastly, with point 4 that there has been no violation of Article 13 of the Convention in respect of all of the applicant companies.

II. APPLICANT COMPANIES' LOCUS STANDI AND ITS LEGAL BASIS

3. The judgment does not explain the legal basis of the applicant companies' *locus standi*; in other words, it does not elaborate on why the applicant companies' claims are admissible *ratione personae* enabling them to bring an individual application before this Court. Hence, I will first proceed by addressing this issue.

A. Positions of the parties at the oral hearing as regards the companies' victim status

4. During the Grand Chamber hearing, I put the following questions to both parties. Referring to the Court's case-law, which has found breaches of legal persons' rights under Articles 6 and 8, among others, I asked whether legal persons had victim status and, if so, on what legal basis. I also asked for clarification on the victim status of legal persons in relation to other Articles of the Convention, like Article 2, the right to life, or Article 3, the right not to be subjected to torture or inhuman or degrading treatment or punishment: if legal persons could not be victims under those Articles, what was the basis for the distinction? I concluded by asking more broadly whether according to Articles 32 and 34, the jurisdiction of the Court *ratione personae* covered legal persons.

5. The applicants' lawyer answered by referring to the Chamber judgment in the case of *Ships Waste Oil Collector B.V. v. the Netherlands* (no. 2799/1616 May 2023), stating that, in it, the Chamber had explained and accepted that companies could rely on their rights under Article 8 in relation to the transmission of data obtained by intercepting telecommunications and their use by other authorities. The lawyer was likely referring to paragraph 41 of that judgment, which briefly addresses the rights of legal persons. The Chamber refers to the Court's case-law to assert that legal persons may claim the rights to respect of their business premises and correspondence under Article 8, and that the transmission of telecommunications data and their use by other authorities could constitute a separate interference with Article 8 rights.

6. The Government's lawyer answered that in the Government's opinion, as a general principle, legal persons have the same rights as natural persons, but that there may be differences. As an example, she pointed to the fact that the Court has held that the margin of appreciation left to States is wider when a measure concerns a legal person rather than a natural person.

7. While the applicants and the Government's lawyers both answered my questions, they did not directly address the points raised about the victim status of companies and the distinction relating to the applicability of different Convention rights in cases pertaining to companies. Thus, I will endeavour to address these points directly in this opinion.

B. Relevant provisions on which the victim status of companies can be based

8. The applicant companies alleged a breach of their rights under Article 8 of the Convention, in relation to the transfer of data from the VROM-IOD to the NMA, and on this basis brought individual applications under Article 34 of the Convention. Those provisions provide as follows:

Article 8

"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."

Article 34

"The Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right."

9. To facilitate our discussion of the interpretation of the relevant provisions of the Convention in harmony with one another, according to the principle of internal coherence (which is an aspect or dimension of the principle of effectiveness), Article 1 of Protocol No. 1 to the Convention will be discussed below as well. It provides as follows:

"Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.

The preceding provisions shall not, however, in any way impair the right of the State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure payment of taxes or other contributions or penalties."

C. In search of the proper legal basis under Article 34 allowing companies to make claims which are admissible *ratione personae*

10. The question at the core of this opinion is whether and how companies are included within the scope of Article 34 of the Convention, and therefore whether they are entitled to bring individual applications before the Court as victims of human rights violations. Under Article 34, in order to bring a claim before the Court, the applicant must claim to be a victim, and either be a "person, non-governmental organisation or group of individuals".

11. These three categories of applicants can be visualised as three windows or doorways. An applicant must be able to pass through one of the three windows for the application to be admissible *ratione personae.* Alternatively, if the categories are visualised as doorways, the applicant must be able to walk through one of them in order to enter the house – entry to the house symbolising the acquisition of procedural standing. This opinion seeks to establish through which window or doorway companies pass to make claims which are admissible *ratione personae* under Article 34, if they can

do so. Indeed, the judgment in the present case omits to inform and invigorate the legal basis for addressing the substance of the applicant companies' claims.

1. "Windows" through which companies can make claims which are admissible ratione personae under Article 34

(a) Companies as "persons"?

12. Under Article 34, the term "person" in the English text appears broader than the wording in the French text. Indeed, legal entities like companies are often referred to as legal persons, so it is worth considering whether companies can bring claims which are admissible *ratione personae* by fitting through the "person" window or doorway mentioned above.

13. However, the French text of Article 34 provides a more restricted meaning of the term "person", as follows (emphasis added):

Article 34

> "La Cour peut être saisie d'une requête par toute *personne physique*, toute organisation non gouvernementale ou tout groupe de particuliers qui se prétend victime d'une violation par l'une des Hautes Parties contractantes des droits reconnus dans la Convention ou ses protocoles. Les Hautes Parties contractantes s'engagent à n'entraver par aucune mesure l'exercice efficace de ce droit."

14. The French text specifies that the first category of applicants comprises "*personne[s] physique[s]*", or, in English, natural persons.

15. Though the Convention indicates that both the English and French texts are "equally authentic", when there is a difference in the meaning of the texts, they must be reconciled and read to give effect to the object and purpose of the treaty (see *Perinçek v. Switzerland* [GC], no. 27510/08, §§ 150-51, 15 October 2015; *Stoll v. Switzerland*, no. 69698/01, § 60, 10 December 2007; *James and Others v. the United Kingdom*, 21 February 1986, § 42, Series A no. 98; *Pakelli v. Germany*, 25 April 1983, § 31, Series A no. 64; *The Sunday Times v. the United Kingdom*, 26 April 1979, § 48, Series A no. 30; see also Article 33 § 4 of the Vienna Convention on the Law of Treaties, which provides that in the event of differences in the meaning of the texts, "the meaning which best reconciles the texts, having regard to the object and purpose of the treaty, shall be adopted").

