NJ 2021/361-362

Dommering, E.J.

Publication date
2021
Document Version
Final published version
Published in
Nederlandse Jurisprudentie

NJ 2021/361

EUROPEES HOF VOOR DE RECHTEN VAN DE MENS (GROTE KAMER)
25 mei 2021, nr. 58170/13, nr. 62322/14, nr. 24969/15
(R. Spano, J.F. Kjølbro, A. Nußberger, P. Lemmens, Y. Grozev, *V.A.* De Gaetano, P. Pinto de Albuquerque, F. Vehabović, I. Antoanella Motoc, C. Ranzoni, M. Mits, G. Kucsko-Stadlmayer, M. Bošnjak, T. Eicke, D. Pavli, E. Wennerström, S. Yüksel)
m.nt. E.J. Dommering onder *NJ* 2021/362

Art. 8, 10 EVRM

NJB 2018/2002
Module Privacy & AVG 2020/3621
Computerrecht 2018/252
NJB 2021/1804
RAV 2021/61
ECLI:CE:ECHR:2018:0913JUD005817013
ECLI:CE:ECHR:2021:0525JUD005817013

Recht op privacy, vrijheid van meningsuiting en journalistieke bronbescherming. Verwerking persoonsgegevens door nationale inlichtingendiensten. Bulkinterceptie van communicatie. Verkrijgen gegevens van buitenlandse inlichtingendiensten. Opvragen gegevens bij communicatie service providers.

Klagers zijn organisaties en burgers die zich inzetten voor mensenrechten en voor rechten van journalisten, allen geheimhouders. Aanleiding voor de klacht was de onthulling van Edward Snowden van het bestaan van surveillance programma's, die worden uitgevoerd door de veiligheidsdiensten van de Verenigde Staten en het Verenigd Koninkrijk. Klagers stellen dat hun elektronische communicatie of communicatiegegevens mogelijk zijn onderschept of verkregen door de veiligheidsdiensten van het Verenigd Koninkrijk en hebben een klacht ingediend bij de Investigatory Power Tribunal (IPT).

Zij klagen daarbij in het bijzonder over:
1. bulkinterceptie van communicatie,
2. het regime voor het verkrijgen van gegevens van buitenlandse inlichtingendiensten,
3. het opvragen van communicatiegegevens bij communicatie service providers en stellen dat deze regimes zowel in strijd zijn met art. 8 als art. 10 EVRM.
Grote Kamer:

Art. 8 EVRM.

Ten aanzien van de bulkinterceptie van communicatie hebben lidstaten een ruime margin of appreciation bij het beslissen welke surveillance noodzakelijk is om de nationale veiligheid te beschermen. Bij de beoordeling of een surveillance-programma de EVRM-toets kan doorstaan, moet evenwel voldaan zijn aan de volgende waarborgen, die in de het nationale recht moeten zijn vastgelegd:
1) op nationaalrechtelijk niveau moet onderzoek worden gedaan naar de noodzakelijkheid en proportionaliteit van de genomen maatregelen in elke fase van het proces,
2) bulkinterceptie moet bij aanvang, wanneer doel en reikwijdte van de operatie worden bepaald, worden onderworpen aan onafhankelijke autorisatie, en
3) de operatie moet worden onderworpen aan supervisie en een onafhankelijke ex post facto beoordeling.
In casu voldeed het programma niet aan deze criteria. Er werd weliswaar toezicht uitgeoefend door de (toenmalige) Interception of Communications Commissioner en van de Investigations Power Tribunal, maar dat is onvoldoende om de gebreken in het regime te compenseren. De inperkingen op de privélevens van burgers zijn aldus niet beperkt tot wat 'noodzakelijk is in de democratische samenleving' was. Volgt: Schending art. 8 EVRM.

Ten aanzien van het verkrijgen van gegevens van buitenlandse inlichtingendiensten geldt dat het nationale recht van het Verenigd Koninkrijk duidelijke, gedetailleerde normen bevatte over wanneer veiligheidsdiensten toestemming hadden voor het opvragen van onderschept materiaal van buitenlandse veiligheidsdiensten en over hoe, als materiaal was ontvangen, dit moest worden onderzocht, gebruikt en opgeslagen. Hiermee was dit regime aan voldoende supervisie onderworpen en was sprake van een effectief ex post facto toezicht. Volgt: geen schending art. 8 EVRM.

Ten aanzien van het verkrijgen van gegevens van communicatie service providers geldt dat de uitvoering van deze regeling niet bij wet was voorzien. Volgt: schending art. 8 EVRM.

Art. 10 EVRM.

Journalistieke bronbescherming is een van de hoekstenen van de persvrijheid. Het ondermijnen van deze bescherming heeft een schadelijk effect op de public watchdog-functie die de pers heeft.

Het nationale recht van het Verenigd Koninkrijk bevatte ten aanzien van bulkinterceptie van communicatie o.a. niet de eis dat het gebruik van selectors of zoekcriteria waarvan bekend is dat die zijn verbonden aan een bepaalde journalist, moet zijn goedgekeurd door een rechter of een ander onafhankelijk en onpartijdig orgaan. Volgt: schending art. 10 EVRM.

Ten aanzien van het regime inzake het opvragen van inlichtingen van buitenlandse regeringen of inlichtingendiensten, geldt dat er voldoende waarborgen waren om te beschermen tegen misbruik en om te verzekeren dat de Britse autoriteiten verzoeken aan buitenlandse inlichtingendiensten niet gebruikten om verplichtingen op grond van nationaal recht en het EVRM te omzeilen. Volgt: geen schending art. 8 EVRM.

Ten aanzien van het opvragen van gegevens van communicatie service providers geldt dat dit regime niet bij wet was voorzien. Volgt schending art. 10 EVRM.

Big Brother Watch e.a.
tegen
Verenigd Koninkrijk

EHRM:

The Law

266. Cumulatively, the applicants in the three joined cases complained about the Article 8 and Article 10 compatibility of three discrete regimes: the regime for the bulk interception of communications under section 8(4) of the Regulation of Investigatory Powers Act 2000 ('RIPA'); the regime for the receipt of intelligence from foreign intelligence services; and the regime for the acquisition of communications data from communications service providers ('CSPs').

267. Before considering each of these regimes in turn, the Grand Chamber will first address a preliminary issue.

I. Preliminary issue before the Grand Chamber

Enz. (*red.*)

II. The Bulk Interception of Communications

A. Territorial jurisdiction

272. In respect of the section 8(4) regime, the Government raised no objection under Article 1 of the Convention, nor did they suggest that the interception of communications was taking place outside the State's territorial jurisdiction. Moreover, during the hearing before the Grand Chamber the Government expressly confirmed that they had raised no objection on this ground as at least some of the applicants were clearly within the State's territorial jurisdiction. Therefore, for the purposes of the present case, the Court will proceed on the assumption that, in so far as the applicants complain about the section 8(4) regime, the matters complained of fell within the jurisdictional competence of the United Kingdom.

