EUROPEAN COURT OF HUMAN RIGHTS

FOURTH SECTION

Application No 37050/22

Foreningen imod Ulovlig Logning v Denmark

REPLY TO GOVERNMENT'S OBSERVATIONS

1. On 20 January 2023, the Court communicated the above-mentioned application to the Government.

2. On 11 July 2023, the Government provided its Observations, and on 31 July 2023 the Court forwarded these Observations to the representatives of the applicant and invited them to reply to the Observations by 10 November 2023, together with their claims for just satisfaction.

3. This document constitutes the applicant's submissions in response to the Government's Observations and sets out the applicant's just satisfaction claim. It is noted that the applicant has also filed a request for the relinquishment of jurisdiction to the Grand Chamber pursuant to Article 30 of the Convention, see directly below.

I. Request for Relinquishment of Jurisdiction to the Grand Chamber

4. As noted by Judges Lemmens, Vehabović and Bošnjak in their partially dissenting opinion in *Big Brother Watch and Others*: "There are rare occasions when the Court adjudicates on a case which shapes the future of our societies. The present one is such an example." (*Big Brother Watch and Others v the United Kingdom* [GC], Appl Nos 58170/13, Jointly Concurring Opinion, para 30, 25 May 2021). The applicant submits that this case presents yet another occasion for the Court to consider the societal implications of the bulk retention of communications data. Although the harm associated with bulk surveillance is difficult to quantify, it is of a nature to potentially undermine the effective functioning of a democratic society. As the Court has stated "a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it" (*Roman Zakharov v Russia*, Appl No 47143/06, para 231, 4 December 2015).

5. The collection and retention of data associated with millions of people, almost all of whom are law-abiding and engaged in normal daily life, exert a profound impact on the workings of a democratic society. Bulk monitoring lifts millions of people into the realm of the potentially suspicious. In such circumstances, suspicion does not precede data collection. Rather, suspicion is generated through the analysis of the data itself. Such practices raise important questions regarding the role of safeguards.

6. The applicant observes that the Court has so far focused on the impact of surveillance in the context of the right to privacy and press freedom, and on the Government sharing the material with other governments and agencies. However, numerous other rights may also be affected, and the impact on these rights may be particularly acute in the context of bulk retention and the advent of artificial intelligence (AI). The present case is, at its core, a prime example of a government that has refused to adhere to the decisions of the Court, and the decisions of the Court of Justice of the European Union (CJEU), and the apparent inability of the national courts to uphold and apply those decisions. In the view of the applicant, it is thus

also necessary for the Court to examine and clarify the role of the national courts, when governments seek to avoid complying with the Convention.

7. For these reasons, it is submitted that the present case raises serious issues of general importance affecting the interpretation of the Convention and the applicant kindly requests that the Chamber relinquish jurisdiction in favour of the Grand Chamber as authorised by Article 30 of the Convention.

II. Admissibility

II.A *Preliminary Remarks Regarding Victim Status and Non-exhaustion of Remedies*

8. The Government has accepted that there has been and still is an (ongoing) interference with the applicant's rights under Article 8 of the Convention, as the applicant's correspondence was retained and is still stored under the retention scheme (Government's Observations, para 38).

9. The applicant reads the initial observations (ibid) to mean that the Government does not dispute the applicant's "victim status" under Article 8 of the Convention. In addition, it is now settled case-law that an applicant may claim to be the victim of a violation of his or her Convention rights by the mere existence of legislation permitting secret surveillance measures where "legislation directly affects all users of communication services by instituting a system where any person can have his communications intercepted" (*Centrum för rättvisa v Sweden*, Appl No 35252/08, para 167, 25 May 2021 and *Roman Zakharov v Russia*, cited above, para 171). Therefore, **question No 1 to the Parties** is partially affirmed by the Government. The affirmation deals both with the previous and current surveillance and retention schemes. In addition, victim status is clear from the Court's case law, as the disputed legislation directly affects all users of communication services in Denmark (cf paras 25-28, below).

10. Not surprisingly the applicant agrees with the Government's assertion on victim status, as stated in the original application. Reference is made to *Ekimdzhiev and Others v Bulgaria*, Appl No 70078/12, para 374, 11 January 2022, in which the Court held that *"*it is settled that the communications of legal persons are covered by the notion of 'correspondence' in Article 8 § 1 of the Convention" (Government's Observations, para 38).

11. The Government has not made any specific objections in regard to Articles 10 and 13 of the Convention (Government's Observations, paras 80 and 138-140). The applicant therefore assumes that the parties concur on the applicability of Articles 10 and 13 to the current case.

12. The Government has, however, submitted that the application (presumably as a whole) should be declared inadmissible due to the non-exhaustion of domestic remedies both in regard to the previous and current surveillance and retention schemes.

13. The applicant submits that the application should be declared admissible.

14. The applicant instituted civil proceedings at the national courts where the applicant's claims were denied. The Danish courts failed to assess the compatibility of the national surveillance and retention scheme in any particular detail with the Convention (and with EU law). The Supreme Court's ruling demonstrates the absence of an effective legal recourse within the national framework for cases pertaining to retention and surveillance.

II.B *Exhaustion of Domestic Remedies*

15. The applicant's case was initiated before the City Court on 1 June 2018 and referred to the Eastern High Court on 28 September. The referral was due to the principal nature of the complaint, in accordance with Section 226 of the Administration of Justice Act. The said provision also requires that the referred case is deemed to be of general significance for the application of the law and legal development or significant for the society. The applicant would in this respect submit at the outset that the referral in itself seems to undermine the suggestions made by the Government that it was clear from the outset that the applicant's lawsuit would fail due to the procedural choices made by the applicant (Government's Observations, para 62-74).

16. In the proceedings before the Eastern High Court, the applicant made the following two claims:

> (1) Executive Order No. 988 of 28 September 2006 on the Retention and Storage of Traffic Data by Providers of Electronic Communications Networks and Services is invalid,
>
> And
>
> (2) The Defendant has not seen to the termination of the invalid state of the law created by Executive Order No. 988 of 28 September 2006 on the Retention and Storage of Traffic Data by Providers of Electronic Communications Networks and Services as soon as possible." (see Exhibit 2, page 2, as provided by the Government).

17. Due to the outcome of the proceedings before the Eastern High Court, the applicant modified their claims before the Danish Supreme Court:

> *Claim 1*
>
> The Defendant, Minister for Justice Nick Hækkerup, the Ministry of Justice, must admit:
>
> Primary claim: that Executive Order No. 988 of 28 September 2006 on the Retention and Storage of Traffic Data by Providers of Electronic Communications Networks and Services ('the Retention Order') is invalid or, in the alternative, was invalid.
>
> First alternative claim: that sections 1, 4, 5 and/or 6 of the Retention Order are invalid
>
> or, in the alternative, were invalid.

Second alternative claim: that the Retention Order is inapplicable or, in the alternative, was inapplicable.

Final alternative claim: that sections 1, 4, 5 and/or 6 of the Retention Order are inapplicable or, in the alternative, were inapplicable.

Claim 2

Minister for Justice Nick Hækkerup, the Ministry of Justice, must admit his failure to fulfil his duty to bring the Danish rules on retention into compliance with EU law as soon as possible after the delivery of the judgment by the European Court of Justice on 8 April 2014 in joined cases C-293/12 and C-594/12 (*Digital Rights Ireland and Others*), or in the first alternative, after delivery of the judgment by the European Court of Justice on 21 December 2016 in joined cases C-203/15 and C-698/15 (*Tele2 and Others*) or in the second alternative, after delivery of the judgment by the European Court of Justice on 6 October 2020 in joined cases C-511/18, C-512/18 and C-520/18 (*La Quadrature du Net and Others*) (See Exhibit 3, page 1-2, as provided by the Government)

18. The Government argues that the proceedings initiated by the applicant related to an "abstract assessment" of Danish law, a process not accommodated by the current provisions of Danish procedural legislation (Government's Observations, para 39).

19. According to the Government, the applicant could "very easily have used the domestic remedies available to it for the specific retention of the applicant's data and have brought a tort action or similar proceedings." (ibid). The Government conveniently neglects to provide any examples of tort law successfully being used by domestic courts to "order" the Government "from applying the national rule that is found to be contrary to, for example, EU law or human rights obligations" (Government's Observations, para 40). Similarly, the Government fails to provide any example of what "similar proceedings" that were or could have been available to the applicant.

20. According to the Court's case law, it is incumbent on the Government claiming non-exhaustion of domestic remedies to satisfy the Court that there was an existing remedy and that this remedy was an effective one, available in theory and in practice at the relevant time (*Vučković and Others v Serbia* (preliminary objection) [GC], Nos 17153/11 and 29 others, para 77, 24 March 2014 and *Akdivar and Others v Turkey,* Appl No 21893/93, para 68, 16 September 1996).

21. The obligation to exhaust domestic remedies requires an applicant to make normal use of remedies which are available and sufficient in respect of the relevant grievances. The existence of the remedies in question must be sufficiently certain not only in theory but in practice. In failing to meet these requirements, they will lack the requisite accessibility and effectiveness (*Vučković and Others*, cited above, para 71 and *Akdivar and Others*, cited above, para 66).

22. In addition, the Court has frequently underlined the need to apply the exhaustion rule with some degree of flexibility and without excessive formalism (*Vučković and Other*s, cited above, para 76; and *Akdivar and Others*, cited above, para 69).

23. The applicant observes that the Government has failed to provide any evidence that an effective remedy was available in practice at the relevant time. This is so because there exist no examples in Danish court practice in which a claimant was able to stop the Government from using an unlawful law or obtain damages due to the Danish data retention scheme. If there had been any examples the Government would surely have cited these.

24. In this regard, the applicant observes that due consideration must be had to the special character of the present case: a total and complete data retention scheme in which no differentiation or assessment of proportionality was or is taking place.

II.C *Sixteen Years of General and Indiscriminate Data Retention*

25. Retention first happened under Executive Order 988 of 28 September 2006 the Retention and Storage of Traffic Data by Providers of Electronic Communications Networks and Services (*logningsbekendtgørelsen*), which came into force on 15 September 2007. This was the Order that the applicant contested in domestic proceedings. Under Executive Order No 988, the "detailed rules" for the retention and storage of traffic data by telecommunication service and network providers were established (Government's Observations, para 11). This Executive Order worked in pursuance with Section 786(4) of the Administration of Justice Act, which obliged telecommunication network and service providers to retain and store communications[1] data for one year for use in criminal investigations and prosecutions (Government's Observations, para 10).

26. Executive Order 988 was amended by Executive Order No 660 of 19 June 2014. The amendment repealed the rules on the retention of session data and meant "that providers of electronic communications networks and services for end users had to retain and store telecommunication traffic data generated or processed in their networks so that such data could be used in criminal investigations and for the prosecution of criminal offences" (Government's Observations, paras 12-13). Under the amendment, the "contents of communications did not have to be retained and stored" (ibid). The rules were revised again by Amendment Act No 291 of 8 March 2022, because the data retention scheme was contrary to EU law as it allowed for access to traffic data and location data generally and indiscriminately retained and stored (Government's Observations, para 23; cf *G.D. v Commissioner of An Garda Síochána* (Case C-140/20), para 123).