16. The narrower wording of Article 34, namely the French text, which restricts the term to "*personne physique*", cannot be reconciled with a possible broader reading of the term "person" in the English text which is broad enough that it could include legal persons.

17. One might wonder, therefore, whether restricting the meaning of the term "person" in Article 34 so that it covers only natural persons, and not legal persons, runs counter to the principle of effectiveness. Indeed, this principle is intended to ensure that the Convention is an effective instrument,

that is, effective in its protection of human rights, and thus requires that rights be given a broad interpretation, while restrictions on rights should be interpreted narrowly. However, in this case, it is crucial to recall two observations on the principle of effectiveness as a method of interpretation and norm of international law: the wording of a given provision, and its object and purpose, both influence the application of this principle. On the wording of Article 34, were the interpretation of this Article to allow legal persons to be included within the term "person", this would be expressly at odds with the French version of the text, which explicitly restricts the word "*personne*" to "*personne physique*", that is, a "natural person".

18. Therefore, it is not incompatible with the principle of effectiveness to restrict the scope of the word "person" in Article 34 to natural persons: rather, it is honouring the meaning of the text as clarified by the French text of the Convention. The French text also serves to elucidate the object and purpose of the provision: if the purpose of Article 34 was to allow companies to bring claims under the category of "person", the French text would not qualify it with the adjective "*physique*". But as it does use that adjective, the purpose must have been to restrict the term "person" to natural persons, excluding legal persons. If the term "person" were to be deemed to include legal persons, this would render the French text a dead letter, as that interpretation would effectively contradict the term "*personne physique*".

19. The conclusion that "person" in Article 34 cannot encompass legal persons is also supported by the formulation of Article 1 of Protocol No. 1 to the Convention, cited above. That Article, which protects property, is at its heart an economic right: it is coherent that the drafters would wish to include commercial companies within its ambit. Thus, they specified that "[e]very natural or legal person is entitled to the peaceful enjoyment of his possessions". From this choice of wording, it is clear that "person" as used in Article 34 could never have been intended, from the outset, to include legal persons: if it had, there would be no need to specify the inclusion of legal persons as the subjects of Article 1 of Protocol No. 1. This is true of both the French and English texts of Article 1 of Protocol No.1: where the English text uses the phrase "every natural or legal person", the French text uses the phrase "*toute personne physique ou morale*".

20. As will be argued later, the historical backdrop and the emphasis on human dignity in the Convention makes it very unlikely that the drafters intended on including legal persons as potential victims within Article 34 in general, and thus, that they intended to include legal persons as potential victims within the term "person". Otherwise stated, it would be against the principle of human dignity and the aim and object of the Convention, if the term "person" were given a meaning which also included legal persons.

(b) **Companies as "non-governmental organisations"? – The case-law's approach**

21. When deciding on whether an applicant company's case is admissible *ratione personae*, the Court has often approached the issue on the basis that for its case to be so admissible, the company must fall under the category of "non-governmental organisation". Much of the case-law in this regard aims to differentiate governmental from non-governmental organisations: when doing so, the Court accounts for an entity's legal status, the rights that the status confers on the entity, the nature of the activity that it carries out, the context in which it carries out its activity and the independence it has from the authorities (see *Islamic Republic of Iran Shipping Lines v. Turkey*, no. 40998/98, § 79, 13 December 2013; for other cases where commercial companies were examined as non-governmental organisations, see *JKP Vodovod Kraljevo v. Serbia* (dec.), nos. 57691/09 and 19719/10, § 24, 16 October 2018; *Východoslovenská Vodárenská Spoločnosť, A.S. v. Slovakia* (dec.), no. 40265/07, 2 July 2013; and *State Holding Company Luganskvugillya v. Ukraine*, no. 23938/05, 27 January 2009).

22. However, there has been no real analysis of why the term "non-governmental organisation" in Article 34 should encompass commercial companies, making their claims admissible *ratione personae*. Early cases in which commercial companies were assessed as potential non-governmental organisations appeared to take this for granted. In *RENFE v. Spain* (no. 35216/97, Commission decision of 8 September 1997, Decisions and Reports 90-B, p. 179), the Commission cited Article 25 (what is now Article 34, no changes having been made to the person, non-governmental organisation and group of individuals categorisation), and deduced from the text that:

> "The question [was], therefore, whether the applicant [could] be considered as a non-governmental organisation within the meaning of this provision."

23. There was no discussion of why companies should be considered as potential "non-governmental organisations": it was taken for granted. These cases cannot provide a legal basis or explanation for considering commercial companies as "non-governmental organisations" under Article 34 when this was just taken for granted, owing to the lack of legal reasoning behind this conclusion. Where there is legal reasoning pertaining to a company's status as a non-governmental organisation, as mentioned above, the point of contention is not whether it is the right "window" or "doorway" through which companies can make claims which are admissible *ratione personae*, the point of contention is often whether a company is separate enough from the State to count as a "non-governmental" entity. In other words, the fact that if a company can make an application which is admissible *ratione personae*, it would be as a non-governmental organisation has never

been questioned; what has been questioned is whether a company is non-governmental enough.