B. The alleged violation of Article 8 of the Convention

273. The applicants in all three of the joined cases complained that the regime for the bulk interception of communications was incompatible with Article 8 of the Convention, which reads:

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

1. The Chamber Judgment

274. The Chamber expressly recognised that States enjoyed a wide margin of appreciation in deciding what type of interception regime was necessary to protect national security, but considered that the discretion afforded to States in operating an interception regime would necessarily be narrower. In this regard, it observed that the Court had identified six 'minimum safeguards' which should be set out in law to avoid abuses of power: the nature of offences which may give rise to an interception order, a definition of the categories of people liable to have their communications intercepted, a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed. These safeguards, which were first set out in *Huvig v. France*, 24 April 1990, § 34, Series A no. 176 B and *Kruslin v. France*, 24 April 1990, § 35, Series A no. 176-A, had been applied routinely by the Court in its case-law on the interception of communications and in two cases specifically concerning the bulk interception of communications (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-XI (*NJ* 2017/185, m.nt. E.J. Dommering; *red.*) and *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008).

275. In the Chamber's view, the decision to operate a bulk interception regime fell within the margin of appreciation afforded to Contracting States. It assessed the operation of the United Kingdom's bulk interception regime by reference to the six minimum safeguards set out in the preceding paragraph. As the first two safeguards did not readily apply to bulk interception, the Chamber reframed these safeguards, considering first, whether the grounds upon which a warrant could be issued were sufficiently clear; secondly, whether domestic law gave citizens an adequate indication of the circumstances in which their communications might be intercepted; and thirdly, whether domestic law gave citizens an adequate indication of the circumstances in which their communications might be selected for examination. In addition, in light of recent case-law (including *Roman Zakharov v. Russia* [GC], no. 47143/06, ECHR 2015) the Chamber also had regard to the arrangements for supervising the implementation of secret surveillance measures, the existence of notification mechanisms and any remedies provided for by national law.

276. It identified the following two areas of concern in the section 8(4) regime: first, the lack of oversight of the selection of bearers for interception, the selectors used for filtering intercepted communications, and the process by which analysts selected intercepted communications for examination; and secondly, the absence of any real safeguards applicable to the searching and selection for examination of related communications data. In view of the independent oversight provided by the Interception of Communications Commissioner ('the IC Commissioner') and the IPT, and the extensive independent investigations which followed the Edward

Snowden revelations, the Chamber was satisfied that the United Kingdom was not abusing its bulk interception powers. Nevertheless, in view of the above-mentioned shortcomings, it held, by a majority, that the bulk interception regime did not meet the 'quality of law' requirement and was incapable of keeping the 'interference' to what was 'necessary in a democratic society'.

2. The parties' submissions

(a) The applicants

277. The applicants contended that bulk interception was in principle neither necessary nor proportionate within the meaning of Article 8 of the Convention and, as such, did not fall within a State's margin of appreciation. *Szabó and Vissy v. Hungary*, no. 37138/14, 12 January 2016 suggested that a secret surveillance measure had to be 'strictly necessary' for safeguarding democratic institutions and obtaining vital intelligence, and it had not been demonstrated that bulk interception satisfied this test. While it was undoubtedly a useful capability, it was clear from the Court's case-law that not everything that was useful to the intelligence services was permissible in a democratic society (see *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, ECHR 2008).

278. According to the applicants, separate interferences with the Article 8 right to respect for private life and correspondence occurred with the interception of a communication (content and/or related communications data); its storage; its automated processing; and its examination. While they agreed that a 'substantial' interference occurred when intercepted communications were examined, they believed it was wrong to suggest that no 'meaningful' interference occurred before this point. On the contrary, the Court's case-law indicated that even the storage of personal information by the State amounted to a serious interference with an individual's rights under Article 8 of the Convention (see, for example, *Rotaru v. Romania* [GC], no. 28341/95, ECHR 2000 V and *S. and Marper*, cited above). This was especially so when the data were subject to automated processing. In fact, as processing power and machine learning advanced rapidly, the storage and electronic processing of data could by itself be highly intrusive, without any underlying content or related communications data being viewed by an individual. In this regard, the applicants contended that, contrary to the 'amorphous soup' relied on by the Government (see paragraph 288 below), the collected data were more akin to a 'well organised and indexed library in which you can rapidly find anything you want'. The availability of automatic processing raised particularly severe privacy concerns and did not, as the Government contended, minimise any intrusion.

279. Should the Grand Chamber consider that the operation of a bulk interception regime was within the State's margin of appreciation, the applicants argued that the section 8(4) regime was not in accordance with the law. First of all, RIPA was unnecessarily complex, a fact acknowledged by all the independent reviewers; so much so, in fact, that the true nature and scope of the surveillance being undertaken had only become clear following the Edward Snowden revelations. Moreover the 'below the waterline' arrangements had been established by GCHQ itself; were neither accessible to nor approved by Parliament; were, as a matter of internal policy, subject to change at the executive's will; and were not binding. The applicants therefore argued that they should play no part in the Court's analysis.

280. In assessing foreseeability, the applicants argued that changes in both society and technology had resulted in a need for the Court to update its existing approach — and enhance the necessary safeguards — to ensure that Convention rights remained practical and effective. The Court's existing jurisprudence on bulk interception derived from the decision in *Weber and Saravia* (cited above), but that decision dated back to 2006, when the world was a different place. Smartphones were basic and had limited functionality; Facebook was used mainly by university students; and Twitter was in its infancy. Today people lived major parts of their lives online, using the Internet to communicate, impart ideas, conduct research, conduct relationships, seek medical advice, keep diaries, arrange travel, listen to music, find their way around and conduct financial transactions. Furthermore, modern technology generated an enormous amount of communications data, which were highly revealing even if the related content was not examined, and which were structured in such a way that computers could process them and search for patterns in them faster and more effectively than similar searches over content. For example, mobile phones constantly generated communications data as they contacted the mobile network, producing a record of the location of the phone, allowing the user's movements to be tracked, and revealing his or her Internet usage.

281. In the applicants' view, the updated and enhanced safeguards should include prior independent judicial authorisation of warrants, the choice of selectors and the selection of intercepted material for examination. In addition, where selectors or search terms referred to a specified individual, there should be objective evidence of reasonable suspicion in relation to that person. Finally, there should also be subsequent notification of any clearly defined surveillance target, where it would not cause substantial harm to the public interest.

282. The applicants identified a number of elements of the United Kingdom's bulk interception regime which they considered to be inadequate. First of all, there was an absence of independent, let alone judicial, authorisation of surveillance. While judicial authorisation might not in itself be a sufficient safeguard against abuse, this did not support the conclusion that it was not a necessary one. In addition, the applicants believed that there should also be independent, if not judicial, approval of the

selectors and search terms used by GCHQ. However, neither the bearers to be intercepted nor the strong selectors were listed in the warrant.