[1] Consistent with the terminology of the Court, these pleadings will adopt the term "communications data" rather than "traffic data", as referred to in Danish law, or "meta data", a term occasionally used in the relevant literature.

27. But the fact that certain parts of the Danish data retention scheme were contrary to EU law did not lead to the conclusion that the rules were generally inapplicable. Nor did the Government halt the generally and indiscriminately retention of communications data. Instead, according to the Government, domestic courts and authorities simply had to "refrain from applying the national provisions that were found to be contrary to EU law" (Government's Observations, para 44). This position was confirmed by the Supreme Court (ibid). Yet, this finding is contrary to the Court's position in *Big Brother Watch and Others* (*Big Brother Watch and Other* [GC]*,* cited above, paras 518-522). Therefore, **question No 2 to the Parties** is settled in the Court's case law and the Supreme Court judgment of 30 March 2022 failed to uphold Articles 8, 10 or 13 of the Convention.

28. The latest amendments, currently in force, provided for two schemes. Under the first scheme, service providers can be ordered to perform communications data retention relating to specific persons and geographical locations in connection with efforts to combat serious criminal offences. Under the second scheme, service providers can be ordered to perform a "general and indiscriminate retention of traffic data" of all telecom customers in Denmark lasting one year when there are "reason to assume that Denmark faces a serious threat to national security that is deemed to be genuine and present or foreseeable" (Government's Observations, para 22). The latter power has been in use since 30 March 2023 and will continue to be in use until 29 March 2024 (ibid). This means that despite the Government's alleged adherence to EU law, there has in reality been no change and the Government is still ordering a general and indiscriminate retention of all communications data. The only change is that this is now done with a spurious reference to "national security". A threat that despite being unspecified and subject to no effective review of any kind is expected to last one year.

29. The applicant observes that it never had and still has no interest in monetary compensation. Nor is there any case law suggesting that the applicant would be able to claim non-pecuniary damage. In accordance with the stated aim of *Foreningen imod Ulovlig Logning*, the applicant had and still has an interest in halting the invasive data retention scheme in Denmark. In this regard, the applicant observes that the Court's case law suggests that a declaration of a violation would constitute just satisfaction in cases concerning bulk retention and secret surveillance, see e.g. *Centrum för rättvisa v Sweden*, Appl No 35252/08, paras 378-380, 25 May 2021; *Association for European Integration and Human Rights and Ekimdzhiev and Others v Bulgaria*, Appl No 62540/00, paras 109-111, 28 June 2007; *Ekimdzhiev and Others v Bulgaria,* cited above, paras 426-428; and *Roman Zakharov v Russia*, cited above, paras 309-312. In the latter case, the Court *inter alia* stated:

> 311. The Court reiterates that, in the context of the execution of judgments in accordance with Article 46 of the Convention, a judgment in which it finds a violation of the Convention or its Protocols imposes on the respondent State a legal obligation not just to pay those concerned any sums awarded by way of just satisfaction, but also to choose, subject to supervision by the Committee of Ministers, the general and/or, if appropriate, individual measures to be adopted in its domestic legal order to put an end to the violation

found by the Court and make all feasible reparation for its consequences in such a way as to restore as far as possible the situation existing before the breach. Furthermore, in ratifying the Convention, the Contracting States undertake to ensure that their domestic law is compatible with it (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, para 111, with further references).

312. The Court considers that **the finding of a violation constitutes sufficient just satisfaction for any non-pecuniary damage caused to the applicant**. (emphasis added)

30. The ruling by the Danish Supreme Court in case U.2017.2929H established that any tort claim alleging violations of the Convention is unlikely to succeed unless the claimant can demonstrate an entitlement to monetary compensation as stipulated in Article 41 of the Convention. In other words, if the European Court of Human Rights has rejected claims for non-pecuniary damage, the claimant would fail if he initiated a suit in tort proceedings under Danish law. This was exactly what happened in U.2017.2929H. In this case, the Supreme Court found against an individual who raised a claim for tort for violations of Article 2 of Protocol 4 to the Convention since the case law of the European Court of Human Rights did not substantiate that the claimant was eligible for non-pecuniary damage. The majority of the Supreme Court (7-1) *inter alia* held:

DANISH:

Højesteret fastslog ved dom af 1. juni 2012 (- - -), at udlændingemyndighedernes afgørelser om at pålægge A opholds- og meldepligt i Center Sandholm »i hvert fald på nuværende tidspunkt udgør« et uproportionalt indgreb i hans bevægelsesfrihed i strid med artikel 2 i Den Europæiske Menneskerettighedskonventions Tillægsprotokol 4. Denne sag angår, om han har krav på en godtgørelse som følge af denne krænkelse

…

Der ses ikke at være domme fra Menneskerettighedsdomstolen, der tager stilling til proportionaliteten af indgreb i bevægelsesfriheden over for personer på tålt ophold, og derfor heller ikke domme, der tager stilling til spørgsmålet om godtgørelse for et sådant indgreb

…

Efter Menneskerettighedsdomstolens praksis er det ikke enhver krænkelse af konventionen, der medfører krav på godtgørelse. Det følger således af Domstolens dom af 18. september 2009 i sag 16064/90 (*Varnava og andre mod Tyrkiet*), at der må sondres mellem de tilfælde, hvor krænkelse har medført bl.a. »evident trauma, whether physical or psychological, pain and suffering, distress, anxiety, frustration, feelings of injustice or humiliation, prolonged uncertainty, disruption of life«, og de tilfælde, hvor en anerkendelse af den krænkelse, som er overgået klageren, er »a powerful form of redress in itself.« Det fremgår endvidere, at i mange tilfælde, hvor en lov, procedure eller praksis ikke lever op til konventionen, er en konstatering heraf tilstrækkelig til at rette op på forholdet, mens krænkelsen i andre tilfælde har haft en sådan påvirkning af klagerens »moral well-being«, at der er behov for yderligere oprejsning, herunder i form af en godtgørelse.

…

…De danske domstole har - i modsætning til de nationale domstole i sagen Sarkizov og andre mod Bulgarien - således foretaget en individuel proportionalitetsvurdering, som førte til, at Højesteret ved dommen af 1. juni 2012 konstaterede, at der var sket en krænkelse af A's ret til bevægelsesfrihed, og til, at denne krænkelse blev bragt til ophør. Udlændingemyndighederne har efter dommen anvendt de kriterier, Højesteret har opstillet for proportionalitetsvurderingen, ved deres regelmæssige vurderinger af, om opholds- og meldepligt pålagt udlændinge på tålt ophold skal lempes eller ophæves.

Uanset om indgrebet i A's bevægelsesfrihed i en kortere periode forud for dommen af 1. juni 2012 ikke længere opfyldte proportionalitetsbetingelsen, finder vi på den anførte baggrund, at det udgjorde et tilstrækkeligt effektivt retsmiddel efter konventionens artikel 13, at Højesteret konstaterede krænkelsen og fik den bragt til ophør. Vi har herved endvidere lagt vægt på, at den frustration, angst, usikkerhed og forstyrrelse af tilværelsen, som A måtte have oplevet under perioden med opholds- og meldepligt i Center Sandholm, i vidt omfang må antages at skyldes ikke opholds- og meldepligten, men udvisningen. Udvisningen indebar som nævnt bl.a., at han ville blive udsendt til Iran, hvis det viste sig muligt, at han ikke måtte tage arbejde i Danmark, og at han kun i meget begrænset omfang havde ret til sociale ydelser. Vi har endelig lagt vægt på, at den periode, hvor A har haft opholds- og meldepligt i Center Sandholm, er indgået ved vurderingen af, at udvisningen af ham skulle ophæves, således at han også derved har fået en kompensation for den skete krænkelse.

Vi stemmer derfor for at tage Udlændingestyrelsen og Udlændinge- og Integrationsministeriets påstand til følge.

…

Konklusion og sagsomkostninger
Højesteret frifinder herefter Udlændingestyrelsen og Udlændinge- og Integrationsministeriet og tager påstanden om tilbagebetaling til følge, idet det bemærkes, at der ikke er gjort indsigelse mod rentepåstanden.

Efter sagens karakter finder Højesteret, at ingen part skal betale sagsomkostninger til nogen anden part for byret, landsret og Højesteret.

Thi kendes for ret
Udlændingestyrelsen og Udlændinge- og Integrationsministeriet frifindes.

UNOFFICIAL TRANSLATION:

The Supreme Court ruled by judgment of 1 July 2012 (---) that the immigration authorities' decisions to impose on a duty to reside and report at the Sandholm Center "at least at the present time constitute" disproportionate interference with his freedom of movement in violation of Article 2 of Protocol 4 to the European Convention on Human Rights. This case concerns whether he is entitled to compensation as a result of this infringement

…

There do not appear to be any judgments from the European Court of Human Rights that address the proportionality of interferences with the freedom of movement for persons under tolerated stay,

and thus no judgments that address the question of compensation for such an interference

…

According to the practice of the European Court of Human Rights, not every violation of the Convention gives rise to a claim for compensation. Thus, it follows from the Court's judgment of *Varnava and others v Turkey* [GC] Appl Nos 16064/90, 16065/90, 16066/90 et al., 18 September 2009 that a distinction must be made between cases where the violation has resulted in, among other things, "evident trauma, whether physical or psychological, pain and suffering, distress, anxiety, frustration, feelings of injustice or humiliation, prolonged uncertainty, disruption of life," and cases where recognition of the violation suffered by the complainant is "a powerful form of redress in itself." **(***Varnava and others v Turkey* [GC], cited above, para 224). **It is also evident that in many cases where a law, procedure, or practice does not comply with the Convention, a finding to this effect is sufficient to remedy the situation, while in other cases, the violation has had such an impact on the complainant's "moral well-being" that further redress is necessary, including in the form of compensation.**

…

…In contrast to the national courts in the case of *Sarkizov and others v Bulgaria,* Appl Nos 37981/06, 38022/06, 39122/06 and 44278/06, 1 June 2006 the Danish courts have thus conducted an individual proportionality assessment, which led the Supreme Court to establish, in its judgment of 1 June 2012, that there had been a violation of A's right to freedom of movement and that this violation had been brought to an end. Following the judgment, the immigration authorities have applied the criteria set out by the Supreme Court for the proportionality assessment in their regular assessments of whether the residence and reporting obligations imposed on tolerated stay foreigners should be relaxed or lifted.

