Written observations of the Kingdom of Belgium

Case C-623/17 *

Document lodged by:

Kingdom of Belgium

Usual name of the case:

PRIVACY INTERNATIONAL

Date lodged:

14 February 2018

KONINKRIJK BELGIË (KINGDOM OF BELGIUM)

Federale Overheidsdienst Buitenlandse Zaken,

Buitenlandse Handel en Ontwikkelingssamenwerking

(Federal Public Service, Foreign Affairs, Foreign Trade and

Development Cooperation)

COURT OF JUSTICE OF THE EUROPEAN UNION

Written Observations of the Belgian Government

Submitted pursuant to the second paragraph of Article 23 of the Protocol on the Statute of the Court of Justice of the European Union by the Belgian Government, represented by the Minister for Foreign Affairs, with Jean-Christophe HALLEUX and Pierre COTTIN, Attachés at the Directorate-General for Legal Affairs of the Federale Overheidsdienst Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking, with offices established at Karmelietenstraat 15, 1000 Brussels, acting as Agents, who hereby agree that the service of procedural

* Language of the case: English.

documents shall take place via e-Curia, or, failing that, by fax on number 0032.2.501.41.97, in the case:

C-623/17

Privacy International

in relation to a question referred for a preliminary ruling pursuant to Article 267 TFEU, lodged by the Investigatory Powers Tribunal — London (United Kingdom) by judgment IPT/15/110/CH of 18/10/2017 and lodged at the Registry of the Court of Justice on 4/12/2017 under number (No 1047819.1), concerning the interpretation of Article 4 TEU and Article 1(3) of Directive 2002/58/EC concerning privacy and electronic communications.

To the President, the Vice-President and the Members of the Court of Justice of the European Union

The Belgian Government wishes to make the following observations:

I. FACTS AND PROCEDURE

1. With regard to the facts and procedure, the Belgian Government refers to the order for reference (pp. 4 to 6 of the Dutch translation).

2. In the order for reference, the following questions were referred to the Court of Justice of the European Union ('the Court of Justice') for a preliminary ruling:

   - *Having regard to Article 4 TEU and Article 1(3) of Directive 2002/58/EC on privacy and electronic communications (the 'e-Privacy Directive'), does a requirement in a direction by a Secretary of State to a provider of an electronic communications network that it must provide bulk communications data to the Security and Intelligence Agencies (SIAs) of a Member State fall within the scope of Union law and of the e-Privacy Directive?*

   - *If the answer to Question (1) is 'yes', do any of the* Watson *Requirements, or any other requirements in addition to those imposed by the ECHR, apply to such a direction by a Secretary of State? And, if so, how and to what extent do those requirements apply, taking into account the essential necessity of the SIAs to use bulk acquisition and automated processing techniques to protect national security and the extent to which such capabilities, if otherwise compliant with the ECHR, may be critically impeded by the imposition of such requirements?*

II. EU-LAW FRAMEWORK

3. The Belgian Government refers to the EU-law framework as set out in the order for reference (pp. 3 and 4 of the Dutch translation).

4. A supplementary reference is also made to Article 5 of the Treaty on European Union ('TEU') and Articles 72, 73 and 346 of the Treaty on the Functioning of the European Union ('TFEU').

5. Article 5 TEU provides as follows:

'1. The limits of Union competences are governed by the principle of conferral. The use of Union competences is governed by the principles of subsidiarity and proportionality.

2. Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States.'

6. Article 72 TFEU provides as follows:

'This Title [i.e. Title V: 'Area of freedom, security and justice'] shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security.'

7. Article 73 TFEU provides as follows:

'It shall be open to Member States to organise between themselves and under their responsibility such forms of cooperation and coordination as they deem appropriate between the competent departments of their administrations responsible for safeguarding national security.'

8. Article 346 TFEU provides as follows:

'1. The provisions of the Treaties shall not preclude the application of the following rules:

(a) no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security;'

III. NATIONAL LEGAL FRAMEWORK

9. The Belgian Government refers to the legal framework of the United Kingdom, as described by the referring court in the order for reference (p. 4 of the Dutch translation).

IV. ANALYSIS

A. First question referred

10. By its first question the referring court seeks to ascertain whether, and — if so — on what legal basis, EU law applies to the activities of the security and intelligence agencies relating to the national security of a Member State.

11. The Belgian Government submits that that question must be answered in the **negative**.

    Article 5 TEU regulates the division of competences between the European Union and the Member States and provides that the European Union may act only within the limits of the competences conferred upon it by the Member States in the Treaties. Competences not conferred upon the European Union remain with the Member States.