283. Secondly, the distinction between internal and external communications was not only poorly defined but also meaningless, with most communications likely to be swept up in the 'external' category. In the applicants' opinion, it would have been possible to have provided more meaningful protection to internal communications. For example, in Sweden all internal communications had to be destroyed immediately if they were discovered.

284. Thirdly, there were limited safeguards for the content of communications of persons known to be in the British Islands, and there were virtually no safeguards for their related communications data. GCHQ was able to retain the entirety of related communications data obtained under the bulk interception regime, subject only to limits on its storage capacity and the maximum retention period. These data — which were extremely intrusive — could be searched according to a factor referable to an individual known to be in the British Islands, without any requirement that the Secretary of State first certify that the search was necessary and proportionate.

285. Fourthly, the regime did not specify, in law and in detail, the purpose for which material could be examined and, according to the Intelligence and Security Committee of Parliament ('the ISC'), the description of material in the Secretary of State's certificate was 'generic'.

286. Finally, the applicants submitted that the IC Commissioner only provided part-time oversight and, with limited resources, had been insufficient to guarantee meaningful and robust oversight. The effectiveness of the IPT was similarly limited as it could not provide a remedy for the absence of prior judicial authorisation and, in any case, persons had to have some basis for believing that they had been subject to secret surveillance before the IPT would accept their complaint.

(b) The Government

287. The Government submitted that the information obtained under the bulk interception regime was critical to the protection of the United Kingdom from national security threats. Not only did it enable them to uncover hitherto unknown threats, but it also allowed them to conduct surveillance on known targets outside their territorial jurisdiction. The unpredictability of the route by which electronic communications were transmitted (and the fact that those communications were broken down into packets which could be transmitted via different routes) meant that in order to obtain even a small proportion of the communications of known targets overseas, it was necessary to intercept all the communications flowing over a selection of bearers. The bulk interception power had been the subject of detailed and repeated consideration by a series of independent bodies in recent years and there was a unanimity of view that there was not 'any alternative' … 'or combination of alternatives sufficient to substitute for the bulk interception power'. According to the Government, States should rightly be afforded a broad margin of appreciation in judging what systems were necessary to protect the general community from such threats, and in subjecting those systems to scrutiny the Court should take care not to undermine the effectiveness of a means of obtaining life-saving intelligence which could not be gathered in any other way.

288. The Government contended that the interception of communications under the bulk interception regime would only have resulted in a meaningful interference with a person's Article 8 rights if his or her communications were either selected for examination (that is, included on an index of communications from which an analyst could potentially choose items to inspect) or actually examined by an analyst. His or her rights could not be said to have been infringed to any more than the most minimal degree if a copy of a communication was either discarded in near-real time or held for a few days at most in a general 'amorphous soup' of data; in other words, if it was searched using selectors and queries but it was not examined or used. The overwhelming bulk of communications flowing over each intercepted cable could not be 'selected for examination', and would therefore have to be discarded.

289. With regard to the necessary safeguards, the Government agreed with the Chamber that it was appropriate to assess a bulk interception regime by reference to the same standards that had been developed by the Court in cases concerning the targeted interception of communications. The Government also largely agreed with the Chamber's assessment of the section 8(4) regime by reference to those standards. They reiterated that there was no possibility of any communications being viewed by an analyst unless and until they had been selected for examination following the automated sifting process; selection and any ensuing examination were very carefully controlled; no intelligence report could be made of any communications or communications data unless they had been viewed by an analyst; section 16(2) of RIPA required the Secretary of State to certify the necessity and proportionality of searching the content of communications according to a factor referable to an individual known to be in the British Islands; and the combined oversight functions of the ISC, the IC Commissioner and the IPT satisfied the requirements of the Convention. At all stages of the bulk interception process, the applicable safeguards were built around the Convention concepts of necessity and proportionality. Those fundamental principles governed the obtaining of the material in the first place, its examination, handling, storage, disclosure, retention and deletion.

290. In respect of those aspects of the regime which, according to the Chamber, had not provided

adequate safeguards against abuse, the Government provided further clarification. First of all, although they acknowledged that the warrant did not specify the individual bearers to be targeted, as there would be serious impracticalities and difficulties with including this information in the warrant, it nevertheless contained a description of what the interception was going to involve and a description of the sorts of bearers that would be intercepted. The IC Commissioner was briefed regularly by GCHQ about the basis on which bearers were selected for interception.

291. Secondly, they clarified that the choice of selectors was in fact carefully controlled. Whenever a new selector was added to the system, the analyst adding it had to complete a written record, explaining why it was necessary and proportionate to apply the selector for the purposes within the Secretary of State's certificate. This was done by the selection of text from a drop down menu, followed by the addition, by the analyst, of free text explaining why it was necessary and proportionate to make the search. In the case of a 'strong selector', the analyst had to explain, for example, the justification for seeking the communications of a particular target; how the selector related to the target's method of communicating; and why selection of the relevant communications would not involve an unacceptable degree of collateral intrusion into privacy. In the case of a new 'complex query', the analyst had to develop selection criteria most likely to identify communications bearing intelligence of value; and similarly had to explain why the criteria were justified, and why their use would be necessary and proportionate for the purposes within the Secretary of State's certificate. Selectors used for target development or target discovery could remain in use for a maximum of three months before a review was necessary.

292. Any selector had to be as specific as possible in order to select the minimum material necessary for the intelligence purpose, and be proportionate. If, through analysis, it was established that selectors were not being used by their intended target, prompt action had to be taken to remove them from relevant systems. The use of selectors had to be recorded in an approved location that enabled them to be audited; created a searchable record of selectors in use; and enabled oversight by the IC Commissioner. Robust independent oversight of selectors and search criteria was therefore within the IC Commissioner's powers: by the time of his 2014 report he had specifically put in place systems and processes to make sure that actually occurred, and, following the Chamber judgment, the Government had been working with the IC Commissioner's Office to ensure that there would be enhanced oversight of selectors and search criteria under IPA. However, the Government asserted that prior judicial authorisation would not have been possible for each selector without fundamentally altering their ability to discover and repel threats. GCHQ systems were necessarily tasked with many thousands of selectors which sometimes had to change rapidly in order to keep pace with fast moving investigations and threat discoveries.

293. Communications to which only the 'strong selector' process was applied were discarded immediately unless they matched the strong selector. Communications to which the 'complex query' process was also applied were retained for a few days, in order to allow the process to be carried out, and were then automatically deleted, unless they had been selected for examination. Communications which had been selected for examination could be retained only where it was necessary and proportionate to do so. The default position was that the retention period for selected communications was no longer than a few months, after which they were automatically deleted (although if the material had been cited in intelligence reporting, the report was retained). In exceptional circumstances a case could be made to retain selected communications for longer, as provided for in the Interception of Communications Code of Practice ('the IC Code').