Regardless of whether the interference with A's freedom of movement in the period leading up to the judgment of 1 June 2012 no longer met the proportionality requirement, we find, on the basis stated, that it constituted a sufficiently effective remedy under Article 13 of the Convention that the Supreme Court established the violation and brought it to an end. We have also taken into account the frustration, anxiety, uncertainty, and disruption of life that A may have experienced during the period of residence and reporting obligations at the Sandholm Center, which to a large extent may be attributed not to the residence and reporting obligations but to the expulsion. As mentioned, the expulsion meant, among other things, that he would be sent back to Iran if it turned out that he could not work in Denmark and that he had only very limited access to social benefits. Finally, we have considered the period during which A had residence and reporting obligations at the Sandholm Center in the assessment that his expulsion should be lifted, so that he has also received compensation for the violation that occurred.

Therefore, we vote to grant the claim of the Danish Immigration Service and the Ministry of Immigration and Integration.

…

Conclusion and Costs
Therefore, the Supreme Court finds for the Immigration Service and the Ministry of Immigration and Integration and allows the claim for repayment, noting that no objection has been made to the claim for interest.

Given the nature of the case, the Supreme Court finds that no party shall pay legal costs to any other party for the district court, the court of appeals, or the Supreme Court.

Thus, is ruled
The Immigration Service and the Ministry of Immigration and Integration are acquitted.

31. The applicant contends that, in a situation like the present case, a tort claim would have no chance of success, thus failing to serve as an effective legal remedy. This assertion is supported by the precedent established in the aforementioned ruling by the Danish Supreme Court.

32. The argument is also supported by a later - rather peculiar - case before the Danish Supreme Court, U.2021.3343H, where an individual (the claimant) raised a claim for compensation (tort) in the amount of 150.000 DKK, due to an alleged violation of her right to property under Protocol 1, Article 1. The claimant, who was supported by the Danish Bar and Law Society (*Advokatsamfundet*), alleged non-compliance by a local municipality with a decision by a higher authority (*Ankestyrelsen*) granting the claimant a right to social pedagogical support (*socialpædagogisk støtte*) during her participation in swimming competitions. She submitted that a violation of Protocol 1, Article 1, had occurred and that she was therefore entitled to compensation. The Supreme Court found against the claimant and stated regarding the applicant's Convention rights:

DANISH:

…
Hvis der foreligger en krænkelse af Menneskerettighedskonventionen eller tilhørende protokoller, følger det af artikel 13 i Menneskerettighedskonventionen sammenholdt med princippet i erstatningsansvarslovens § 26, at der skal tilkendes en godtgørelse, hvis vedkommende i henhold til Menneskerettighedsdomstolens praksis efter konventionens artikel 41 ville have ret til godtgørelse, jf. bl.a. Højesterets domme af 21. juni 2017 (UfR 2017.2929) og 10. september 2019 (UfR 2019.4010).

Efter Menneskerettighedsdomstolens praksis er det ikke enhver krænkelse af konventionen, der medfører krav på godtgørelse. Det følger således af Domstolens dom af 18. september 2009 i sag nr. 16064/90 (Varnava og andre mod Tyrkiet), præmis 224, at det i mange tilfælde, hvor en lov, procedure eller praksis ikke lever op til konventionen, er tilstrækkeligt at rette op på forholdet ved at konstatere krænkelsen, mens der i andre tilfælde er behov for yderligere oprejsning, herunder i form af en godtgørelse

…
Der ses ikke at være domme fra Menneskerettighedsdomstolen, der belyser, om og i givet fald under hvilke omstændigheder begrebet ejendom i artikel 1 omfatter et tilfælde som det foreliggende, hvor Ankestyrelsens afgørelse af 6. juli 2016 indebar en ret til efter kommunens undersøgelse af det nærmere behov at få tildelt en støtteperson ved deltagelsen som svømmer i visse stævner.

Uanset om det foreliggende tilfælde måtte være omfattet af artikel 1, finder Højesteret, at der ikke vil være krav på godtgørelse som følge af kommunens undladelse af at efterleve Ankestyrelsens afgørelse. Det bemærkes herved, at der er sket en oprejsning ved, at Ankestyrelsen i sin afgørelse af 29. maj 2017 kritiserede, at kommunen ikke havde fulgt styrelsens afgørelse, hvilket førte til, at kommunen derefter tildelte hende en støtteperson. Hertil kommer, at A i den omhandlede periode deltog i de pågældende

svømmestævner uden en støtteperson, og at hun desuden deltog i svømmestævner i Danmark og udlandet, som hun ikke havde ansøgt om at få en støtteperson til. Der er heller ikke nærmere oplysninger om andre konsekvenser for hende.

Konklusion og sagsomkostninger

Højesteret tiltræder, at A ikke har ret til godtgørelse efter erstatningsansvarslovens § 26, stk. 1, eller princippet heri, og stadfæster derfor landsrettens dom.

UNOFFICIAL TRANSLATION:

…

If there is a violation of the Human Rights Convention or its related protocols, it follows from Article 13 of the Human Rights Convention in conjunction with the principle in Section 26 of the Tort Liability Act that compensation must be awarded if the person, according to the practice of the European Court of Human Rights under Article 41 of the Convention, would be entitled to compensation, (cf among others, the Supreme Court judgments of 21 June 2017 (UfR 2017.2929) and 10 September 2019 (UfR 2019.4010)).

According to the practice of the European Court of Human Rights, not every violation of the convention entails a claim for compensation. It follows, for example, from the Court's judgement of 18 September 2009 in *Varnava and others v. Turkey,* Appl No 16064/90, para 224 that in many cases where a law, procedure, or practice does not comply with the Convention, it is sufficient to remedy the situation by establishing the violation, while in other cases there is a need for further redress, including compensation.

...

There do not appear to be any judgments from the European Court of Human Rights that clarify whether, and if so, under what circumstances the concept of property in Article 1 includes a case such as the present one, where the decision of the Board of Appeal of 6 July 2016 entailed a right, after the municipality's investigation of the specific needs, to be assigned a support person for participation as a swimmer in certain competitions.

Regardless of whether the present case may be covered by Article 1, the Supreme Court finds that there is no claim for compensation as a result of the municipality's failure to comply with the decision of the Board of Appeal. It is noted in this regard that there has been redress in that the Board of Appeal in its decision of 29 May 2017 criticised the municipality for not following the Board's decision, which led to the municipality subsequently assigning her a support person. In addition, A participated in the relevant swimming competitions during the period in question without a support person, and she also participated in swimming competitions in Denmark and abroad for which she had not applied for a support person. There are also no further details about any other consequences for her.

Conclusion and costs

The Supreme Court agrees that A is not entitled to compensation under Section 26(1) of the Tort Liability Act or the principle therein and therefore upholds the decision of the Court of Appeal.
… (emphasis added)

33. Thus, the Supreme Court did not have to rule on the substance of the Convention complaint since the claimant would not be entitled to compensation under Article 41. The claimant

therefore lost the case and was liable to pay costs. In the view of the applicant, the case confirms that raising a claim in tort would not be sufficiently "certain in law and in practice" and would have no "reasonable prospects of success" as the applicant would not be eligible for compensation. The applicant recalls that, according to the Court's case law, an applicant in a case such as the present one would *not* be entitled to compensation (para 29, above), and thus Danish courts would not rule on the substance of the applicant's Convention complaints.

34. The Government has also made reference to U.2017.1243H concerning practice in discovery proceedings, arguing that the case serves as an example of an effective remedy (Government's Observations, para 76). Yet in this case the Supreme Court only found that the Ministry of Employment was liable to pay compensation to the plaintiff for the Government's failure to revise a statute (the Holiday Act) to make it in accord with EU law (Directive 2003/88/EC concerning certain aspects of the organisation of working) in a timely manner. The Supreme Court did not order the Government to stop an unlawful practice.

35. The Government further made reference to case U.2019.2019Ø (Government's Observations, para 77). The applicant cannot see how this judgement demonstrates the availability of an effective remedy to the applicant. The case concerned a civil dispute pertaining to alleged copyright infringements. The claimant, a private party, requested the Danish courts to issue a discovery order against two teleservice providers. This order was sought for the disclosure of the identity of more than 4,000 IP addresses, which, according to the claimant, were involved in the illegal sharing of copyrighted material.

36. The High Court rejected the request for a discovery order only because the teleservice providers objected. The applicant contends that U.2019.2019Ø does not constitute a pertinent precedent and fails to exemplify an instance where a claimant has achieved legal standing or secured a substantive review of the applicant's grievances.

37. If the Court accepts that U.2019.2019Ø would demonstrate that effective remedies were available, the Court would at the same time accept that a Member State's adherence to the Convention (or EU Law) depends solely on the favour of the private teleservice provider's willingness to object to disclosure requests from the authorities.

38. The applicant notes that U.2019.2019Ø in fact demonstrates the possibility that a private party involved in a civil dispute could be granted access to information gathered in contravention of EU law. This is noteworthy given that the data in question was exclusively collected and retained for utilisation in criminal investigations and proceedings, in accordance with Section 786 of the Administration of Justice Act. Thus, rather than support the Government's position, it seems to provide an example of how egregious the use of retained data is in Denmark (cf *Procedure for Obtaining Access*, paras 106-119).

39. The applicant observes that the Danish Supreme Court ruled on 4 October 2023 (Case No 59/2022) that any data collected in violation of EU law and/or the EU Charter, due to

undifferentiated data retention, would not automatically be precluded from being used as evidence in criminal proceedings. The ruling serves to show that even Article 8 complaints raised in criminal proceedings regarding the use of surveillance measures would not prompt the Danish courts to perform any examination of the substance of the Article 8 complaint and would thus not constitute an effective remedy.

40. The applicant further observes that the Court has continuously held that proceedings, where national courts are only empowered to examine questions relating to the admissibility of evidence, are not capable of providing an effective remedy (cf *Hambardzumyan v Armenia*, Appl No 43478/11, paras 40-44, 5 December 2019).

41. Should the Court find that the applicant ought to have worded its claims differently before the national courts or raised a separate claim for compensation to be able to exhaust domestic remedies, the applicant submits that the Supreme Court did – albeit succinctly – examine the substance of the applicant's Convention complaint (cf *Verein gegen Tierfabriken Schweiz (VgT) v Switzerland* (No 2), Appl No 32772/02, paras 43-44, 30 June 2009). Both the High Court and the Supreme Court found that the applicant's claim No 1 regarding the validity of Executive Order No 988 of 28 September 2006 as a whole was admissible. The national courts found in favour of the Minister of Justice since there were no grounds for claiming the Executive Order invalid as a whole or even partially, rejecting the applicant's legal arguments under EU law and/or the Convention as it could not be ruled out that the Executive Order on Data Retention is invalid in all circumstances. It is noted, this reading is in contradiction of EU law (cf *An Garda Síochána* (Case C-140/20), cited above, para 123).