24. This is problematic from the standpoint of invigorating the legal basis for individual applications before the Court, but also because it clearly runs counter to the common understanding of what a "non-governmental organisation" is, especially taken against the historical backdrop of the Convention. The Convention, the Court and, for that matter, the Council of Europe were created with the intention of preventing and providing justice in the face of the kinds of horrors that marked the beginning of the twentieth century. The Preamble of the Convention refers to the Universal Declaration of Human Rights, which itself has as its cornerstone the "recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family". The Convention's Preamble further refers to effective political democracy and a common understanding and observance of human rights as the best way to maintain fundamental freedoms. The intention behind the Convention was to provide a framework to provide justice to those who had been the victims of human rights abuses, the core of which is human dignity.

25. In view of the above, it is difficult to conceive that against the backdrop of the murder, torture and exploitation of millions by authoritarian regimes, the victims anticipated by the drafters of the Convention could include for-profit companies whose interests are commercial rather than humanitarian or philanthropic. Any application from commercial companies coming before the Court would not bolster or advance the protection of human dignity, given the nature of the applicants, who are neither human nor motivated by the pursuit of human rights.

26. Further, within the realm of international human rights law, "non-governmental organisations", known as NGOs, are often understood to advocate for human rights advances and represent victims of human rights abuses, rather than act for commercial gain. For instance, Article 71 of the UN Charter expressly provides for "consultation with non-governmental organizations which are concerned with matters within [the competence of the Economic and Social Council]": this was not with the intention, or effect, of overwhelming the Council with suggestions and lobbying from commercial companies. Still within the United Nations, the UN Development Programme defines a "non-governmental organisation" as a "non-profit organization, group or institution that operates independently from a government and has humanitarian or development objectives"[1]. These definitions, and this use of the term "non-governmental organisation", are much more coherent with the accepted understanding of what a "non-governmental organisation" is, than any definition that would, through

[1] See https://popp.undp.org/taxonomy/term/6216.

a very literal approach, include commercial companies as NGOs simply because they are not affiliated with a government.

27. The above discrepancy between what is generally understood to be a non-governmental organisation and what the Court is including within the term "non-governmental organisations" in Article 34 requires that the Court justify its approach in assessing commercial companies within the category of "non-governmental organisation", because nothing in the common understanding, or the natural meaning, of what a non-governmental organisation is explains this approach. Simply taking for granted the fact that companies can be non-governmental organisations under Article 34 is not satisfactory.

28. There is also a historical argument justifying the exclusion of commercial companies from the ambit of Article 34. According to the *travaux préparatoires* of the Convention, the initial draft included the phrase "corporate person", which was then changed to "corporate body", before becoming "non-governmental organisation". Though some argue that there was no doctrinal significance for this change[2], it cannot be insignificant: there must be a reason why the drafters decided to opt for one formulation rather than the other. I would argue that this represents a distancing from the impliedly commercial term "corporate", in favour of the term "non-governmental organisation", which is understood to refer to philanthropic or humanitarian bodies.

29. An additional point could be made on the meaning of "non-governmental organisations", relating to the wording used in Article 1 of Protocol No. 1. If the term "non-governmental organisation" was meant to describe companies as well, it seems difficult to justify using the term "legal persons" in Article 1 of Protocol No. 1: one could imagine that the drafters could have used the same term, "non-governmental organisation", to designate commercial companies in Protocol No. 1, if it were clear that that term encompassed companies.

30. Further, the principle of internal coherence or harmony, which, as stated above, is an aspect of the principle of effectiveness, dictates that it is very unlikely that companies were intended to be included within the "non-governmental organisation" category. As established above, the intention of the drafters was not to include companies within Article 34 of the Convention under the category of "person": the French text makes this abundantly clear. If the drafters had wished to include companies within Article 34, they could have used the phrase "natural and legal person", as they did less than two years later, in Article 1 of Protocol No. 1. So, it is worth questioning why, having deliberately excluded legal persons from the ambit

[2] See Marius Emberland, *The Human Rights of Companies*, Oxford University Press, 2006, at p. 35, and William Schabas, *The European Convention on Human Rights: A Commentary*, Oxford University Press, 2015, at p. 732.

of the term "person" in Article 34, the drafters would have then intended for it to be included under "non-governmental organisation" within the same provision. It seems much more coherent and logical that they did not intend for companies to be included at all.

(c) Companies as "groups of individuals"?

31. The final remaining "window" or "doorway" is the "group of individuals" category. However, this category is relevant to applicants who are affected by a potential breach of rights as individuals in their autonomous capacity, not as subsumed by a legal entity, such as a company. Indeed, the Court has found that applicants fall within the category of a "group of individuals" where "the rights and freedoms relied upon concern them individually" and are not attributable to an institution that they are a part of (see *Forcadell I Lluis and Others v. Spain*, no. 72147/17, § 19, 7 May 2019).

32. When a company brings a claim before the Court, the rights and freedoms that are allegedly breached are not those of the individuals within the company: after all, in the present case, the applicant companies argued that the rights of the companies themselves had been breached. Furthermore, when a company is the applicant, it runs counter to the point of focusing on a breach of the company's rights to identify individual members within that company. This category within Article 34 has never been used by the Court to justify finding that a company's application was admissible *ratione personae*. Therefore, companies, though they are from a purely descriptive angle made up of a group of persons, cannot have their applications deemed admissible *ratione personae* on the basis that they are a "group of individuals": they cannot use that "window" or "doorway".