294. The Government reiterated that any analysts who examined selected material had to be specially authorised to do so, and received mandatory regular training, including training on the requirements of necessity and proportionality. They were also vetted. Before they examined the material, they had to create a record setting out why access to the material was required, why it was consistent with the Secretary of State's certificate and the requirements of RIPA; and why it was proportionate (including considerations of any circumstances likely to give rise to a degree of collateral infringement of privacy). Unless such a record had been created, GCHQ's systems did not permit access to material.

295. As to the safeguards in respect of related communications data, the Government argued that examining the content of the most sensitive and private communications always involved a greater degree of intrusion than examining related communications data, irrespective of whether those data were aggregated to provide a detailed picture of where an individual was located, what websites he or she visited, or with whom he or she chose to communicate. On that basis, it remained appropriate for the rules governing content to be more exacting than those governing related communications data. Nevertheless, the Government accepted that the Secretary of State should be required to certify the necessity of examining related communications data under a bulk warrant pursuant to a regime analogous (though not identical) to the certification regime in place for the content of communications under section 16 of RIPA. The new Code of Practice was to be amended to this effect.

296. Until then, however, communications data were subject to the same initial filtering process as content, by which GCHQ's processing systems automatically discarded certain types of communica-

tions in near-real time. They were then subjected by automated means to simple or complex queries. However, there were two main differences between the treatment of content and the treatment of related communications data. First of all, the safeguards in section 16 — which provided that, in order to be examined, material had to fall within the Secretary of State's certificate and could not be selected according to a factor referable to an individual known for the time being to be in the British Islands and the purpose of which was to identify his or her communications — only applied to content. According to the Government, it would not be practicable to apply this safeguard to related communications data. Significantly more queries were made against communications data (as many as several thousand in one week), and in a large number of cases the identity of the person to whom the data might relate was unknown. In addition, related communications data often had a temporal quality, and having to delay conducting searches of such data pending the acquisition of an individual authority would seriously risk undermining their utility in intelligence terms. Requiring the Secretary of State to certify necessity and proportionality in each individual case, in advance of the searches being undertaken, could not possibly be done.

297. Secondly, related communications data which were not selected for examination were not immediately discarded. The principal reason for this was that communications data were to a large extent used to discover threats or targets of which GCHQ might previously have been unaware. They therefore required more analytical work, over a lengthy period, to discover 'unknown unknowns'. That discovery could very often involve an exercise of piecing together disparate small items of communications data to form a 'jigsaw' revealing a threat; and would include the possible examination of items that initially appeared to be of no intelligence interest. Discarding unselected communications data immediately, or after a few days only, would render that exercise impossible.

298. Nevertheless, the Government confirmed that before any analyst could examine any communications data at all, they had to complete a record explaining why it was necessary and proportionate to do so, in pursuit of GCHQ's statutory functions. An auditable record was therefore produced, setting out the justification for examination, and these records were available for inspection. Moreover, no intelligence reporting could be made on the basis of communications data unless and until they had been examined. Finally, related communications could be retained only where it was necessary and proportionate to do so, for a maximum period of several months, unless an exceptional case to retain for longer was made. Otherwise related communications data were automatically deleted once the maximum period had expired.

299. Finally, in light of the Chamber judgment the Government confirmed that it was taking steps to ensure that where non-content data were to be selected for examination by reference to a person believed to be in the British Islands, the selection had to be certified by the Secretary of State as necessary and proportionate on a specific thematic basis. Pending the introduction of a 'thematic' certification regime, by means of changes to the code governing the interception of communications under IPA, GCHQ had been working with the IC Commissioner's office to generate management information that could be used by the IC Commissioner to enhance *ex post facto* oversight of related communications data. In particular, GCHQ had made changes to its systems so that in any case where an analyst intended to select secondary data for examination relating to a person believed to be in the British Islands by reference to a factor relating to that person, that case would be flagged along with the supporting justification for selecting the relevant data.

3. Third party submissions

(a) The Government of France

300. The French Government submitted that in the face of threats such as international and cross-border crime, and in view of the increasing sophistication of communication technologies, the strategic bulk surveillance of communications was of vital importance to States in protecting democratic society. Moreover, it was wrong to assume that bulk interception constituted a greater intrusion into the private life of an individual than targeted interception, which by its nature was more likely to result in the acquisition and examination of a large volume of the subject's communications. In their view, there was no reason why the criteria set out by the Court in *Weber and Saravia* (cited above) could not be considered equally relevant to the effective supervision of data interception and processing under a bulk interception regime. These criteria should, however, be applied in the context of an overall assessment, weighing any shortcomings against existing guarantees and the effectiveness of the safeguards against abuse.

301. There was no justification for adding the need for 'reasonable suspicion' to these criteria. The authorities were generally not in a position to know in advance whose electronic communications it might be useful for them to monitor in the interests of law and order or national security, and such a requirement would deprive the surveillance measure of all operational interest. Moreover, in the Government's view there was no need for a judicial authority to be involved in the authorisation of such intelligence operations, or to carry out *ex post facto* control, provided that the authorising authority was independent of the executive, the supervisory body was vested with sufficient powers and competence to exercise effective and continuous control, and the two bodies were independent of one another.

302. Finally, the intervening Government submitted that metadata were by their nature less intrusive than content, as they clearly contained less

sensitive information about the behaviour and the private life of the person concerned. This view was supported by the report of the Venice Commission (see paragraphs 196–201 above) and the CJEU in *Digital Rights Ireland* (see paragraphs 209–213 above).

(b) The Government of the Kingdom of the Netherlands

303. The Government of the Kingdom of the Netherlands also submitted that bulk interception was necessary to identify hitherto unknown threats to national security. In order to protect national security, intelligence services needed the tools to investigate emerging threats in a timely and effective manner. For this they needed the powers necessary to enable them to detect and/or prevent not only terrorist activities (such as attack planning, recruitment, propaganda and funding), but also intrusive State or non-State actors' cyber activities aimed at disrupting democracy (for example, by influencing national elections or obstructing investigations by national and international organisations. An example of this was the attempted hacking of the investigation of the use of chemical weapons in Syria by the Organisation for the Prohibition of Chemical Weapons in The Hague). Moreover, the increasing dependency of vital sectors on digital infrastructures meant that such sectors, including water management, energy, telecoms, transport, logistics, harbours and airports, were increasingly vulnerable to cyber-attacks. The consequences of disruption in such sectors would have a deep impact on society, far beyond the substantial monetary damage.