42. Finally, the applicant would like to note that the Danish Minister of Justice acknowledged during an open consultation (*åbent samråd*) with the Legal Affairs Committee of the Danish Parliament (*Folketingets Retsudvalg*) on 14 January 2021 that the Danish rules on retention could not be legally enforced against Danish telecommunications providers. Even so, the Minister encouraged the providers to continue to provide access to retained data. In a written answer to question No 562 of 21 January 2021 to the Committee (enclosed as **exhibit 5**), the Minister *inter alia* stated (see further the summarisation in the Eastern High Court judgement, page 51):

> DANISH:
>
> Da de gældende logningsregler pålægger teleselskaberne at registrere og opbevare oplysninger om teletrafik til brug for efterforskning af alle strafbare forhold, er det således Justitsministeriets opfattelse, at teleselskaberne, indtil nye logningsregler er på plads, ikke vil kunne straffes, hvis de ikke følger reglerne om logning i logningsbekendtgørelsen, idet der ikke i de gældende danske regler sondres mellem, til hvilke formål oplysningerne logges.
>
> Mine udtalelser på samrådet den 14. januar 2021 om, at jeg – indtil vi får vedtaget en ny logningslovgivning – håber, at teleselskaberne har forståelse for, at politiet har behov for adgang til loggede oplysninger til at efterforske grov kriminalitet og beskytte den nationale sikkerhed, skal ses i dette lys.

UNOFFICIAL TRANSLATION:

Since the current data retention rules impose on telecommunications companies the obligation to retain and store information on teletraffic for the purpose of investigating all criminal offences, **it is the view of the Ministry of Justice that telecommunications companies, until new retention rules are in place, will not be liable to punishment if they do not comply with the retention rules in the Executive Order, as the current Danish rules do not distinguish between the purposes for which the information is retained.**

My statements at the hearing on 14 January 2021, that, **until we have adopted new retention legislation, I hope that telecommunications companies understand that the police need access to retained data** to investigate serious crime and protect national security, should be seen in this light. (emphasis added)

43. By letter dated 29 January 2021 (**exhibit 6**) to the Telecommunications Industry Association in Denmark (*Teleindustrien*) the Minister of Justice proclaimed that the Executive Order on Data Retention could not be enforced, but was nevertheless still in effect. From page 1-2 and 4 it follows:

DANISH

Det fremgår af § 1 i logningsbekendtgørelsen, at "[u]dbydere af elektroniske kommunikationsnet eller -tjenester til slutbrugere skal foretage registrering og opbevaring af oplysninger om teletrafik, der genereres eller behandles i udbyderens net, således at disse oplysninger vil kunne anvendes som led i efterforskning og retsforfølgning af strafbare forhold".

Det nærmere omfang af logningsforpligtelsen efter logningsbekendtgørelsens § 1 er reguleret i bekendtgørelsens kapitel 2 (§§ 4-9).

Disse regler om teleselskabernes logningsforpligtelse er således ikke efter EU-Domstolens dom af 6. oktober 2020 sat ud af kraft eller gjort umiddelbart ugyldige.

Det er imidlertid Justitsministeriets vurdering, at logning af trafik- og lokaliseringsdata efter dommen af 6. oktober 2020 ikke vil kunne begrundes af hensyn til bekæmpelsen af almindelig kriminalitet. Da de gældende logningsregler pålægger teleselskaberne at registrere og opbevare oplysninger om teletrafik til brug for efterforskning af alle strafbare forhold, er det således Justitsministeriets opfattelse, at teleselskaberne, indtil vi har de nye logningsregler på plads, ikke vil kunne straffes, hvis de ikke følger reglerne om logning i logningsbekendtgørelsen, idet der ikke med afsæt i de danske regler vil kunne sondres mellem til, hvilke formål oplysningerne er blevet logget.

Mine udtalelser på samrådet den 14. januar 2021 om, at jeg – indtil vi får vedtaget en ny logningslovgivning – håber, at teleselskaberne har forståelse for, at politiet har behov for adgang til loggede oplysninger til at efterforske grov kriminalitet og terror, skal således ses i dette lys.

…

Opsamling

Det er således vurderingen, at den logningsforpligtelse, der følger af logningsbekendtgørelsen, fortsat er i kraft, men at teleselskaberne, indtil vi har de nye logningsregler på plads, ikke vil kunne straffes, hvis de ikke følger reglerne om logning i logningsbekendtgørelsen…

UNOFFICIAL TRANSLATION:

According to section 1 of the Executive Order, it is stated that "providers of electronic communications networks or services to end-users must register and store information about teletraffic generated or processed in the provider's network so that this information can be used as part of the investigation and prosecution of punishable offences."

The specific scope of the Executive Order pursuant to Section 1 of the retention scheme is regulated in Chapters 2 (sections 4-9) of the regulation.

Therefore, these rules concerning telecommunications companies' retention obligations have not been repealed or immediately invalidated by the judgment of the EU Court of Justice on 6 October 2020.

However, the Ministry of Justice assesses that retention of traffic and location data following the judgment of 6 October 2020, cannot be justified for the purpose of combating ordinary crime. **Since the current retention rules impose on telecommunications companies the obligation to register and store data about teletraffic for the purpose of investigating all punishable offences, the Ministry of Justice's view is that telecommunications companies, until we have the new** retention **rules in place, cannot be punished if they do not comply with the rention rules in the** retention **regulation.** This is because there will be no distinction based on Danish rules as to the purposes for which the information has been retained.

My statements at the hearing on January 14, 2021, expressing the hope that telecommunications companies understand that the police need access to retained information to investigate serious crime and terrorism until we have adopted new retention legislation, should be seen in this light.

…

Summary

The assessment is thus that the retention obligation following from the retention regulation is still in force, but that telecommunications companies, until we have the new retention **rules in place, will not be able to be penalised if they do not follow the retention rules in the retention regulation**... (emphasis added)

44. The applicant finds it challenging to comprehend how the Executive Order on Data Retention can be deemed "in force" while, simultaneously – due to the supremacy of EU law – authorities are unable to fully enforce this order. From the applicant's perspective, this apparent conflict suggests the invalidity of the legislation in question.

45. It follows that the Danish authorities were fully aware that the data retention scheme was unlawful as it stood when the applicant pursued the case before the domestic courts. The applicant submits that the admission made both to the Legal Affairs Committee and to the Telecommunications Industry goes to the heart of the applicant's claims: that Executive Order No 988 of 28 September 2006 on the Retention and Storage of Traffic Data as it stood at the time was invalid and that telecommunication companies were under no legal obligation to retain and store data in accordance with the Executive Order. Despite several amendments to the Executive Orders, this position has not changed (cf paras 25-28, above).

46. Shortly after Amendment Act No 291 of 8 March 2022 came into force, the CJEU delivered its judgement in *An Garda Síochána* (Case C-140/20, cited above). Following this judgement, the Minister yet again conceded that the (newly enacted) legislation was contrary to EU law, but assured the public that the authorities would administer the scheme in accordance with EU law. A press release dated 25 May 2022 *inter alia* stated:

> DANISH:
>
> Justitsministeriet vurderede i umiddelbar forlængelse af afsigelsen af dommen, at dommen indebærer, at politiet under efterforskning af grov kriminalitet, som f.eks. røveri eller drab, ikke længere kan få adgang til de trafikdata, som er logget generelt og udifferentieret af teleudbyderne med henblik på at beskytte den nationale sikkerhed. Denne vurdering bekræfter Justitsministeriet nu.
>
> Der er derfor behov for at ændre visse af retsplejelovens regler om logning med henblik på at bringe bestemmelserne i overensstemmelse med EU-retten. Justitsministeriet vil fremsætte lovforslag herom efter sommerferien. Indtil da skal de gældende logningsregler fortolkes og anvendes i overensstemmelse med EU-retten.
>
> UNOFFICIAL TRANSLATION:
>
> Immediately following the judgment [*G.D. v Commissioner of An Garda Síochána*], the Ministry of Justice assessed that the ruling implies that the police, in their investigation of serious crimes, such as robbery or murder, can no longer access the traffic data that has been broadly and indiscriminately logged by telecommunications providers for the purpose of national security. The Ministry of Justice has now confirmed this assessment.
>
> Therefore, there is a need to amend certain rules of the Administration of Justice Act regarding data retention to align these regulations with EU law. The Ministry of Justice will propose legislation on this matter after the summer holiday. Until then, the current data retention rules must be interpreted and applied in accordance with EU law.

47. It bears repeating, that in *An Garda Síochána* (Case C-140/20, cited above) the CJEU reiterated its established case law that the general and indiscriminate retention of communications data is contrary to EU law, even when aimed at combating serious crime (ibid, Judgement, para 129). Significantly, the CJEU refrained from discussing the matter of general and indiscriminate retention of communications allegedly for national security purposes, as such considerations fall outside its jurisdiction. However, it is submitted that the present case well illustrates how vague invocations of national security can undermine the effective protection of fundamental rights. In this regard, this Court takes on an important role. As noted by the Court, under the Convention system secret surveillance of citizens is only tolerated to the extent that it is strictly necessary for safeguarding democratic institutions (*Kennedy v the United Kingdom*, Appl No 26839/05, para 153, 18 May 2010; *Klass and Others*, cited above, paras 49-50; and *Weber and Saravia*, cited above, para 106).

II.D *Special Nature of the Case*

48. The Government acknowledges that in cases regarding secret surveillance and retention, such as in the present case, the Court has accepted a "right to challenge a law *in abstracto" (*Government's Observations, para 51). However, the Government has not elaborated on this matter, insisting that the application should be declared inadmissible due to the non-exhaustion of national remedies.

49. As stated in the applicant's original application of 22 July 2022, the Court has accepted the examination of legislation *in abstracto* provided specific conditions are fulfilled. It is submitted that these conditions are fulfilled, as explained in more detail below.

50. The Government has made no attempt to address the special nature of the case at hand (secret surveillance and data retention and storage) and how that affects the issue of admissibility.

51. The applicant refers to the submission made below regarding the merits of the complaint which, in the view of the applicant, warrants an examination of Danish legislation *in abstracto*, rather than of specific instances of such surveillance. The applicant would in this respect highlight that it is impossible for an individual or legal person to know for certain whether their data has been accessed by the authorities. For example, the Danish authorities are expressly exempt from notifying individuals (cf Section 788(5) of the Administration of Justice Act) when accessing data covered by Section 780(1)(4) regarding extended telecommunication information ("*udvidet teleoplysning"*). The applicant refers to *Ekimdzhiev and Others v Bulgaria*, cited above, paras 383-384.

II.E *Applicable Time Frame*

52. The Government states that it is "essential to distinguish between the two legal contexts of the present case, i.e., the situations *before and after* the enactment of Amendment Act No 291 of 8 March 2022", which entered into force on 30 March 2022 (Government's Observations, para 38, original emphasis). Yet, in cases such as the present one, in which the applicants complain in the abstract about a system of secret surveillance, the relevant national laws and practices are to be scrutinised as they stand when the Court examines the admissibility of the application rather than as they stood when it was lodged (*Centrum för rättvisa v Sweden* [GC], No 35252/08, para 151, 25 May 2021; *Big Brother Watch and Others* [GC]*,* cited above, para 270; and *Ekimdzhiev and Others v Bulgaria*, cited above, para 293).