2. Case-law assuming that companies have locus standi without any explanation at all

33. There are also cases where the Court appears to bypass the *ratione personae* assessment entirely. It takes entirely for granted that companies can submit claims which are admissible *ratione personae*, without engaging with a broader discussion of whether they fall into the category of "person", "non-governmental organisation" or "group of individuals".

34. A clear, but not unique, example of this approach is in the case of *Liblik and Others v. Estonia* (nos. 173/15 and 5 others, 28 May 2019). There were six applicants in this case: two of them were companies. They alleged that their rights under Article 6 had been violated owing to the excessive length of criminal proceedings against them, and that their rights under Article 8 had also been violated owing to the retrospective justification of secret-surveillance authorisations. When considering the admissibility of the companies' claims under Article 8, the Court did not consider what "window" or "doorway" would enable the companies to make their applications

admissible *ratione personae*. Instead, it considered the following issue: one applicant was a member of the supervisory boards of the two applicant companies, and the secret-surveillance authorisations had been granted in respect of this applicant. The information gathered from this surveillance had been used to convict the applicant companies, but the Government in that case contested the claim that the companies' rights under Article 8 had been interfered with: they argued that the supervisory board member's rights had been interfered with, but not the companies'. The Court found that there was "no reason to distinguish between the 'correspondence' of the third applicant, an individual, and that of the applicant companies, legal entities" (ibid., § 112). Thus, it did not consider whether companies like the applicant companies could even bring individual applications under Article 34, or through which "window" such applications could be made: it considered the substance of the application and deduced from it that the "applicant companies [could] accordingly claim to be victims within the meaning of Article 34 of the Convention" (ibid.).

35. Though the analysis described above was set out by the Court under the heading "The Court's assessment as to the victim status of the applicant companies" and the section began by citing Article 34 of the Convention, it proceeded to discuss the validity of the claim *ratione materiae*, before concluding that the applicant companies could claim that they were victims within the meaning of Article 34.

36. This amounted to bypassing the *ratione personae* analysis by considering other elements of the claim and deducing from them that the applicant company could claim to be a victim under Article 34 (see also *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, §§ 60-61, 28 June 2007). Article 8 should not provide wider scope for companies to have claims declared admissible *ratione personae* than is provided for by Article 34.

37. Further, the living instrument doctrine should not be used to expand the rights that companies can vindicate before the Court. In *Société Colas Est and Others v. France* (no. 37971/97, ECHR 2002-III), the Court once again did not address which category of Article 34 applicant the applicant in that case, a commercial company, fell within. Instead, it confined its analysis to whether a legal person like the applicant company had the right to a home under Article 8. It based its assessment on case-law according to which interference with a natural person's office can amount to interference with his or her right to respect for home, and case-law according to which companies have a right to compensation in respect of non-pecuniary damage sustained as a result of a violation of Article 6 § 1 of the Convention. On the basis of those cases, the Court concluded that, under the living instrument doctrine,

> "the time [had] come to hold that in certain circumstances the rights guaranteed by Article 8 of the Convention [could] be construed as including the right to respect for a company's registered office, branches or other business premises ..."

38. That interpretation of the living instrument doctrine was flawed. The doctrine should be used to broaden a right within the scope of the object of the Convention, rather than expand the scope of a right *contra legem*. In that case, the Court widened the scope of cases in which companies could claim to be victims: it established that companies could vindicate a right to respect for their "home", that is, their offices. The living instrument doctrine was used to justify this step, when in fact, it could not do so: by further expanding the rights that companies can vindicate, the Court here acted counter to the object and purpose of Article 34 of the Convention, which is not to include companies as applicants capable of bringing claims which are admissible *ratione personae*.

3. Widespread assumption of companies' victim status under Article 34 – established practice

39. Even though, as detailed above, companies pose challenges to every "window" under Article 34, the Court has a long-established practice of assuming that they are able to bring claims under Article 34. The Court has heard cases on alleged breaches of companies' rights under Article 6 (see *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [GC], no. 931/13, 27 June 2017, and *Altius Insurance Ltd v. Cyprus*, no. 41151/20, 24 October 2023), Article 8 (see *Société Colas Est and Others*, cited above), Article 10 (see *Couderc and Hachette Filipacchi Associés v. France* [GC], no. 40454/07, ECHR 2015 (extracts)) and Article 1 of Protocol No. 1 (see *Euromak Metal Doo v. the former Yugoslav Republic of Macedonia*, no. 68039/14, 14 June 2016) and it has awarded non-pecuniary damage to companies under Article 41 of the Convention (see *Comingersoll SA v. Portugal* [GC], no. 35382/97, ECHR 2000-IV).

40. Given this body of case-law, it would be extremely difficult to suggest turning back and asserting that companies cannot bring claims under Article 34. Therefore, I am not suggesting that, in the present case, the Court should have abandoned this assumption. However, it should have attempted to elucidate the legal basis for it, especially given that the question of legal basis was raised during the oral hearing.

41. In my opinion, the least problematic legal basis to support the Court's assumption that companies can bring claims which are admissible *ratione personae* under Article 34 is the "non-governmental organisation" category.

42. Although the original meaning of the term "non-governmental organisation" was likely not intended to include commercial companies, one could argue that the meaning of the term, through its application to commercial companies in the case-law, has now changed. In other words, one could argue that now that companies have persistently been labelled as "non-governmental organisations" in the Court's case-law, the term's scope has widened to include companies.