12. Article 4 TEU provides that the European Union must respect the essential State function of the safeguarding of national security and that, arising therefrom, national security remains the sole responsibility of each Member State.

13. The Belgian Government is therefore of the view that the activities of the intelligence agencies (in Belgium these are the Veiligheid van de Staat en Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht (State Security Service and the General Intelligence and Security Service of the Armed Forces), including the collection of personal data, do not come within the scope of the European Treaties and secondary EU legislation. [1]

14. The Belgian Government submits that, given that primary EU law (TEU) cannot be amended by secondary EU law, the e-Privacy Directive is also not applicable to the activities of the intelligence agencies.

15. Moreover, Article 1(3) of the e-Privacy Directive provides that that directive does not apply in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

16. The Belgian Government is of the view that that provision is in line with Article 4 TEU and precludes the application of the EU rules. The retention and use of traffic and location data for reasons of national security thus come within the exclusive competence of the national law of the Member States. The derogation provided for in Article 15 of the Directive is thus not applicable.

[1] See, inter alia, the e-Privacy Directive and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (‘the General Data Protection Regulation’ or ‘the GDPR’.

17. In addition, the Belgian Government wishes to point out that the activities of the intelligence agencies which infringe the rights guaranteed by the European Convention on Human Rights ('ECHR') must meet the requirements of that Convention and the case-law arising from it. In the case of an infringement of the right to respect for privacy and family life, such an infringement must have its basis in law, it must be necessary in a democratic society, it must meet a social necessity and the principle of publicity and foreseeability. Those guarantees, as provided for in Article 8 ECHR, safeguard the balance between the protection of citizens and their privacy, and are sufficient to review the activities of the Member States with regard to national security (and thus also the activities of their intelligence agencies).

B. Second question referred

18. In the hypothesis that the first question is answered in the affirmative, by its second question referred for a preliminary ruling the referring court wishes to ascertain whether and, if applicable, to what extent the *Tele2 & Watson* judgment [2] has an impact on the retention of electronic communications data for reasons of national security.

19. Alternatively, if the Court of Justice answers the first question referred for a preliminary ruling in the affirmative, the Belgian Government submits that the second question should be answered in the negative.

20. In the *Tele2 & Watson* judgment, the Court of Justice imposed strict conditions for the retention of electronic communications data with a view to fighting serious crime (limited amount of data, limited retention period, personal and territorial limits).

21. The Court of Justice has thus held that the e-Privacy Directive does not preclude national legislation which provides for the targeted retention of data for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary. [3]

22. According to the Court of Justice, such national legislation must be clear and precise and must contain sufficient guarantees that personal data will be protected against the risk of misuse. It must indicate in what circumstances and under which conditions a data retention measure may, as a preventive measure, be adopted.

[2] Judgment of 21 December 2016, *Tele2 Sverige & Watson*, C-203/15, EU:C:2016:970, paragraphs 119 to 125.

[3] Judgment of 21 December 2016, *Tele2 Sverige & Watson*, C-203/15, EU:C:2016:970, paragraph 108.

The reason for that would be to ensure that such a measure is in fact limited to what is strictly necessary. [4]

23. Such legislation must, in particular, be based on objective evidence which makes it possible to identify persons whose data may have a link with serious criminal offences and to contribute to fighting serious crime or to preventing a serious risk to public security. [5]

24. In the points below, the Belgian Government wishes (a) to underscore the importance of the retention of electronic communications data for the intelligence agencies, and also (b) to explain the impact of the possible application of the strict *Tele2 & Watson* requirements on national security.

(a) Importance of data retention for intelligence agencies [6]

25. In all investigations of activities which threaten the State — investigations relating to terrorism, radicalisation, foreign financing of extremist faith communities, espionage or other clandestine operations by foreign powers — electronic communications data are a crucial information source for the intelligence agencies. Such data (the so-called metadata) make it possible to detect who is in contact with whom and where persons are located. The Belgian Government submits that this is a safe and efficient way of recognising patterns and identifying networks. Furthermore, the analysis of communications data avoids the need to use more privacy-intrusive methods to obtain the same information: shadowing persons in unsafe neighbourhoods, installing cameras or microphones, or intercepting telephone and internet traffic (taking note of the content of the conversation). Such operations require more manpower and involve more risks for the safety of personnel and operations. By way of illustration: in order to shadow one person on a 24-hour basis requires a complement of 25 agents. Furthermore, observing someone visually is much more privacy-intrusive and results in the acquisition of more information that is strictly necessary for the investigation.