53. Mirroring the scope of the Government's submission, the applicant will nonetheless address both the legal context *before and after* the entry into force of Amendment Act No 291 of 8 March 2022. The applicant submits that there has been a violation of Articles 8, 10 and 13 of the Convention before and after the amendment and would like to emphasise that the new scheme was conceived due to the civil suit that the applicant brought. Before addressing the

merit of the applicant's submissions in relation to these Articles, it is useful to make some introductory remarks on secret surveillance and the bulk retention of communications data and the implications for a functioning democracy.

III. Introductory Remarks: The Need for Enhanced Standards

54. So far, the Court has had limited opportunities to develop its case law on bulk interception. Yet, given the significant issues involved – relating not only to the protection of individuals' rights but also to the effective functioning of democracy itself – bulk interception is of monumental importance. This was among other issues noted by Judges Lemmens, Vehabović and Bošnjak in their partially dissenting opinion in *Big Brother Watch and Others (Big Brother Watch and Others* [GC]*,* cited above, Jointly Concurring Opinion, para 30).

55. The Court is already familiar with the concept of "traffic", "communications" or "meta" data. Yet, it bears repeating what and how important this data is. A common analogy compares communications data to the information on the outside of an envelope and content data to the information within the letter itself. Nevertheless, this analogy falls short of accurately depicting the complexity and invasive potential of communication data in today's world. In an age where digital integration is woven into the fabric of daily life, individuals generate a substantial volume of communications data with every routine activity. This trove of information can divulge profound insights into personal habits, offering a nearly exhaustive chronicle of a person's locations, interactions, frequency, and duration of communication.

56. As noted by the Advocate General of the CJEU in *Tele2/Watson*, the use of such data makes it possible to "create both a faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his personal identity" (*Tele2/Watson*, cited above, Opinion of AG Saugmandsgaard Øe, para 253).

57. Similarly, the UN Special Rapporteur on Freedom of Opinion and Expression has stated:

> When accessed and analysed, even seemingly innocuous transactional records about communications can collectively create a profile of an individual's private life, including medical conditions, political and religious viewpoints and/or affiliation, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications alone. By combining information about relationships, location, identity and activity, States are able to track the movement of individuals and their activities across a range of different areas, from where they travel to where they study, what they read or whom they interact with. (UNGA, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue' (2013) UN Doc A/HRC/23/40, para 42).

58. David Anderson, the former UK Reviewer of Terrorism Legislation, has cautioned that the employment of bulk surveillance powers carries significant potential for adverse human rights impacts. He noted that these powers:

> involve potential access by the state to the data of large numbers of people whom there is not the slightest reason to suspect of threatening national security or engaging in serious crime. Any abuse of those powers could thus have particularly wide-ranging effects on the innocent. Even the perception that abuse is possible, and the fear that it could go undetected, can generate a corrosive mistrust. (D Anderson, 'Report of the Bulk Powers Review' (2016) Investigatory Powers Bill: bulk powers review 1, 120).

59. In contrast with traditional targeted surveillance measures, bulk data retention enables mass interference of individuals who, as highlighted by Anderson, are not suspected of endangering national security or perpetrating serious crimes, presenting an intrusion of alarming scope.

60. The contrast between mass and targeted surveillance is best understood by way of example. Should a state wish to identify all individuals with a psychological disorder, analysing the content of all communications within the national territory would require considerable resources. In contrast, the use of communications data could instantly reveal all individuals who have contacted a psychologist during the data retention period. This example could extend to other medical fields, various service provisions, or any are where modern communication is used (cf *Tele2/Watson*, cited above, Opinion of AG Saugmandsgaard Øe, paras 257-259).

61. Similarly, if a state aims to identify individuals who attended a specific protest march or oppose a certain government policy, relying on content analysis would be resource intensive. In contrast, a brief review of retained communications data can immediately uncover everyone present at the protest site during the specified timeframe as well as those who communicated with an opposition group (by phone, message, email, or website visit), additionally providing details such as the frequency of contact.

62. In other words, communications data is not benign. It can be used to reveal highly sensitive personal information, including sensitive health conditions, psychological well-being, sexual orientation, relationship status, political affiliation and activist histories. In Denmark, the Government has obliged telecommunication network providers and telecommunication service providers to retain and store data on fixed-line and mobile telecommunications as well as on SMS, EMS and MMS messages. The data to be retained included data on calling and receiving numbers, the exact time of the start and end of telecommunications and, as far as mobile communications were concerned, the transmitter mast(s) that a mobile phone connected to at the start and end of the relevant communication and the exact geographic or physical location in the cell at the time of the communication as well as data on the use of anonymous telecom services (pre-paid calling cards) (Government's Observations, para 14).

63. This intrusive data is required to be retained for a period of one year and affects all telecom customers in Denmark. In 2023, 94 per cent of the Danish population had a mobile phone (*Danmarks Statistik*, 3 May 2023). Given the limited publicly available information on the

use of the scheme set up in pursuance of sections 786b to 786d of the Administration of Justice Act, it is difficult to assess their utility or necessity in a democratic society.

64. The deficiency of information is among others apparent in the Government's Observations, which are notably lacking in detail.

65. It is submitted that in order to ensure public trust and the legitimacy of data gathering, democracies need to place all intelligence activities on a solid legal footing and subject them to rigorous and effective oversight. On this basis, it is submitted that a more enhanced level of protection must be developed by the Court. As warned by Anderson, "even the perception that abuse is possible, and that it could go undetected, can generate corrosive mistrust." (*Report of the Bulk Powers Review*, cited above, 120).

66. Enhanced protection, among others, entails that the content and communications data should have the same protection. As noted by the Court:

> The acquisition of that data through bulk interception can therefore be just as intrusive as the bulk acquisition of the content of communications, which is why their interception, retention and search by the authorities must be analysed by reference to the same safeguards as those applicable to content (see *Centrum för rättvisa*, cited above, para 277; *Big Brother Watch and Others* [GC], para 363; and *Ekimdzhiev and Others v Bulgaria*, cited above, para 394).

67. Enhanced protection further means that any analysis of surveillance-related harm must extend beyond privacy implications; and that given the societal implications a more nuanced approach to bulk communications data must be developed. These issues will be addressed in more detail under the submitted violations of Articles 8, 10 and 13 of the Convention.

IV. The Applicant Submits That There Has Been a Violations of Article 8

68. As stated initially, the Government does not dispute that there has been an interference with the applicant's Article 8 rights, although they submit that the interference is in accordance with law and necessary in a democratic society (Government's Observations, para 88).

69. Thus, the Government submits that the data retention rules and the rules on the authorities' subsequent access are in accordance with law and pursue one or more of the legitimate aims set out in Article 8(2) of the Convention, as they are intended to protect national security and public safety and/or prevent serious crimes (Government's Observations, para 90).

70. The applicant would at the outset submit that the Data Retention and Storage scheme and subsequent access to data has not been "in accordance with law". The Court held in *Big Brother Watch and Others* that due to the "primacy of EU law", and the "Government's concession" in this respect at the domestic level that the provisions governing the retention of communications data was incompatible with EU law and therefore not in "accordance with law" (*Big Brother Watch and Others* [GC], cited above, paras 518-522). Both the Chamber

and the Grand Chamber found it "clear" that domestic law required that any regime permitting the authorities to access data retained should limit access to the purpose of combating "serious crime" and subject to prior review by a court, which was not the case (ibid). On this background the Court held that such a regime could not be said to be in "accordance with law" (ibid).

71. As stated above (para 38), the Danish Minister of Justice conceded both before the Legal Affairs Committee and to the Telecommunications Industry that the Executive Order remained in force, but due to EU law it would be unlawful to enforce it. Shortly after the Amendment Act of 8 March 2022 came into force, it became clear that the undifferentiated retention and storage scheme was still unlawful due to the judgement in *An Garda Síochána* (Case C-140/20, cited above). Reference is in this context made to the Ministry's press release dated 25 May 2022 (para 46, above) in which the Ministry acknowledges that the new scheme is still in violation of EU law. The applicant submits that the Danish scheme which suffered and still suffers similar flaws as the Investigatory Powers Act in *Big Brother Watch and Others* lacks a basis in domestic law due to the primacy of EU law and therefore, cannot be said to be "in accordance with law" within the meaning of Article 8(2) of the Convention. Furthermore, the Government has accepted that parts of the retention scheme was in violation of the EU Charter and thus, was not "prescribed by law", as required by the Convention Article 8 (and 10) (Government's Observations, para 44).

72. The applicant would at the outset like to reiterate the submission made by the applicants and numerous interest organisations in *Big Brother Watch and Others* that bulk interception is in principle neither necessary nor proportionate within the meaning of Article 8 of the Convention and, as such, does not fall within a State's margin of appreciation (*Big Brother Watch and Others* [GC]*,* cited above, para 277) .

73. This argument was to some extent accepted by the CJEU in *Tele2/Watson* (an upheld in later case law), which found that "general" and "indiscriminate" data retention is incompatible with the EU Charter of Fundamental Rights (*Tele2/Watson*, cited above, para 103).

74. The applicant would further like to highlight that in *Big Brother Watch and Others*, the Court argued that the interception regimes considered in its early case law were now more than ten years old. Stating further that:

> …in the intervening years technological developments have significantly changed the way in which people communicate. Lives are increasingly lived online, generating both a significantly larger volume of electronic communications, and communications of a significantly different nature and quality, to those likely to have been generated a decade ago. The scope of the surveillance activity considered in those cases would therefore have been much narrower. (*Big Brother Watch and Others* [GC], cited above, para 341).

75. The judgement was rendered just over two years ago, yet it feels more pertinent now than ever. With the advent of AI privacy concerns related to the bulk retention of communication

data intensified. AI can analyse vast quantities of communications data more quickly and in much more depth than humans. This means that patterns and profiles can be generated with greater precision, potentially revealing highly sensitive information about individuals' behaviours and preferences. AI can potentially infer personal attributes (such as health conditions, political affiliations, or sexual orientation) from seemingly innocuous data, leading to privacy breaches without direct access to personal content. AI can potentially link data from various sources to create comprehensive profiles of individuals, a process that can be more invasive than the analysis of communications alone (For an account of how AI methods are used for the analysis of large datasets, see eg *Artificial Intelligence and National Security*, (2018) Congressional Research Service, 1, 9).

76. From a Convention perspective, the issue is not whether bulk data retention is useful, but rather whether it is "strictly necessary in a democratic society", including whether it is "strictly necessary... for the obtaining of vital intelligence in an individual operation" (*Szabó and Vissy v Hungary*, Appl No 37138/14, para 73, 12 January 2016).