304. A complicating factor in all of this was the development of new means of digital communication and the exponential increase of data that were transmitted and stored globally. In many instances the nature and origin of a particular threat was unknown and the use of targeted interception was not feasible. However, while bulk interception was not as tightly defined as targeted interception, it was never completely untargeted. Rather, it was applied for specific aims.

305. In the intervening Government's view, there was no need for additional or updated minimum safeguards; those previously identified by the Court were sufficiently robust and 'future proof'. The additional requirements proposed by the applicants before the Chamber — in particular, the requirement to demonstrate 'reasonable suspicion' — would unacceptably reduce the effectiveness of the intelligence services without providing any meaningful additional protection of individuals' fundamental rights.

306. Furthermore, according to the intervening Government, it was still relevant to distinguish between content and communications data, as the content of communications was likely to be more sensitive than communications data. The intervening Government also agreed with the Chamber that it was wrong automatically to assume that bulk interception constituted a greater intrusion into the private life of an individual than targeted interception, since with targeted interception it was likely that all, or nearly all, of the intercepted communications would be analysed. This was not true of bulk interception, where restrictions on the examination and use of data determined the intrusiveness of the interception on the individuals' fundamental rights.

307. Finally, the intervening Government submitted that any requirement to explain or substantiate selectors or search criteria in the authorisation would seriously restrict the effectiveness of bulk interception in view of the high degree of uncertainty regarding the source of a threat. *Ex post* oversight provided sufficient safeguards.

(c) The Government of the Kingdom of Norway

308. The Norwegian Government submitted that with regard to the decision of States to introduce and operate some form of bulk interception regime for national security purposes, the margin of appreciation had to be wide. This was because intelligence services had to keep pace with the rapid advances in information and communications technology. Hostile actors changed their devices and digital identities at a pace which made it difficult to track them over time. It was also difficult to discover and counteract hostile cyber operations in a timely manner without tools capable of discovering anomalies and relevant signatures. It was therefore without doubt that modern capacities like bulk interception were needed in order to find unknown threats operating in the digital domain, and to enable the services to discover and follow relevant intelligence threats.

309. In the view of the Norwegian Government, the Court's oversight should be based on an overall assessment of whether the procedural safeguards against abuse were adequate and sufficient. It should avoid absolute requirements. It should also not apply criteria that would undermine indirectly the wide margin of appreciation afforded to States in deciding to operate a bulk interception regime for national security reasons. A 'reasonable suspicion' or 'subsequent notification' requirement would have this effect.

310. Finally, the intervening Government encouraged the Court to refrain from importing concepts and criteria from the CJEU. First of all, at the relevant time nineteen Council of Europe Contracting States were not members of the European Union. Secondly, while the Convention and the Charter of Fundamental Rights had many features in common, there were also differences, most notably Article 8 of the Charter which contained a right to the protection of personal data. The CJEU also formulated 'proportionality' differently, using a 'strict necessity' method which did not compare to that used by the Court.

(d) The United Nations' Special Rapporteur on the promotion of the right to freedom of opinion and expression

311. The Special Rapporteur argued that surveillance cast a shadow over communications, such that individuals might refrain from engaging in activities protected under international human rights law. That was not to say that all surveillance operations constituted a violation of human rights law; some might be tolerable when the conditions of legality, necessity and legitimacy were met. However, all types of surveillance required a rigorous evaluation of whether they were consistent with the norms of international human rights law.

312. In the Special Rapporteur's view, the right to privacy had to be protected not only as a fundamental right independent of all others, but also in order to protect other rights, such as freedom of opinion and expression, which depended on a zone of privacy for their enjoyment. As the Special Rapporteur had indicated in his 2015 report, surveillance systems might undermine the right to form an opinion as the fear of unwilling disclosure of online activity could deter individuals from accessing information.

313. The UN High Commissioner's report counselled against distinguishing metadata from content when examining the severity of the interference with rights protected under the International Covenant on Civil and Political Rights ('ICCPR'). Her 2014 report indicated that the aggregation of metadata by way of Government surveillance might reveal more private detail about an individual than perhaps even a private communication would. The Special Rapporteur further indicated that the distinction between internal and external communications might run counter to the ICCPR. The ICCPR placed States under a duty to respect and ensure all the rights therein to all within their jurisdiction, and in its latest General Comment the Human Rights Committee interpreted this standard as including State activities that directly impacted rights outside its own territory.

314. Finally, the Special Rapporteur emphasised the importance of safeguards to protect against abuse, in particular, the need for a court, tribunal or other adjudicatory body to supervise the application of an interference measure; subsequent notification of surveillance subjects; publication of information on the scope of surveillance techniques and powers; and the right to effective remedies in case of abuse.

(e) Access Now

315. Access Now submitted that the mass surveillance at issue in the present case failed to comply with the ICCPR and the International Principles on the Application of Human Rights to Communications Surveillance since the United Kingdom had not demonstrated that such surveillance was strictly necessary or proportionate. They further contended that surveillance programmes should not be considered independently but should instead be viewed in relation to the entirety of a nation's surveillance activities as machine learning, through which mathematical algorithms could draw inferences from collections of data, had increased the invasiveness of big data sets and data mining.

(f) Article 19

316. Article 19 submitted that the indiscriminate and suspicionless collection, analysis and retention of individuals' communications was inherently disproportionate. In Article 19's opinion, only targeted surveillance based on reasonable suspicion and authorised by a judge would constitute a legitimate restriction on privacy rights.

(g) European Digital Rights ('EDRi') and other organisations active in the field of human rights in the information society

317. EDRi and others argued that the present case offered the Court a crucial opportunity to revise its framework for the protection of metadata. Governments had built their surveillance programmes based on the distinction drawn between content and metadata in *Malone v. the United Kingdom*, 2 August 1984, Series A no. 82, but at the time that case was decided neither the Internet nor mobile phones existed. Today, metadata could paint a detailed and intimate picture of a person: they allowed for mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with. Moreover, the level of detail that could be gleaned was magnified when analysed on a large scale. Indeed, Stewart Baker, general counsel of the NSA, had indicated that metadata could disclose everything about someone's life, and that if you had enough metadata, you would not need content. As a result, different degrees of protection should not be afforded to personal data based on the arbitrary and irrelevant distinction between content and metadata, but rather on the inferences that could be drawn from the data.

(h) Open Society Justice Initiative ('OSJI')

318. OSJI submitted that both the amount of data available for interception today and governments' appetite for data far exceeded what was possible in the past. Consequently, bulk interception was a particularly serious interference with privacy which could, through its 'chilling effect', potentially interfere with other rights such as freedom of expression and freedom of association. To be lawful, bulk interception should therefore satisfy several preconditions: the governing law had to be sufficiently precise; the scope of the information gathered had to be limited by time and geography; and information should only be gathered based on 'reasonable suspicion'.