26. The importance of information relating to who communicates with whom, where, when and how, increases as more and more people substitute classic telephony and messaging services (sms) for internet communication. Communication via applications (apps) such as Skype, WhatsApp, Viber, Telegram and Messenger is encrypted, as a result of which the content of the conversations thus remains hidden from the intelligence agencies. Moreover, the intelligence agencies do not

4 Judgment of 21 December 2016, *Tele2 Sverige & Watson*, C-203/15, EU:C:2016:970, paragraph 109.

5 Judgment of 21 December 2016, *Tele2 Sverige & Watson*, C-203/15, EU:C:2016:970, paragraph 111.

6 Wetsontwerp betreffende het verzamalen en het bewaren van de gegevens in de sector van de elektronische communicatie (Draft legislation on the collection and retention of data in the electronic communications sector), Belgische Kamer van Volksverteenwoordigers (Belgian Chamber of Representatives), DOC 54, 1567/001, pp. 5-7.

have the technical means to keep abreast of the explosion of new means of communication which criminals and persons of evil intent are so keen to use.

27. It should be noted that providers of electronic communications services for *commercial purposes* keep masses of personal data relating to their customers. Users of social media, communication apps and even on-line games declare their agreement to the providers gaining access to their contact lists, photos, location and suchlike in order to be able to make use of those commercial services. This allows the providers to compile detailed profiles of their users and on that basis to send targeted advertisements and to make suggestions with regard to services.

28. It will certainly be argued that the difference is that that type of data processing takes place with the user's consent. However, the Belgian Government is of the view that such consent is always more relative, on the one hand, due to the complexity of the clauses and, on the other hand, because those instruments are indispensable to the social life of ever more citizens. On the other hand, it must also be stated that for a large proportion of the population such — more or less informed — consent for the processing of bulk data for commercial reasons is indicative of a fundamental evolution in the sphere of privacy and that case-law does not always take this into account.

29. In order to guarantee the *safety of citizens*, the intelligence agencies in their turn would like to make use of well-defined information which the providers have at their disposal. Belgian legislation requires the retention of certain electronic communications data (datasets), for twelve months [7]: data on the identity of users and their means of communication (gsm, fixed telephony, email address, IP address), who communicates with whom and where the devices are located. The legislation does not require the providers to retain the content of telephone, messaging or internet communications. The obligatory retention of data (data retention) is limited to the metadata.

30. EU Member States have an obligation to protect their citizens and must use all available means to guarantee their safety: the intelligence agencies are responsible for national security. It is important for those agencies that the providers of electronic communications services keep extensive datasets, naturally with the necessary guarantees for their safety, confidentiality and accuracy. An extensive retention duty is necessary and permissible in a democratic society, provided that access to such information is very strictly controlled by an independent body. Law enforcement and intelligence agencies may only request those data which are strictly necessary for the execution of their duties, with respect for the principles

[7] Article 126 of the wet van 13 juni 2005 betreffende de elektronische communicatie (Law of 13 June 2005 on electronic communication), inserted by the wet van 19 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie (Law of 19 May 2016 on the collection and retention of data in the electronic communications sector), *B.S.*, 18 December 1998. As a result of the *Tele2 & Watson* judgment, the latter Law was challenged before the Belgian Constitutional Court, Joined Cases Nos 6599, 6601, 6590 and 6597.

of proportionality and subsidiarity and in compliance with strict procedural guarantees.

31. The Belgian Government is of the opinion that a general retention duty is permissible if access is strictly controlled. As far as Belgium is concerned, the wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (Law of 30 November 1998 on the regulation of the intelligence and security agencies; 'WIV') [8] makes provision for a sound system which satisfies the requirements of Article 8 ECHR.

32. In that Belgian law the request for traffic and location data is regarded as a specific method of gathering information (Article 18/8 WIV). Such a method may be employed only if a method which is less privacy intrusive does not suffice (principle of subsidiarity) and if it is proportionate to the potential threat being investigated (principle of proportionality) (Article 18/3 WIV). Moreover, access to the data is modulated as a function of the nature of the threat:

> 1. only in the case of a threat relating to terrorism or extremism can historical information regarding the preceding 12 months be requested;
>
> 2. in the case of threats relating to espionage, interference in decision processes, the activities of foreign intelligence agencies and the distribution of weapons of mass destruction, information for a maximum period of 9 months may be requested;
>
> 3. in the case of a threat emanating from criminal organisations or harmful sectarian organisations, only data for a maximum period of 6 months may be requested.