77. The general retention of communications data by communications service providers and its access by the authorities in individual cases must be accompanied, *mutatis mutandi*s, by the same safeguards as secret surveillance (*Ekimdzhiev and Others v Bulgaria*, cited above, para 293). This includes:

    1. Accessibility of the law;

    2. Protection of retained data by communications service providers;

    3. Grounds on which retained data can be accessed by the authorities;

    4. Procedure for obtaining access;

    5. Amount of time for which the authorities may store and use accessed data not subsequently used in criminal proceedings

    6. Procedures for storing, accessing, examining, using, communicating and destroying data accessed by the authorities

    7. Oversight arrangements;

    8. Notification;

    9. Remedies.

78. The applicant will address each in turn, but will in line with the Court's case law on secret surveillance also include: the grounds on which bulk interception may be authorised (cf *Big Brother Watch and Others* [GC], cited above, para 361), which will be addressed first.

79. In *Szabo and Vissy* the Court stated:

> A measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration, for the safeguarding the democratic institutions and, moreover, if it is strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation. In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. (*Szabó and Vissy v Hungary*, Appl No 37138/14, para 73, 12 January 2016)

80. Two requirements emerge from this statement. First, the use of secret surveillance, including bulk retention, must be restricted to circumstances that are strictly necessary to safeguard democratic institutions. This indicates that powers may be used only in relation to certain categories of serious crime that affect the components essential for a democratic society. Second, if such powers are appropriate as a general consideration, then the strict necessity test further requires that at an operational level power must be "vital" to an individual operation.

IV.A *Strictly Necessary to Safeguard Democratic Institutions*

81. The application submits that is is necessary to distinguish between the scheme for general and indiscriminate retention of communications data, in pursuance of section 786e of the Administration of Justice Act, and the scheme for specific persons and geographical locations in pursuance of sections 786b to 786d of the Administration of Justice Act (cf para 29, above).

82. The applicant submits that the scheme for general and indiscriminate retention of communications date, which permits the retention of communications data for a period of up to 12 months when a national security threat is cited (which been in effect since 30 March 2023), is contrary to the Convention (and EU Law, cf *Tele2/Watson*, cited above, para 103) as it is not strictly necessary to safeguard democratic institutions and provides an unfettered power to the Government.

83. The Court has emphasised that in matters affecting fundamental rights, it would be contrary to the rule of law for a discretion granted to the executive in the sphere of national security to be expressed in terms of unfettered power (*Roman Zakharov v Russia*, cited above, para 247). Yet this is exactly what the Danish law does. Similar to the Russian system under review in *Zakharov*, there is no safeguard in Danish law concerning the standard of national security, effective oversight or circumstances in which the bulk interception must be discontinued. Thus, the threat to national security may disappear (if it ever existed), but surveillance will continue. In practice, this means that interceptions in the framework of criminal proceedings (discussed immediately below) are attended by more safeguards than interceptions conducted outside such a framework.

84. It is further noteworthy that the Government makes no reference to the actual security threat. The Government merely states:

> The Ministry of Justice made its assessment based on contributions from the Director of Public Prosecutions (*Rigsadvokaten*), the Danish Security and Intelligence Service (*Politiets Efterretningstjeneste*), the Centre for Terror Analysis (*Center for Terroranalyse*), the Danish Defence Intelligence Service (*Forsvarets Efterretningstjeneste*) and the Centre for Cyber Security (*Center for Cybersikkerhed*). When making its assessment, the Ministry of Justice also took into account the contents of a number of publicly available analysis documents from the Danish Security and Intelligence Service, the Centre for Terror Analysis, the Danish Defence Intelligence Service and the Centre for Cyber Security. (Government's Observations, para 22)

85. The Government has not even referenced the "publicly available analysis documents" rendering it impossible for both the applicant and the Court to evaluate the basis for a 12 month general and indiscriminate retention of communications data. The lack of any independent oversight is equally striking (cf *Oversight Arrangements*, para 127-134, below).

IV.B *Strict Necessity Requires that Powers Must be "Vital" to an Individual Operation*

86. It is submitted that the second requirement of *Szabo and Vissy,* which is applicable to th scheme for specific persons and geographical locations, necessitates an assessment of whether there exists an alternative to bulk interception. Only in those circumstances where bulk interception is not merely advantageous but "vital" to an operation would satisfy the second requirement.

87. It is submitted that Danish law satisfies neither of the two *Szabo and Vissy* requirements.

88. As to the first requirement, the targeted data retention scheme is not limited to serious crimes or crimes that affect the components essential for a democratic society. In fact, the scheme may be applied to comparatively minor crimes. Under the law currently in force, the police can be granted access to data if an investigation concerns a criminal offence that carries a sentence of imprisonment for a term of three years or more. This access is permissible for the interception of communications as outlined in section 781(1) and (3), and section 78la as well as for discovery pursuant to sections 804 and 804a of the Administration of Justice Act (Government's Observations, para 28).

89. This low threshold includes several crimes that evidently do not threaten national security, such bigamy and child endangerment, as well as certain instances of indecent exposure, in accordance with Sections 208, 215a and 232 of the Danish Criminal Code (Law No 1851 of 20 September 2021). Additionally, when crimes such as theft, embezzlement, fraud, and usury are of a particularly grave nature, they too fall under this threshold (cf Sections 276, 278, 279 and 282 read in light of Section 286 of the Danish Criminal Code). These are but some of the many crimes that satisfy the disproportionate three year threshold.

90. It should be added that the threshold of application was deliberately lowered from six to three years by Amendment Act No 291 of 8 March 2022. As noted in the Government's Observations, a "substantial litigation risk" was assumed in the preparatory works ("*travaux*

préparatoires") of the Amendment Act (Government's Observations, para 23). In the remarks to the proposed the bill (Forslag til Lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester) of 18 November 2021 the words "litigation risk" ("procesrisiko") appears several times. The Government further states that the Ministry of Justice has previously assessed that the insertion of a criminality requirement in the law would not be compatible with Article 16 of the Council of Europe's Convention on Cybercrime (CETS No 185) (ibid).

91. As to the second requirement, that access to bulk interception data must not merely be advantageous but "vital" to an operation. The Government's Observations only states that it is "a general condition in order for the police to be granted access to retained and stored data that a certain evidentiary threshold is met." (Government's Observations, para 29). It further states that it is "a general condition that such access is of *some* importance to the investigation" (Government's Observations, para 30, emphasis added).

92. It is submitted that this notable succinct information is a reflection of the fact that Danish law did not and does not contain clear and precise rules on who can get access and under what conditions.

93. Having made this preliminary submission, the application will follow the safeguards as set out in *Ekimdzhiev and Others v Bulgaria*, cited above.

1. Accessibility of the Law

94. The applicant does not dispute that statutory provisions governing the retention and storage of communications data have been officially published and are thus accessible to the public. Yet, the applicant notes that the Minister of Justice proclaimed by letter of 29 January 2021 (exhibit 6) that the Executive Order on Data Retention could not be enforced, but was nevertheless still in effect (cf para 43, above).

2. Protection of Retained Data by Communications Service Providers

95. The applicant does not dispute that communications service providers are required to store and process retained communications data in line with the rules governing the protection of personal data, but submits that there is insufficient oversight and safeguards (cf the section on *Oversight Arrangements*, paras 127-134, below).

3. Grounds on which Retained Data can be Accessed by the Authorities

96. Defining the circumstances access to retained data may be accessed by the authorities is crucial to safeguard human rights. So far, the Court has accepted, among others, "detecting or investigating serious criminal offences" (*Ekimdzhiev and Others v Bulgaria*, cited above,

para 293). It has further accepted that three years or more imprisonment, may qualify as a "serious criminal offence" (*Big Brother Watch and Others* [GC], cited above, paras 369-371).

97. Yet as noted by Judges Lemmens, Vehabović and Bošnjak in their partially dissenting opinion in *Big Brother Watch and Others*:

> Such a definition covers a very broad scope of behaviour, which raises serious doubts regarding the proportionality of this ground. Furthermore, in a democratic society, intelligence services should not have any competence in combating crime, unless the criminal activities threaten national security. (*Big Brother Watch and Other*s [GC], cited above, Joint Partly Concurring Opinion of Judges Lemmens, Vehabović and Bošnjak, para 29)

98. In his partly Concurring and Partly Dissenting Opinion Judge Pinto De Albuquerque stated that bulk interception is "definitively not compatible with the concept of serious crime prevailing in international law, in so far as the domestic concept encompasses offences punishable by imprisonment for a term of less than four years." (*Big Brother Watch and Other*s [GC], cited above, Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque, paras 34-35).

99. This is in line with the Article 2(b) of the United Nations Convention against Transnational Organized Crime (UNTOC), which defines "serious crime" as conduct punishable by a maximum deprivation of liberty of at least four years or more. The UNTOC has been almost universally ratified.

100. Judge Pinto De Albuquerque suggested that grounds that may justify the adoption of an interception order "must correspond either to a list of specific serious offences or generally to offences punishable by four or more years' imprisonment."(*Big Brother Watch and Others* [GC], cited above, Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque, para 34).

101. The applicant submits that a list of specific serious offences is the only approach that satisfies the first requirement of *Szabo and Vissy,* to safeguard democratic institutions. The veracity of this submission is apparent from the mundane crimes that may be subject to discovery (cf paras 89, above).

102. The Government states in relation to the standard procedure, that "only the police can access data." (Government's Observations, para 114). In this regard, the applicant recalls that the Eastern High Court held in U.2019.2019Ø (referenced in paras 36-38, above) that a private party is not excluded from obtaining a discovery order for data stored pursuant to Section 786 of the Administration of Justice Act and the Executive Order on Data Retention.

103. Similarly, the Tax Control Act (Skattekontrolloven), Act No 1535 of 19 December 2017, establishes a duty for businesses and other legal entities to provide information to public agencies.

DANISH:

§ 61. Offentlige myndigheder, erhvervsdrivende og juridiske personer, som ikke er erhvervsdrivende, skal efter anmodning give told- og skatteforvaltningen oplysninger til brug for kontrol af en identificerbar fysisk eller juridisk persons skattepligt eller skatteansættelse, jf. dog stk. 3.

…

Stk. 3. Stk. 1 gælder ikke ved indhentelse af oplysninger om omsætning m.v. mellem erhvervsdrivende, jf. §§ 57 og 58, finansielle virksomheders oplysninger om kundernes økonomiske forhold, jf. § 59, og advokaters oplysninger om klientforhold, jf. § 60.

UNOFFICIAL TRANSLATION

Section 61. Public authorities, business operators, and legal persons, who are not business operators, are required, upon request, to provide information to the customs and tax administration for use in the control of an identifiable individual or legal entity's tax liability or tax assessment, see, however, subsection 3.

...

Subsection 3. Subsection 1 does not apply to the collection of information on transactions, etc., between business operators, see sections 57 and 58, financial institutions' information about customers' financial circumstances, see section 59, and lawyers' information about client relationships, see section 60.