(i) The Helsinki Foundation for Human Rights ('HFHR')

319. The HFHR described their experience challenging the surveillance of communications by public authorities in Poland, which culminated in the Constitutional Tribunal finding certain aspects of the relevant legislation to be unconstitutional. The legislation was subsequently amended.

(j) The International Commission of Jurists ('ICJ')

320. The ICJ submitted that in light of the scale and scope of the interference with privacy entailed in mass surveillance, the distinction between metadata and content had become out-dated. Furthermore, the fact that, in a mass surveillance operation, elements of the interference with rights might take place outside a State's territorial jurisdiction did not preclude that State's responsibility, since its control over the information was sufficient to establish jurisdiction.

(k) The Law Society of England and Wales

321. The Law Society expressed deep concern about the implications of the section 8(4) regime for the principle of legal professional privilege. In its view, the regime permitted the interception of legally privileged and confidential communications between lawyers and clients, even when both were in the United Kingdom. It also permitted the routine collection of metadata attaching to such communications. Furthermore, once intercepted these legally privileged communications could be used, provided that the primary purpose and object of the warrant was the collection of external communications. This arrangement — and the absence of adequate constraints on the use of such material — was apt to have a potentially severe chilling effect on the frankness and openness of lawyer-client communications.

4. The Court's assessment

(a) Preliminary remarks

322. The present complaint concerns the bulk interception of cross-border communications by the intelligence services. While it is not the first time the Court has considered this kind of surveillance (see *Weber and Saravia* and *Liberty and Others*, both cited above), in the course of the proceedings it has become apparent that the assessment of any such regime faces specific difficulties. In the current, increasingly digital, age the vast majority of communications take digital form and are transported across global telecommunications networks using a combination of the quickest and cheapest paths without any meaningful reference to national borders. Surveillance which is not targeted directly at individuals therefore has the capacity to have a very wide reach indeed, both inside and outside the territory of the surveilling State. Safeguards are therefore pivotal and yet elusive. Unlike the targeted interception which has been the subject of much of the Court's case-law, and which is primarily used for the investigation of crime, bulk interception is also — perhaps even predominantly — used for foreign intelligence gathering and the identification of new threats from both known and unknown actors. When operating in this realm, Contracting States have a legitimate need for secrecy which means that little if any information about the operation of the scheme will be in the public domain, and such information as is available may be couched in terminology which is obscure and which may vary significantly from one State to the next.

323. While technological capabilities have greatly increased the volume of communications traversing the global Internet, the threats being faced by Contracting States and their citizens have also proliferated. These include, but are not limited to, global terrorism, drug trafficking, human trafficking and the sexual exploitation of children. Many of these threats come from international networks of hostile actors with access to increasingly sophisticated technology enabling them to communicate undetected. Access to such technology also permits hostile State and non-State actors to disrupt digital infrastructure and even the proper functioning of democratic processes through the use of cyberattacks, a serious threat to national security which by definition exists only in the digital domain and as such can only be detected and investigated there. Consequently, the Court is required to carry out its assessment of Contracting States' bulk interception regimes, a valuable technological capacity to identify new threats in the digital domain, for Convention compliance by reference to the existence of safeguards against arbitrariness and abuse, on the basis of limited information about the manner in which those regimes operate.

(b) The existence of an interference

324. The Government do not dispute that there has been an interference with the applicants' Article 8 rights, although they submitted that for the purposes of Article 8 of the Convention the only meaningful interference could have occurred when communications were selected for examination.

325. The Court views bulk interception as a gradual process in which the degree of interference with individuals' Article 8 rights increases as the process progresses. Bulk interception regimes may not all follow exactly the same model, and the different stages of the process will not necessarily be discrete or followed in strict chronological order. Nevertheless, subject to the aforementioned caveats, the Court considers that the stages of the bulk interception process which fall to be considered can be described as follows:

(a) the interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications);

(b) the application of specific selectors to the retained communications/related communications data;
(c) the examination of selected communications/related communications data by analysts; and
(d) the subsequent retention of data and use of the 'final product', including the sharing of data with third parties.

326. At what the Court has taken to be the first stage, electronic communications (or 'packets' of electronic communications) will be intercepted in bulk by the intelligence services. These communications will belong to a large number of individuals, many of whom will be of no interest whatsoever to the intelligence services. Some communications of a type unlikely to be of intelligence interest may be filtered out at this stage.

327. The initial searching, which is mostly automated, takes place at what the Court has taken to be the second stage, when different types of selectors, including 'strong selectors' (such as an email address) and/or complex queries are applied to the retained packets of communications and related communications data. This may be the stage where the process begins to target individuals through the use of strong selectors.

328. At what the Court has taken to be the third stage, intercept material is examined for the first time by an analyst.

329. What the Court has taken to be the final stage is when the intercept material is actually used by the intelligence services. This may involve the creation of an intelligence report, the disseminating of the material to other intelligence services within the intercepting State, or even the transmission of material to foreign intelligence services.

330. The Court considers that Article 8 applies at each of the above stages. While the initial interception followed by the immediate discarding of parts of the communications does not constitute a particularly significant interference, the degree of interference with individuals' Article 8 rights will increase as the bulk interception process progresses. In this regard, the Court has clearly stated that even the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116), and that the need for safeguards will be all the greater where the protection of personal data undergoing automatic processing is concerned (see *S. and Marper*, cited above, § 103). The fact that the stored material is in coded form, intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons, can have no bearing on that finding (see *Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II and *S. and Marper*, cited above, §§ 67 and 75). Finally, at the end of the process, where information about a particular person will be analysed or the content of the communications is being examined by an analyst, the need for safeguards will be at its highest. This approach of the Court is in line with the finding of the Venice Commission, which in its report on the Democratic Oversight of Signals Intelligence Agencies considered that in bulk interception the main interference with privacy occurred when stored personal data were processed and/or accessed by the agencies (see paragraph 196 above).

331. Thus, the degree of interference with privacy rights will increase as the process moves through the different stages. In examining whether this increasing interference was justified, the Court will carry out its assessment of the section 8 (4) regime on the basis of this understanding of the nature of the interference.

(c) Whether the interference was justified
(i) General principles relating to secret measures of surveillance, including the interception of communications

332. Any interference with an individual's Article 8 rights can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which that paragraph refers and is necessary in a democratic society in order to achieve any such aim (see *Roman Zakharov*, cited above, § 227; see also *Kennedy v. the United Kingdom*, no. 26839/05, § 130, 18 May 2010). The wording 'in accordance with the law' requires the impugned measure to have some basis in domestic law (as opposed to a practice which does not have a specific legal basis — see *Heglas v. the Czech Republic*, no. 5935/02, § 74, 1 March 2007). It must also be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must therefore be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov*, cited above, § 228; see also, among many other authorities, *Rotaru*, cited above, § 52; *S. and Marper*, cited above, § 95, and *Kennedy*, cited above, § 151).