D. Conclusion

43. This overview of the Court's approach to the admissibility *ratione personae* of individual applications brought by commercial companies serves to demonstrate the importance of the Grand Chamber providing guidance and clarity on this issue.

44. The present case could have served to clarify the legal basis for allowing companies like the applicant companies to bring individual applications before the Court under Article 34, especially given that the question of legal basis was raised during the oral hearing. However, the Court regrettably missed its opportunity to do so: this judgment does not address the issue at all.

45. Based on the case-law discussed in section 3 (c) above, I do not suggest that it is for the Court in this case to change its practice of recognising that companies are able to make claims which are admissible *ratione personae* under Article 34 of the Convention. What is left for it to do is to clarify the legal basis for this practice.

46. In my opinion, despite the fact that, as demonstrated above, the classification of companies within any of the three "windows" or "doorways" of Article 34 is problematic, the least problematic for companies to pass through is the "non-governmental organisation" window. This is because it could be argued that in a departure from the original and commonly understood meaning of the term, "non-governmental organisations" can be understood to include companies. It would be more difficult for companies to pass through the "person" window, because the express reference to "*personne physique*" in the French text firmly excludes this possibility. Also, by definition, the "group of individuals" window could not enable companies to have victim status.

47. Not only does the French term "*personne physique*" bar companies from having victim status through the "person" window, but it may also bar the Court from affording victim status to different forms of artificial intelligence through this window in its future case-law.

48. If forms of artificial intelligence possessing some of the functions of natural persons, like robots, seek protection before the Court, the term "*personne physique*" will prevent them from passing through the "person" window.

49. If, one day, member States decide to provide some kind of protection for artificial intelligence, it would be better done through a new Protocol. A new Protocol would also offer the opportunity to firmly and clearly set out a legal basis for the claims of entities other than natural persons, including companies. However, one can only wonder how such developments in the future, if they came to be, could be reconciled with the Convention's primary aim for the effective protection of human rights and the principle of human dignity! If, in the future, artificial intelligence has rights similar or adjacent

to human rights safeguarded by the Convention, as granted by a new Protocol to the Convention, how could one be certain that it would itself respect human rights, the rule of law and the principle of democracy. Though it may be conceivable that autonomous artificial intelligence may in the future benefit from the protection of rights similar or adjacent to human rights contained in the Convention, at the same time, it is crucial that this goes hand in hand with the capacity and obligation of such artificial intelligence to respect human rights, the rule of law and the principle of democracy. However, I cannot continue further this interesting, though theoretical and philosophical discussion, since this is not the issue here.

III. WHETHER THERE HAS BEEN A VIOLATON OF ARTICLES 8 AND 13

50. Having concluded that the applicant companies had *locus standi*, I examined whether there has been a violation of Articles 8 and 13 and my reasoning and conclusion are fully reflected in the dissenting opinion of Judge Arnardóttir joined by Judges Serghides and Šimáčková and the joint dissenting opinion of Judges Serghides and Arnardóttir.

51. It is to be clarified that in this opinion, I found it necessary to examine first the *locus standi* of the applicant companies. Had I not come to the conclusion that they had *locus standi*, I would not have proceeded to examine the merits of the case and to find, together with the other two Judges in the dissenting opinion of Judge Arnardóttir which I joined, a violation of Article 8 of the Convention and, together with the eminent Judge Arnardóttir, a violation of Article 13 of the Convention.

IV. JUST SATISFACTION

52. Having found that there has been a violation of Articles 8 and 13 in respect of all of the applicant companies, I would award them pecuniary damage. However, being in the minority, there is no need to determine the appropriate amount of pecuniary damage to be granted to them.

53. Since, like natural persons, companies are able to submit requests in respect of non-pecuniary damage[3], I would also award an amount in this respect had the applicant companies submitted such a request.

[3] See Eloïse Ward, "Blurring the line between natural and legal persons in a company's compensation for non-pecuniary damage: *Affaire SCI Le Château du Francport c. France*", in Strasbourg Observers, 10 December 2024 (https://strasbourgobservers.com/2024/12/10/blurring-the-line-between-natural-and-legal-persons-in-a-companys-compensation-for-non-pecuniary-damage-affaire-sci-le-chateau-du-francport-c-france/).

JOINT DISSENTING OPINION OF JUDGES SERGHIDES AND ARNARDÓTTIR

For the reasons set out in paragraphs 12-18 of the dissenting opinion of Judge Arnardóttir joined by Judges Serghides and Šimáčková, we are unable to agree with the majority of the Grand Chamber that Article 13 was not violated in the present case.

DISSENTING OPINION OF JUDGE ARNARDÓTTIR, JOINED BY JUDGES SERGHIDES AND ŠIMÁČKOVÁ

1. We respectfully disagree with the majority's conclusion that there has been no violation of Article 8 of the Convention in the applicant companies' case.

2. The approach taken by the majority is based on the well-founded premise that the interception of communications and the transmission of the data thereby obtained for use in pursuit of a different purpose constitute two separate interferences, which must each be justified in accordance with the requirements of Article 8 § 2. We agree with majority's approach that such data transmissions must never become an instrument for circumventing the strict safeguards applicable to the interception of communications. We can also agree in principle with the safeguards against arbitrariness and abuse and with the elaboration of the Court's proportionality assessment as set out in paragraphs 160 and 161 of the judgment, as well as with the approach taken by the majority as regards the level of protection for legal persons and the margin of appreciation in such matters.