104. Moreover, Section 299 of the Administration of Justice Act, concerning third-party disclosure requirements, allows for the collection of communications data when deemed relevant by a court. The application of this provision was confirmed in the above-mentioned case U.2019.2019Ø (referenced in para 40, above) and explicitly referred to the preparatory work to Amendment Act No 291 of 8 March 2022 (Bill no. L 93 dated 18 November 2021).

105. Section 299 does not require that the disclosed data be conclusive to the case, nor does it restrict its application solely to "serious criminal offences".

4. Procedure for Obtaining Access

106. The Government distinguishes between the "Standard procedure", "Urgent procedure" and "Access to IP-addresses" and has submitted that access to retained data is granted only when it is genuinely necessary and the procedures provide for sufficient safeguard (Government's Observations, paras 112-119).

107. As stated above, the Government has emphasised that "only the police can access data" (Government's Observations, para 114). The applicant recalls that the Eastern High Court held in U.2019.2019Ø (referenced in paras 36-38, above) that a private party in civil proceedings is not excluded from obtaining a discovery order for data, even though data is retained for criminal investigations pursuant to Section 786 of the Administration of Justice Act and the Executive Order on Data Retention. Thus, the applicant would as a starting point contest the Government's preliminary assertion.

108. According to the Court's case law safeguards must be in place to make sure that access to data is granted only when genuinely necessary and proportionate in each case.

109. Regarding the "Standard procedure", the Government has observed that both interception of communications and discovery proceedings require a court order (Government's Observations paras 33 and 114). Moreover, legal counsel is assigned in both interception proceedings and discovery proceedings to represent the person whose data are the subject matter of the request.

110. As to the requirements for obtaining access pursuant to Sections 781 and 806 of the Administration of Justice Act, the applicant observes at the outset that the authorities are under *no* legal obligation to disclose to the national court all matters relevant to the well-foundedness of an access request, including matters which may weaken the request. Also, the law does *not* require that supporting materials be enclosed with applications for access. In the view of the applicant, the absence of such a requirement risks preventing the judge who deals with the application from properly checking whether the application is indeed well-founded. Such elements have been identified by the Court as relevant safeguards (*Ekimdzhiev and Others v Bulgaria*, cited above, paras 403-404).

111. The applicant submits that the "Standard procedure" does not provide for sufficient safeguards against abuse.

112. In regards to the "Urgent procedure" provided for in sections 783(4) and 806(10) of the Administration of Justice Act, the applicant observes that the procedure is not limited or circumscribed to a set of *particular* serious offences, but applies to the same offences as the "Standard procedure". The applicant observes that the police is required to apply for a court order within 24 hours after utilising the urgent procedure, but it does not transpire that any material obtained should be destroyed. Should a court refuse to grant a subsequent order of approval, Section 783(4) merely states that the court should alert the attorney general or Ministry of Justice depending on whether the data was accessed by the police or the Danish Intelligence Service (*Politiets Efterretningstjeneste*).

113. In this regard, the applicant submits that the "Urgent procedure" does not provide for sufficient safeguards. Thus as mentioned, the "Urgent procedure" is not limited to serious crime. Moreover, a refusal by the national court to grant a subsequent order does not trigger a duty to destroy the obtained data by the authorities, contrary to the established safeguards in *Ekimdzhiev and Others v Bulgaria* (cited above, para 407).

114. In regards to the "urgent procedure" for disclosure under Section 806, the applicant observes that section 806(4) does not entail a duty for the police to seek a subsequent court order, but leaves it to the accused to make a potential request.

115. In regards to the procedure in general, the applicant would highlight that there have been several cases regarding the inadequacy of the procedures. One example is the lack of standardised procedures when filing interception requests. Thus, the lack of correct use of terminology when applying for interception of communication led to telecommunication companies disclosing vast amounts of text messages from several thousand individuals to the police. In the so-called "*Telenor* case", a telecommunications provider handed over the specific content of text messages to the police requesting "signal data" (*signaleringsdata*) (see enclosed **exhibit 8,** an article dated 28 January 2020). Reference is also made to question No 633 dated 11 February 2020 posed by a Member of the Danish Parliament requesting the Minister of Justice to account for the case (**exhibit 9**). To this date, the relevant question is still unanswered by the Minister.

116. According to a letter dated 27 March 2020 (**exhibit 10**) from Telecommunications Industry to the Police and Prosecution Service "signal data" is an incorrect and overly broad technical term (which apparently has been used by the police and granted by the Danish courts) in interception proceedings. The Telecommunications Industry generally raised the concern that the terms and definitions were unclear, which gave rise to challenges in connection with, among other things, police requests and court orders for data disclosure.

117. The examples serve to show that better safeguards and oversight is needed to be able to ensure human rights protection.

118. In the view of the applicant, such deficiencies support the applicant's assertion that the procedures are not sufficiently circumscribed.

119. Finally, while it is true that a court order is at the outset necessary for obtaining access to retained data, Danish law does not provide for an *ex post facto* review, which must be considered as a fundamental safeguard.

5. Amount of Time for Which the Authorities May Store and Use Accessed Data Not Subsequently Used in Criminal Proceedings

120. The Government refers to section 791(1) of the Administration of Justice Act, stating that accessed communication data must be destroyed if no charges are preferred or charges are dropped in the criminal case for which access was granted (Government's Observations, para 122).

121. The applicant submits that Section 791(1) neither stipulates a timeframe nor outlines a procedure for the disposal of such data (cf *Ekimdzhiev and Others v Bulgaria,* cited above, paras 329-330).

6. Procedures for Storing, Accessing, Examining, Using, Communicating and Destroying Data Accessed by the Authorities

122. So far, the Court has provided limited guidance on the standard for erasing and destroying retained data. This is despite the fact that this is a "matter of serious concern" (*Big Brother Watch and Others* [GC], cited above, Joint Partly Concurring Opinion of Judges Lemmens, Vehabović and Bošnjak, para 12).

123. As noted by Judges Lemmens, Vehabović and Bošnjak in *Big Brother Watch and Others* [GC]:

> …a lack of transparency, at the very least, can hardly meet the requirement of foreseeability, this in turn being one of the preconditions for the lawfulness of any interference with the rights protected by Article 8 of the Convention.

124. Here also, Danish law provides limited information. The proper deletion of data is an important challenge. Technically, it is not as easy as one may think to securely "delete" data. This is because "deleting" a file typically only marks the space it occupies as usable. Until the disk space is overwritten, the data is still there and can be retrieved. To ensure that the deleted data cannot be retrieved any longer, the physical records on a storage medium must be overwritten with other data several times.

125. A recent review of legislation and oversight practices from thirteen countries (which in addition to Denmark included Australia, Belgium, Canada, France, Germany, New Zealand, Norway, Sweden, Switzerland, The Netherlands, United Kingdom, United States) noted that:

> Many oversight bodies seem to agree that much more work needs to be done to independently verify that the services honor their obligations to delete data. Drafting standards for what constitutes proper deletion would be one important step in this direction (T Wetzling and K Vieth, *Upping the Ante on Bulk Surveillance* (Heinrich Böll Foundation 2018) 130).

126. The Government states that data provided by telecommunication service providers to the police are subject to the general duty of confidentiality incumbent on public servants (Government's Observations, para 128). The applicant, however, points out the absence of analogous regulations for individuals not in public service roles, despite these being the parties who actually retain and manage retained communications data. This deficiency is further exacerbated by the lack of effective oversight, as explained immediately below.

7. Oversight Arrangements

127. The Court has stated that it requires that bulk interception regimes be subject to supervision and independent review. In the Court's view, this is one of several fundamental safeguards "which will be the cornerstone of any Article 8 compliant bulk interception regime" (*Big Brother and Others* [GC], cited above, para 350).

128. In *Ekimdzhiev and Others*, Court found that oversight of the the Commission for Protection of Personal Data and a special parliamentary committee, which issued annual reports demonstrating that it regularly carries out inspections via the experts it employs, provided insufficient safeguards. Among others, the Court noted that, these bodies had no power to order remedial measures (*Ekimdzhiev and Others v Bulgaria,* cited above, paras 426-428)

129. There is no equivalent regime under the Danish retention scheme. Instead, highly sensitive data is retained and stored by private companies, with little oversight. The only oversight bodies are the Danish Business Authority and the Danish Data Protection Authority, which "may" ask service providers to provide them with data relevant to their mandate (Government's Observations, para 131).

130. The Government has provided no evidence that the Authorities have ever requested data relevant to their mandate information. Nor do these Authorities have any no power to order remedial measures.

131. The applicant further submits that they have complained to the Danish Data Protection Agency (*Datatilsynet*). The Agency refused to take action upon the applicant's request or at its own motion. It merely took note of the Ministry of Justice's assessment made in the Ministry's press release of 25 May 2022 (para 46, above) that the retention scheme due to the judgement in *Commissioner of An Garda Síochána* (Case C-140/20), cited above) should be amended (**exhibit 11**)

132. In this regard, the applicant recalls that non-judicial bodies may be considered compatible with the Convention, provided that the supervisory body is "independent of the authorities carrying out the surveillance, and is vested with sufficient powers and competence to exercise an effective and continuous control" (see *Roman Zakharov v Russia*, cited above, para 275).

133. The applicant submits that the reply from the Data Protection Agency illustrates its lack of independence.

134. On this basis, the applicant submits that the current system does not appear capable of providing effective guarantees against abusive surveillance.

8. Notification

135. As noted by the Court, the interception, retention and search by the authorities of communications data must be analysed by reference to the same safeguards as those applicable to content (*Centrum för rättvisa*, cited above, para 277; *Big Brother Watch and Others* [GC], para 363; and *Ekimdzhiev and Others v Bulgaria*, cited above, para 394). It follows that all those that have had their communications data accessed by the authorities should be notified (*Klass and Others v Germany*, Appl No 5029/71, para 58, 6 September

1978; *Weber and Saravia v Germany* (dec.), Appl No 54934/00 para 135, 26 June 2006; and, more recently, *Roman Zakharov*, cited above, para 287).

136. Section 788 applies both to requests for interception of communications (section 781) and requests for discovery (section 806(10)). In this regard, it is noted that Section 788(5) of the Administration of Justice Act explicitly states that notification is *not* given to individuals whose telecommunications data has been accessed through extended telecommunications data ("*udvidet teleoplysning*") provided for by Section 781(1)(4). Extended telecommunications data includes extremely sensitive personal information on phones within a specified area that have been or are being connected to other phones.

137. As noted by the Court, notification is an important safeguard as there is little scope for recourse to the courts by an individual unless the latter is advised of the measures taken without his or her knowledge and thus, able to challenge their legality retrospectively (*Roman Zakharov*, cited above, para 234; *Klass and Others*, cited above, para 57; and *Weber and Saravia*, cited above, para 135).

138. Considering the absence of notifications to individuals whose communication data has been accessed, the applicant submits that there are insufficient safeguards to protect against abusive surveillance practices.