333. The meaning of 'foreseeability' in the context of secret surveillance is not the same as in many other fields. In the special context of secret measures of surveillance, such as the interception of communications, 'foreseeability' cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Roman Zakharov*, cited above, § 229; see also *Malone*, cited above, § 67; *Leander*, cited above, § 51; *Huvig*, cited above, § 29; *Kruslin*, cited above, § 30; *Valenzuela*

Contreras v. Spain, 30 July 1998, § 46, *Reports of Judgments and Decisions* 1998-V; *Rotaru*, cited above, § 55; *Weber and Saravia*, cited above, § 93; and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 75, 28 June 2007). Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see *Roman Zakharov*, cited above, § 230; see also, among other authorities, *Malone*, cited above, § 68; *Leander*, cited above, § 51; *Huvig*, cited above, § 29; *Kruslin*, cited above, § 30; and *Weber and Saravia*, cited above, § 94).

334. In cases where the legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the 'necessity' test has been complied with and it is therefore appropriate for the Court to address jointly the 'in accordance with the law' and 'necessity' requirements. The 'quality of law' in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when 'necessary in a democratic society', in particular by providing for adequate and effective safeguards and guarantees against abuse (see *Roman Zakharov*, cited above, § 236; see also *Kennedy*, cited above, § 155).

335. In this regard it should be reiterated that in its case-law on the interception of communications in criminal investigations, the Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power:

(i) the nature of offences which may give rise to an interception order;

(ii) a definition of the categories of people liable to have their communications intercepted;

(iii) a limit on the duration of interception;

(iv) the procedure to be followed for examining, using and storing the data obtained;

(v) the precautions to be taken when communicating the data to other parties; and

(vi) the circumstances in which intercepted data may or must be erased or destroyed (see *Huvig*, cited above, § 34; *Kruslin*, cited above, § 35; *Valenzuela Contreras*, cited above, § 46; *Weber and Saravia*, cited above, § 95; and *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 76).

In *Roman Zakharov* (cited above, § 231) the Court confirmed that the same six minimum safeguards also applied in cases where the interception was for reasons of national security; however, in determining whether the impugned legislation was in breach of Article 8, it also had regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (see *Roman Zakharov*, cited above, § 238).

336. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, the Court has held that it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure (see *Roman Zakharov*, cited above, § 233; see also *Klass and Others v. Germany*, 6 September 1978, §§ 55 and 56, Series A no. 28).

337. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is a relevant factor in assessing the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of surveillance powers. There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively (see *Roman Zakharov*, cited above, § 234; see also *Klass and Others*, cited above, § 57, and *Weber and Saravia*, cited above, § 135) or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts, whose jurisdiction does not depend on notification to the surveillance subject of the measures taken (see *Roman Zakharov*, cited above, § 234; see also *Kennedy*, cited above, § 167).

338. As to the question whether an interference was 'necessary in a democratic society' in pursuit of a legitimate aim, the Court has recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see *Weber and Saravia*, cited above, § 106).

339. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for order-

ing them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the 'interference' to what is 'necessary in a democratic society' (see *Roman Zakharov*, cited above, § 232; see also *Klass and Others*, cited above, §§ 49, 50 and 59, *Weber and Saravia*, cited above, § 106 and *Kennedy*, cited above, §§ 153 and 154).

(ii) Whether there is a need to develop the case-Law

340. In *Weber and Saravia* and *Liberty and Others* (cited above) the Court accepted that bulk interception regimes did not *per se* fall outside the States' margin of appreciation. In view of the proliferation of threats that States currently face from networks of international actors, using the Internet both for communication and as a tool, and the existence of sophisticated technology which would enable these actors to avoid detection (see paragraph 323 above), the Court considers that the decision to operate a bulk interception regime in order to identify threats to national security or against essential national interests is one which continues to fall within this margin.

341. In both *Weber and Saravia* and *Liberty and Others* (cited above) the Court applied the above-mentioned six minimum safeguards developed in its case-law on targeted interception (see paragraph 335 above). However, while the bulk interception regimes considered in those cases were on their face similar to that in issue in the present case, both cases are now more than ten years old, and 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 (see paragraph 322 above). The scope of the surveillance activity considered in those cases would therefore have been much narrower.

342. This is equally so with related communications data. As the ISR observed in its report, greater volumes of communications data are currently available on an individual relative to content, since every piece of content is surrounded by multiple pieces of communications data (see paragraph 159 above). While the content might be encrypted and, in any event, may not reveal anything of note about the sender or recipient, the related communications data could reveal a great deal of personal information, such as the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. Furthermore, any intrusion occasioned by the acquisition of related communications data will be magnified when they are obtained in bulk, since they are now capable of being analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with (see paragraph 317 above).

343. More importantly, however, in *Weber and Saravia* and *Liberty and Others* the Court did not expressly address the fact that it was dealing with surveillance of a different nature and scale from that considered in previous cases. Nonetheless, targeted interception and bulk interception are different in a number of important respects.

344. To begin with, bulk interception is generally directed at international communications (that is, communications physically travelling across State borders), and while the interception and even examination of communications of persons within the surveilling State might not be excluded, in many cases the stated purpose of bulk interception is to monitor the communications of persons outside the State's territorial jurisdiction, which could not be monitored by other forms of surveillance. For example, the German system aims only to monitor foreign telecommunications outside of German territory (see paragraph 248 above). In Sweden, the intercept material cannot relate to signals where both the sender and recipient are in Sweden (see today's judgment in the case of *Centrum för rättvisa v. Sweden* (application no. 35252/08)).

345. Moreover, as already noted, the purposes for which bulk interception may be employed would appear to be different. In so far as the Court has considered targeted interception, it has, for the most part, been employed by respondent States for the purposes of investigating crime. However, while bulk interception may be used to investigate certain serious crimes, Council of Europe member States operating a bulk interception regime appear to use it for the purposes of foreign intelligence gathering, the early detection and investigation of cyberattacks, counter-espionage and counter-terrorism (see paragraphs 303, 308 and 323 above).

346. While bulk interception is not necessarily used to target specified individuals, it evidently can be — and is — used for this purpose. However, when this is the case, the targeted individuals' devices are not monitored. Rather, individuals are 'targeted' by the application of strong selectors (such as their email addresses) to the communications intercepted in bulk by the intelligence services. Only those 'packets' of the targeted individuals' communications which were travelling across the bearers selected by the intelligence services will have been intercepted in this way, and only those intercepted communications which matched either a strong selector or complex query could be examined by an analyst.

347. As with any interception regime, there is of course considerable potential for bulk interception to be abused in a manner adversely affecting the right of individuals to respect for private life. While

Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, and States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary, for these purposes, in operating such a system the margin of appreciation afforded to them must be narrower and a number of safeguards will have to be present. The Court has already identified those safeguards which should feature in a Convention-compliant targeted interception regime. While those principles provide a useful framework for this exercise, they will have to be adapted to reflect the specific features of a bulk interception regime and, in particular, the increasing degrees of intrusion into the Article 8 rights of individuals as the operation moves through the stages identified in paragraph 325 above.