33. Article 18/3 WIV lays down the procedure for requesting communications data: that specific method may only be employed after a written and reasoned decision by the agency head and after the notification of that decision to the commission charged with supervising the specific and exceptional intelligence methods ('the Commission'). The decision must mention, inter alia, the following elements:

> - the natural persons or legal persons, the associations or groupings, the objects, places, events or information which are the subject of the specific method;
>
> - the potential threat which justifies the use of the specific method;
>
> - the factual circumstances which justify the use of the specific method, the reasoning with regard to subsidiarity and proportionality, including the connection between the two;

[8] *B.S.*, 20 June 2005.

- the period for which the specific method may be used, calculated from the time of the notification of the decision to the Commission;

- the name(s) of the intelligence officer(s) responsible for monitoring the use of the specific method;

- if applicable, the concurrence with a criminal or judicial investigation;

- the justification for the length of the period relating to the collection of traffic and location data.

(b) Impact of the *Tele2 & Watson* judgment

34. The Belgian Government is of the opinion that the requirements which the Court of Justice imposes with regard to the retention of metadata for the purpose of fighting crime has an immediate and direct impact on the operation of the law enforcement agencies. In the case of cybercrime, for example, where the perpetrator leaves only digital traces, investigation is possible solely on the basis of digital communications data. If these are not retained or not retained for long enough, further investigation is impossible. When the body of a missing person is found only a year after his or her disappearance, it is impossible to detect on the basis of gsm signals who was in the vicinity at the time of that person's disappearance or death.

35. It must be pointed out that in the *Tele2 & Watson* judgment the Court of Justice did not give a ruling on the retention of metadata for the purpose of protecting national security. After all, those agencies have a different goal to the police services and the judicial authorities.

36. Intelligence agencies can be differentiated from police services by the fact that their activities are not crime-oriented and that they do not collect criminal evidence. They look for trends, activities, persons or organisations which may pose a threat to the State but in respect of which there is not necessarily any evidence of criminal offences. The information which an intelligence agency makes available to the State does not have any particular evidential value and may only serve as initial information or supporting evidence. No one can be convicted purely and solely on the basis of information obtained from an intelligence agency. Given the specific nature of intelligence work, a limited retention duty, as required by the Court of Justice, is thus unworkable:

   – Limiting the data to be retained to certain categories of persons leads to the stigmatising of certain ethnic groups and is discriminatory.

   – A geographic limitation is not possible. One cannot predict in advance where activities which pose a threat to the State will occur. People can in fact adapt their behaviour if they are aware of geographic criteria.

– The analysis of metadata enables the elimination of certain lines of thought so that the agency can focus on the real threats. In that way the intelligence agency can set to work in a more targeted fashion, thus also providing an additional guarantee to avoid the investigation of persons who cannot possibly be involved in any way.

– The investigation of the data of all means of communication may be relevant (mobile, fixed and internet telephony). If only mobile telephone data is kept, ill-intentioned persons could switch to internet telephony.

– Identification, traffic and location data are all relevant. It is therefore important that all those categories of data are kept.

37. The arguments set out above show with ample clarity that the intelligence and security agencies would be effectively crippled if the Court of Justice were to be of the opinion that the conditions laid down in the *Tele2 & Watson* judgment also apply to the retention of communications data for the purpose of national security. The intelligence and security agencies would be cut off from an important source of information.

V. CONCLUSION

38. Taking the foregoing into account, the Belgian Government proposes that the Court of Justice should consider answering the first question referred for a preliminary ruling along the following lines:

1. Having regard to Article 4 TEU and Article 1(3) of Directive 2002/58/EC concerning privacy and electronic communications, a request to a provider of an electronic communications network to store communications data and provide those data to the security and intelligence agencies falls outside the scope of EU law.

2. Primarily, the Belgian Government is of the opinion that the second question referred for a preliminary ruling is devoid of purpose.

However, if the Court of Justice should answer the first question in the affirmative, the Belgian Government submits in the alternative that the *Tele2 & Watson* requirements or other requirements do not apply to the acquisition of communications data by the security and intelligence agencies. This is because the acquisition of communications data by those agencies pursues a different goal to that of fighting serious crime and is accompanied by adequate guarantees.

Brussels, 14 February 2018

Jean-Christophe HALLEUX Pierre COTTIN

Agents of the Belgian Government