9. Remedies

139. Under Danish law, there are no remedies available for the illegal retention or access of communication data. As previously mentioned, individuals are not notified when their communication data is accessed, rendering it impossible for them to contest any such actions. The prolonged legal battle faced by the applicant serves as a testament to the deficiencies of the current system.

V. The Applicant Submits That There Has Been a Violations of Article 10

140. As noted initially (para 11), the Government has not made any specific objections in regard to Article 10 and applicant assumes that the parties concur on the applicability of this Article (e.g. *Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands,* Appl No 39315/06, 22 November 2012).

141. The Court has consistently held that freedom of expression constitutes one of the essential foundations of a democratic society. Accordingly, the Court has always subjected the safeguards for respect of freedom of expression in cases under Article 10 of the Convention to special scrutiny (*Big Brother Watch and Others* [GC], cited above, para 442).

142. The applicants argue that the widespread and undiscriminating retention and storage of communication data constitutes a violation of Article 10, as such extensive interference infringes upon the right to freedom of communication by creating a "chilling effect"

143. The concept of a chilling effect is well established in the Court's case law (Pech L, 'The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU' (2021), 8-11; see also, *Donnelly v the United Kingdom,* Appl Nos 5577/72 and 5583/72, para 39, 5 April 1973; *Navalny v Russia*, Appl Nos 29580/12, 36847/12, 11252/13, 12317/13 and 43746/14, para 103, 15 November 2018, amongst others).

144. The existence of a surveillance-related "chilling effect" is a well-known phenomenon that arises when individuals or groups modify their behaviour due to a fear of the consequences that may result if that behaviour is observed (e.g. D Murray and P Fussey, *Bulk Surveillance In The Digital Age*, 2019, 43-47).

145. As the CJEU noted in *Tele2/Watson*:

> The fact that the data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance. (*Tele2/Watson*, cited above, Judgement para 100).

146. In evaluating the legitimacy of bulk surveillance, the Court must take into account the "competing interests" at play. That is the potential impact on human rights, for example, the maintenance of national security against the potential harm to human rights through interference with the right to privacy, freedom of assembly, and freedom of expression. As the Court has previously stated:

> The Court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. (*S. and Marper v the United Kingdom*, Appl Nos 30562/04 and 30566/04, para 112, 4 December 2008).

147. It is submitted that the same is true for Article 10, as well as the other rights within the Convention. People are different under surveillance than when they have privacy. Limitations of this right should be strictly justified.

148. Therefore, a proportionality assessment of the interference with Article 10 rights must take into account of not only the direct impact of surveillance on privacy rights but also the indirect, but no less significant, "chilling effect" that surveillance has on the willingness of all members of society, but especially writers, journalists, publishers, human rights defenders and others to communicate with sources, share information, and publish in the exercise of the right to freedom of expression.

149. As regards journalists, the Court has held that the safeguards to be afforded to the press are of particular importance, and the protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public about matters of public interest and the vital public-watchdog role of the press may be undermined (*Big Brother Watch and Others* [GC], cited above, para 442; see also, *Goodwin v the United Kingdom*, Appl No 17488/90, para 39, 27 March 1996; *Sanoma Uitgevers B.V. v the Netherlands*, Appl No 38224/03, para 50, 31 March 2009; and *Weber and Saravia*, cited above, para 143).

150. An interference with the protection of journalistic sources cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest (*Big Brother Watch and Others* [GC], cited above, para 444; *Sanoma Uitgevers B.V*., cited above, para 51; *Goodwin*, cited above, para 39; *Roemen and Schmit v Luxembourg*, Appl No 51772/99, para 46, 25 February 2003; and *Voskuil v the Netherlands*, Appl No 64752/01, para 65, 22 November 2007). Furthermore, any interference with the right of the protection of journalistic sources must be attended with legal procedural safeguards commensurate with the importance of the principle at stake (*Big Brother Watch and Others* [GC], cited above, para 444; *Sanoma Uitgevers B.V*., cited above, paras 88-89).

151. In *Big Brother Watch and Others*, the Court found that the UK bulk interception regime had violated the right of journalists to protect their sources as guaranteed under Article 10 of the Convention. This was despite there being special protection for journalists and newsgathering organisations.

152. The additional safeguards in respect of confidential journalistic material were set out in the Interception of Communications Code of Practice (*Big Brother Watch and Others* [GC], cited above, para 96). According to the code, any application for a warrant had to state whether the interception was likely to give rise to a collateral infringement of privacy, including where journalistic communications were involved and, where possible, it had to specify the measures to be taken to reduce the extent of the collateral intrusion.

153. The Court further placed emphasis on the existence of an *ex ante* review by a body with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing over of such material. The decision of this body should be governed by clear criteria, including whether a less intrusive measure can suffice to serve the overriding public interests established (*Big Brother Watch and Others* [GC], cited above, Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque, para 19).

154. The Government has not met the burden of proof to demonstrate that there are adequate safeguards in place for journalists or news-gathering organisations. Additionally, there is a

notable absence of any *ex ante* review by any authoritative body, either generally or specifically for journalists.

VI. The Applicant Submits That There Has Been a Violations of Article 13

155. According to the Court' case law, an assessment of whether there has been a violation of Article 13 depends on the conclusions drawn by the Court when examining the case under Article 8 (*Ekimdzhiev and Others*, cited above, para 361).

156. The applicant's arguments in regards to its Article 13 complaint rests to a large extent on the same arguments as put forward above in part II.B on alleged *Exhaustion of Domestic Remedies* and part IV.A.1 on *Notification*. Accordingly, the Article 13 complaint is closely linked to the aforementioned parts.

157. The Government has not furnished any instances demonstrating how the applicant might feasibly contest the lawfulness of the data retention scheme. Moreover, it has not supplied any statistical data on the number of individuals who have been notified of data retention or who have effectively contested the retention or use of such data. This despite such data having been retained since 5 September 2007, that is more than 16 years. The applicant posits that this lack of evidence is indicative of the lack of an effective remedy.

158. In *Rotaru v Romania* [GC], Appl No 28341/95, 4 May 2000, the applicant was confronted by information retained by the Romanian Intelligence Service. The applicant found the information to be defamatory. The Court held that a general action to protect non-pecuniary rights (e.g. tort claim) provided for by Romanian law did not suffice when dealing with the retention of personal data, since the applicant should be able to challenge the retention itself. The respondent Government failed to provide any precedent or statutory provision that would enable the applicant to challenge the retention, and the Court found a violation of Article 13 (*Rotaru v Romania* [GC], cited above, paras 70-73).

159. The applicant submits that the Government has similarly failed to substantiate that an effective remedy exists in the case at hand, and on that background there has been a violation of Article 13 of the Convention.

160. Finally, an effective remedy should be available to anyone who suspects that his or her communications have been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime. In the targeted interception context, the Court has repeatedly found the subsequent notification of surveillance measures to be a relevant factor in assessing the effectiveness of remedies before the courts and hence the existence of effective safeguards against the abuse of surveillance powers. However, it has acknowledged that notification is not necessary if the system of domestic remedies permits any person who suspects that his or her

communications are being or have been intercepted to apply to the courts or an independent body; in other words, where the courts' jurisdiction does not depend on notification.

161. The CJEU also similarly stated that persons affected must be notified "as soon as this is no longer liable to jeopardise the investigations being undertaken by those authorities" (*Tele2/Watson*, cited above, para 121) as this is necessary for these persons to be able to exercise their right to a legal remedy.

162. As mentioned above, notification is limited under Danish law, and there exists no machinery in which an individual or legal person can be afforded redress for Convention complaints, and therefore, for these reasons a breach of Article 13 has occurred.

VII. Costs and expenses:

163. The applicant claims costs and expenses for the procedure before the Court and before the domestic courts.

VII.A *Costs and Expenses Before Domestic Courts*

164. Costs of the domestic proceedings may be awarded if they are incurred by an applicant in order to try to prevent the violation found by the Court or to obtain redress therefore (see, among other authorities, *Lopata v Russia*, Appl No 72250/01, para 168, 13 July 2010).

165. In the view of the applicant, there can be no doubt that the proceedings brought at the national level were aimed at preventing a violation of the Convention.

166. Before the domestic courts, the applicant has spent 3,294,779.47 DKK in legal fees at Bird&Bird law firm to litigate the case and 74,250.50 DKK for mandatory audit - **3,369,529.47 DKK in total** (documentation enclosed as **exhibit 12**).

167. It is also recalled that at the national level the applicant was held to pay legal costs to the Minister of Justice: 125.000 DKK both in the Eastern High Court and the Supreme Court, **250,000 DKK in total**.

168. The applicant claims to be compensated to the fullest extent possible and to have the legal costs to the Minister of Justice lifted.

VII.B *Costs and Expenses Before the Court*

169. The applicant has accumulated expenses in legal fees for his counsel and co-counsel in the **total amount of 390,075 DKK**. Documentation enclosed as **exhibit 13** and **exhibit 14**.

170. It is noted that the applicant has been granted legal aid (*retshjælp*) to conduct the proceedings before the Court in the (standardised) amount of 40,000 DKK by the Department of Civil Affairs (*Civilstyrelsen)*, cf letter dated 21 September 2023 (**exhibit 15**). According to the

letter from the Department of Civil Affairs, it is a precondition for legal aid that the applicant applies for legal aid with the Court, which will be done in a separate document.

10 November 2023

Tobias Stadarfeld Jensen
Counsel

Attorney at law

Jacques Hartmann
Co-counsel

Professor in International Law and Human Rights

List of Cited Sources

Books

Wetzling T and Vieth K, *Upping the Ante on Bulk Surveillance* (Heinrich Böll Foundation 2018). Available at: <https://www.boell.de/en/2018/11/09/upping-ante-bulk-surveillance>.

Articles

Pech L, 'The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU' (2021) Open Society Foundations 2. Available at: <https://www.opensocietyfoundations.org/publications/the-concept-of-chilling-effect>

Online Reports

Anderson QC, D, 'Report of the Bulk Powers Review' (2016) Investigatory Powers Bill: Bulk Powers Review 1. Available at: <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf>

Bosanac Z, 'Electronics in the home'(*Danmarks Statistik*, 3 May 2023) available at <https://www.dst.dk/da/Statistik/emner/oekonomi/forbrug/elektronik-i-hjemmet>

Hoadley DS and Lucas NJ, 'Artificial Intelligence and National Security', (2018) Congressional Research Service 1. Available at: <https://crsreports.congress.gov/product/pdf/R/R45178/9>.

Pech L, *The Concept of Chilling Effect: Its Untapped Potential to Better Protect Democracy, the Rule of Law, and Fundamental Rights in the EU* (2021) Open Society Foundations. Available at: <https://www.opensocietyfoundations.org/publications/the-concept-of-chilling-effect>.

Preparatory work to the Amendment Act No 291 of 8 March 2022 (Forslag til Lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester). Available at: <https://www.retsinformation.dk/eli/ft/202112L00093>.