3. In our opinion, however, the Grand Chamber did not attach sufficient importance to the object pursued by such data transmissions for the function of the State's margin of appreciation and, consequently, for the Court's review of proportionality. We find that the Grand Chamber should have stated more clearly that the transmission of intercept criminal data for purposes unrelated to the original purpose of the interception can only be justified in pursuit of weighty interests. We regret that the majority have opted for an approach that may result in a considerably lower level of protection than that provided under the ePrivacy Directive (Directive 2002/58/EC (as amended by Directives 2006/24/EC and 2009/136/EC) of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ 2002 L 201)). We note in this regard that the ePrivacy Directive provides protection for the legitimate interests of legal persons (see Article 1(2) of the Directive). As interpreted by the CJEU, it further provides that intercept data cannot in principle be transmitted for use in pursuit of purposes of lesser importance than those which justified the interception (see the CJEU's judgment of 7 September 2023 in *Lietuvos Respublikos generalinė prokuratūra*, C-162/22, EU:C:2023:631).

4. We also have objections to the majority's approach concerning the application of the general principles laid down by the Grand Chamber to the facts of the applicant companies' case. In this connection, we find that the majority have not given sufficient weight to the interests of those affected by transmission of intercept criminal data for a purpose unrelated to the purpose of collection and have thereby opened the door to unnecessary conflict with

the standards developed in EU law. What follows is an explanation for our position in this regard.

5. Firstly, in paragraph 160 of the judgment, the Grand Chamber lays down the important safeguard that the circumstances in which intercept criminal data may be transmitted to another law-enforcement authority must be set out sufficiently clearly in domestic law. This certainly follows the logic of the Court's established case-law in the fields of covert intelligence-gathering and criminal data protection alike. We note in this connection that the Grand Chamber has held that for such legislation to be foreseeable for the purposes of the Convention, it is essential that it contain "clear, detailed rules governing the scope and application of measures", which includes defining with sufficient clarity "the scope of discretion conferred on the competent authorities and the manner of its exercise" (see *Roman Zakharov v. Russia* [GC], no. 47143/06, §§ 229-230, ECHR 2015, and *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, §§ 95 and 99).

6. In applying this safeguard to the applicant companies' complaint that the data transmissions formally authorised by the Public Prosecution Service were unlawful for the purposes of the Convention, the majority find that the above requirement under Article 8 § 2 of the Convention was satisfied by section 39f of the Judicial and Criminal Data Act ("the WJSG"). In so far as relevant, this legal provision authorises the transmission of "criminal data" to "persons or public authorities" for the "enforcement of legislation", when necessary "in view of a compelling general interest" (see paragraph 61 of the judgment). As regards the exercise of the power to transmit data in practice, the Instructions on the transmission of criminal data for purposes not related to the administration of criminal justice ("the WJSG Instructions") provide no further clarification, aside from requiring that "grounds must exist" for the recipient to receive the data and explaining in general terms that the Public Prosecution Service must perform an assessment of the necessity and proportionality of the transfer of data (see paragraph 69 of the judgment).

7. In our opinion, the "enforcement of legislation" purpose is too broadly formulated in the WJSG to meet Convention standards. We note, in particular, that it does not contain any minimum severity threshold and provides no other details as to the nature of the breaches of legislation that might justify such transmissions. It thus leaves public prosecutors wide discretion in determining which breaches of legislation are serious enough to justify transmission of intercept criminal data. Furthermore, this discretion is not narrowed by any limitation on the recipients of such data. Instead, the list of possible recipients is open-ended, consisting of any "persons or public authorities" responsible for such enforcement. Nor is this discretion limited by reference to restrictions on the type of data that may be transmitted. Rather, the term "criminal data", as interpreted by the domestic courts, seems to cover any data processed in the context of criminal investigations (see

paragraphs 31 and 57 of the judgment). Moreover, the broad discretion to transmit data in pursuit of the "enforcement of legislation" is not limited by any description of what might constitute a "compelling general interest". In fact, as is evident from the Explanatory Memorandum to the relevant bill, this term is intended to be broadly understood and may even include private interests (see paragraph 63 of the judgment).

8. In the light of the above, the discretion conferred by Dutch law on the competent authorities to transmit intercept criminal data for use in pursuit of unrelated purposes is too broad to guard against arbitrary interference and abuse of power. The general requirement to perform a necessity and proportionality assessment, as set out in the WJSG and the WJSG Instructions, cannot replace the minimum Convention requirements in this regard. In our opinion, therefore, the Grand Chamber ought to have found a violation of Article 8 of the Convention in respect of all the applicant companies on the ground that the relevant Dutch legislation did not meet the Convention requirement of "foreseeability".

9. Secondly, we note that the applicant companies also complained that there had been no foreseeable basis in law for the transmission of intercept data when it came to the "exploratory interactions" that had taken place prior to the issuance of formal transmission authorisations under section 39f of the WJSG. In this connection, all the applicant companies complained that, following the formally authorised data transmissions, the NMA had provided the investigators with search terms to be applied to the criminal files in their entirety, on the basis of which the transmission of additional material had been authorised. We note, however, that this did not result in any data being accessed before formal authorisation was given for additional data transmissions. However, the Janssen companies also complained that the NMA had been given access to intercept data before the issuance of any transmission authorisation whatsoever. We are therefore of the opinion that, in its analysis, the Grand Chamber should have distinguished between these different aspects of the applicant companies' complaints about the "exploratory interactions" and should have found a violation of Article 8 in respect of the Janssen companies based on the complete absence of a legal basis for the access given to their data.

10. In this respect, we note that, prior to the first transmission authorisation in the Janssen companies' case, the NMA was given access, on police premises and in strict confidence, to a selection of transcripts of intercepted telephone conversations. The public prosecutor also sent the NMA, for information purposes only and in strict confidence, a CD containing audio recordings of about thirty conversations, explicitly prohibiting their use for any other purpose, before the transmission of data was formally authorised (see paragraphs 37-38 of the judgment). Section 39f of the WJSG, however, only authorised the Public Prosecution Service to "transmit" data for the purpose of the "enforcement of legislation".

Furthermore, section 39f of the WJSG, as explained in the WJSG Instructions, required the prosecutor to assess the necessity and proportionality of the envisaged transmission for that purpose prior to performing the "factual act" of transmission (see paragraphs 63 and 69 of the judgment). In our view, section 39f of the WJSG could not serve as a legal basis for informal access to intercept data by third parties before the formal transmission of that data in accordance with the above requirements. We also note that neither the domestic courts nor the Government referred to any domestic legal provision capable of serving as a legal basis for such access and that the Supreme Administrative Court for Trade and Industry merely found that this access had not rendered the formal transmission of data incompatible with the WJSG (see paragraphs 57 and 127 of the judgment). It follows, in our opinion, that in the Janssen companies' case, the NMA officials were informally given access to confidential intercept data in the absence of a clear legal basis permitting such access.

11. The Convention requirement that there should be a legal basis for all interferences reflects the principle of the rule of law, which is inherent in the system of protection established by the Convention and the Protocols thereto, and which is expressly mentioned in the Preamble to the Convention. If criminal investigators are allowed to grant access to intercept data, informally, for purposes other than those set forth in legislation and without following the legally prescribed procedure, this amounts to a violation of Article 8 of the Convention of such gravity that it cannot be remedied by retrospectively granting authorisation in accordance with the law. The Supreme Administrative Court for Trade and Industry nevertheless found such retrospective authorisation sufficient to render the interference with the Janssen companies' rights lawful and that reasoning, unfortunately, has been accepted by the majority of the Grand Chamber (see paragraphs 57 and 179 of the judgment). By the time retrospective authorisation was granted, however, the damage had already been done for the purposes of the Convention, to the extent that the NMA had already unlawfully gained knowledge of the intercept material. This fact alone should therefore have sufficed for the Grand Chamber to find a violation of Article 8 in respect of the Janssen companies.

12. Thirdly, in paragraph 160 of the judgment the Grand Chamber sets out the important safeguard that the transmission of intercept data for a purpose beyond the original criminal context for their collection must be subject to effective review by a judicial or otherwise independent body. While we can agree with this statement of principle, we would have preferred the Grand Chamber to have highlighted the fact that *ex post facto* review in cases of this kind should preferably be judicial. For the reasons set out below, we also find that the majority's application of the above standard is highly problematic.

13. In the circumstances of the present case, we are concerned about the absence of any reasoning in the transmission authorisations, which contained no verifiable assessment as to whether the transmissions were "necessary in a democratic society", including whether they were proportionate to the legitimate aim pursued. The prosecutors were required by Article 3:4 of the General Administrative Law Act ("the AWB") and the WJSG Instructions to assess the necessity and proportionality of any data transmission (see paragraphs 69 and 79 of the judgment). At the same time, because data transmission is characterised under domestic law as a "factual act", and not as a "decision" within the meaning of the AWB, prosecutors are not explicitly required to record their assessment in a written reasoned decision under either the WJSG or the WJSG Instructions. As can be seen from the Dutch Supreme Court's case-law in civil proceedings, the lawfulness of the "factual act" of transmission does not, therefore, depend on the reasons given by the prosecutor at the time of authorisation; the assessment of the lawfulness of a "factual act" can be carried out retrospectively and independently by a reviewing court (see paragraphs 71-72 of the judgment). In the present case, the Supreme Administrative Court for Trade and Industry took the same approach, finding that it was not necessary to have the prosecutor's reasoning and carrying out its own *de novo* assessment of whether the data transmissions had been lawful and compatible with the Convention (see paragraphs 31 and 57 above).

14. The Court has held in the context of the interception of communications that the contemporaneous provision of reasons is a vital safeguard against arbitrariness and abuse because it ensures that the authorising authority has properly reviewed the necessity and proportionality of the interference with Article 8 rights (see *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, § 313, 11 January 2022). Indeed, in some cases, too succinct a reasoning, without the production of any supporting documents demonstrating that the domestic court nevertheless verified the existence of a reasonable suspicion and examined the necessity and proportionality of the interception of communications, has led the Court to find a violation of Article 8 (see *Moskalev v. Russia*, no. 44045/05, §§ 41-44, 7 November 2017, and *Dudchenko v. Russia*, no. 37717/05, §§ 96-99, 7 November 2017). The Court has also noted that the practice of accepting reasoning provided retrospectively to justify the interception of communications calls for caution as, at later stages, the courts inevitably have more information about how the alleged offences were committed (see *Liblik and Others v. Estonia*, nos. 173/15 and 5 others, § 141, 28 May 2019). It has noted, moreover, that when an interception warrant contains no reasoning, it cannot be reviewed in terms of necessity in a democratic society for the purposes of Article 8 § 2 of the Convention (see *Potoczká and Adamčo v. Slovakia*, no. 7286/16, § 76, 12 January 2023).

15. While these strict requirements for authorisation procedures have been developed by the Court in the context of the interception of communications, we note that the transmission and use of intercept criminal data for a new purpose constitutes a significant interference with Article 8 rights. We also note that, in the present case, the circumstances in which such transmission could be authorised were extremely broadly defined in law (see paragraphs 5-7 above). Given that context, it is our opinion that an individualised prior assessment of the necessity and proportionality of the transmission is particularly important as a key safeguard against abuse (compare and contrast *L.B. v. Hungary* [GC], no. 36345/16, § 117, 9 March 2023). In such situations, we also find that written reasoning, even if succinct, is required to ensure that the authorising authority has properly reviewed the necessity and proportionality of the interference with Article 8 rights and to enable effective *ex post facto* review. This constitutes an important safeguard against arbitrariness and abuse in the context of the transmission of intercept material for purposes unrelated to the original purpose of the interception, ensuring that such transmissions are not ordered haphazardly, irregularly or without due and proper consideration.

16. In the present case, the absence of reasoned transmission authorisations seriously weakened the effectiveness of the available *ex post facto* remedies. When the applicant companies challenged the transmissions before the domestic courts, they were unaware of the reasons which had prompted the decisions to transmit the data. This impeded their ability to challenge the transmissions effectively (compare *Zubkov and Others v. Russia*, nos. 29431/05 and 2 others, § 91, 7 November 2017). While the NMA provided its own assessment of the lawfulness, necessity and proportionality of the transmissions in the administrative proceedings, that assessment was inevitably retrospective and speculative, and therefore could not effectively compensate for the absence of traceable reasoning behind the prosecutor's decisions to transmit the data. When coupled with the excessively wide discretion afforded by section 39f of the WJSG to public prosecutors in ordering the transmission of intercept data for unrelated purposes, the absence of written reasoning in the transmission authorisations simply rendered it too difficult, upon judicial review, for the applicant companies to demonstrate that the transmissions had been in breach of Dutch law and the Convention (in a similar vein, see *Gillan and Quinton v. the United Kingdom*, no. 4158/05, §§ 80 and 86, ECHR 2010 (extracts); *Lashmankin and Others v. Russia*, nos. 57818/09 and 14 others, § 428, 7 February 2017; and *Ivashchenko v. Russia*, no. 61064/10, § 88, 13 February 2018).

17. Since the absence of written reasoning made it impossible to review the prosecutors' assessment of the transmissions' "necessity in a democratic society" for the purposes of Article 8 § 2 of the Convention (compare *Potoczká and Adamčo*, cited above, § 76), the Supreme Administrative Court

for Trade and Industry carried out its own independent assessment of whether the transmissions had been lawful and compatible with the Convention (see paragraphs 31 and 57 of the judgment), as did the provisional-measures judge in the civil proceedings (see paragraph 46 of the judgment). However, such *ex post facto* review could only provide retrospective reasoning. It could not replace prior scrutiny for the purpose of verifying whether there had been, at the material time, relevant and sufficient reasons for authorising transmissions of intercept material, since the courts, at that later stage, had the benefit of hindsight (compare *Liblik and Others*, cited above, § 141).

18. For the above reasons, we cannot agree with the majority when they find that the absence of written reasoned transmission authorisations was compensated for by the *ex post facto* review conducted in the applicant companies' case. In our view, the authorisation procedures were deficient and the *ex post facto* review carried out by the domestic courts did not sufficiently compensate for those deficiencies. On the contrary, the available remedies were undermined by the absence of written reasoning in the transmission authorisations and the wide discretion afforded to public prosecutors in ordering data transmissions. In our opinion, the Grand Chamber should therefore also have concluded that there has been a violation of Article 8 of the Convention in respect of all the applicant companies, as the domestic system of transmission authorisation and review did not afford them adequate safeguards against arbitrariness and abuse and was incapable of restricting the contested transmissions to what was "necessary in a democratic society".

APPENDIX

List of cases:

No.	Application no.	Case name	Lodged on	Applicant Year of incorporation Place of statutory seat	Represented by
1.	2799/16	Ships Waste Oil Collector B.V. v. the Netherlands	07/01/2016	**SHIPS WASTE OIL COLLECTOR B.V.** 1974 Rotterdam	Ms M. C. VAN HEEZIK
2.	2800/16	Janssen de Jong Groep B.V. and Others v. the Netherlands	07/01/2016	**JANSSEN DE JONG GROEP B.V.** 1965 Son en Breugel **JANSSEN DE JONG INFRA B.V.** 1957 Son en Breugel **JANSSEN DE JONG INFRASTRUCTUUR NEDERLAND B.V.** 1994 Son en Breugel	Ms M. C. VAN HEEZIK

No.	Application no.	Case name	Lodged on	Applicant Year of incorporation Place of statutory seat	Represented by
3.	3124/16	Burando Holding B.V. v. the Netherlands	07/01/2016	**BURANDO HOLDING B.V.** 1985 Rotterdam	Mr H. A. BRAVENBOER, Mr M. BOL
4.	3205/16	Port Invest B.V. v. the Netherlands	07/01/2016	**PORT INVEST B.V.** 1986 Rotterdam	Mr H. A. BRAVENBOER, Mr M. BOL