(iii) The approach to be followed in bulk interception cases

348. It is clear that the first two of the six 'minimum safeguards' which the Court, in the context of targeted interception, has found should be defined clearly in domestic law in order to avoid abuses of power (that is, the nature of offences which may give rise to an interception order and the categories of people liable to have their communications intercepted: see paragraph 335 above), are not readily applicable to a bulk interception regime. Similarly, the requirement of 'reasonable suspicion', which can be found in the Court's case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence. Nevertheless, the Court considers it imperative that when a State is operating such a regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted. The remaining four minimum safeguards defined by the Court in its previous judgments — that is, that domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed — are equally relevant to bulk interception.

349. In its case-law on targeted interception, the Court has had regard to the arrangements for supervising and reviewing the interception regime (see *Roman Zakharov*, cited above, §§ 233–234). In the context of bulk interception the importance of supervision and review will be amplified, because of the inherent risk of abuse and because the legitimate need for secrecy will inevitably mean that, for reasons of national security, States will often not be at liberty to disclose information concerning the operation of the impugned regime.

350. Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to 'end-to-end safeguards', meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and that the operation should be subject to supervision and independent *ex post facto* review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8 compliant bulk interception regime (see also the report of the Venice Commission, at paragraph 197 above, which similarly found that two of the most significant safeguards in a bulk interception regime were the authorisation and oversight of the process).

351. Turning first to authorisation, the Grand Chamber agrees with the Chamber that while judicial authorisation is an 'important safeguard against arbitrariness' it is not a 'necessary requirement' (see paragraphs 318–320 of the Chamber judgment). Nevertheless, bulk interception should be authorised by an independent body; that is, a body which is independent of the executive.

352. Furthermore, in order to provide an effective safeguard against abuse, the independent authorising body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted. This would enable the independent authorising body to assess the necessity and proportionality of the bulk interception operation and also to assess whether the selection of bearers is necessary and proportionate to the purposes for which the interception is being conducted.

353. The use of selectors — and strong selectors in particular — is one of the most important steps in the bulk interception process, as this is the point at which the communications of a particular individual may be targeted by the intelligence services. However, while some systems allow for the prior authorisation of categories of selectors (see, for example, the Swedish system described in detail in the judgment in *Centrum för rättvisa v. Sweden* (application no. 35252/08)), the Court notes that the Governments of both the United Kingdom and the Netherlands have submitted that any requirement to explain or substantiate selectors or search criteria in the authorisation would seriously restrict the effectiveness of bulk interception (see paragraphs 292 and 307 above). This was accepted by the IPT, which found that the inclusion of the selectors in the authorisation would 'unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic' (see paragraph 49 above).

354. Taking into account the characteristics of bulk interception (see paragraphs 344–345 above), the large number of selectors employed and the inherent need for flexibility in the choice of selectors, which in practice may be expressed as technical combinations of numbers or letters, the Court would accept that the inclusion of all selectors in the authorisation may not be feasible in practice. Nevertheless, given that the choice of selectors and query terms determines which communications will be eligible for examination by an analyst, the authorisation should at the very least identify the types or categories of selectors to be used.

355. Moreover, enhanced safeguards should be in place when strong selectors linked to identifiable individuals are employed by the intelligence services. The use of every such selector must be justified — with regard to the principles of necessity and proportionality — by the intelligence services and that justification should be scrupulously recorded and be subject to a process of prior internal authorisation providing for separate and objective verification of whether the justification conforms to the aforementioned principles.

356. Each stage of the bulk interception process — including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material — should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the 'interference' to what is 'necessary in a democratic society' (see *Roman Zakharov*, cited above, § 232; see also *Klass and Other*, cited above, §§ 49, 50 and 59; *Weber and Saravia*, cited above, § 106 and *Kennedy*, cited above, §§ 153 and 154). In particular, the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. In order to facilitate this supervision, detailed records should be kept by the intelligence services at each stage of the process.

357. 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; in other words, where the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his or her communications (see *Roman Zakharov*, cited above, § 234 and *Kennedy*, cited above, § 167).

358. The Court considers that a remedy which does not depend on notification to the interception subject could also be an effective remedy in the context of bulk interception; in fact, depending on the circumstances it may even offer better guarantees of a proper procedure than a system based on notification. Regardless of whether material was acquired through targeted or bulk interception, the existence of a national security exception could deprive a notification requirement of any real practical effect. The likelihood of a notification requirement having little or no practical effect will be more acute in the bulk interception context, since such surveillance may be used for the purposes of foreign intelligence gathering and will, for the most part, target the communications of persons outside the State's territorial jurisdiction. Therefore, even if the identity of a target is known, the authorities may not be aware of his or her location.

359. The powers and procedural guarantees an authority possesses are relevant in determining whether a remedy is effective. Therefore, in the absence of a notification requirement it is imperative that the remedy should be before a body which, while not necessarily judicial, is independent of the executive and ensures the fairness of the proceedings, offering, in so far as possible, an adversarial process. The decisions of such authority shall be reasoned and legally binding with regard, *inter alia*, to the cessation of unlawful interception and the destruction of unlawfully obtained and/or stored intercept material (see, *mutatis mutandis, Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 120, ECHR 2006-VII and also *Leander*, cited above, §§ 81–83 where the lack of power to render a legally binding decision constituted a main weakness in the control offered).

360. In the light of the above, the Court will determine whether a bulk interception regime is Convention compliant by conducting a global assessment of the operation of the regime. Such assessment will focus primarily on whether the domestic legal framework contains sufficient guarantees against abuse, and whether the process is subject to 'end-to-end safeguards' (see paragraph 350 above). In doing so, it will have regard to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 92).

361. In assessing whether the respondent State acted within its margin of appreciation (see paragraph 347 above), the Court would need to take account of a wider range of criteria than the six *Weber* safeguards. More specifically, in addressing jointly 'in accordance with the law' and 'necessity' as is the established approach in this area (see *Roman Zakharov*, cited above, § 236 and *Kennedy*, cited

above, § 155), the Court will examine whether the domestic legal framework clearly defined:
1. the grounds on which bulk interception may be authorised;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure to be followed for granting authorisation;
4. the procedures to be followed for selecting, examining and using intercept material;
5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

362. Despite being one of the six *Weber* criteria, to date the Court has not yet provided specific guidance regarding the precautions to be taken when communicating intercept material to other parties. However, it is now clear that some States are regularly sharing material with their intelligence partners and even, in some instances, allowing those intelligence partners direct access to their own systems. Consequently, the Court considers that the transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself. First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law. Secondly, the transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. This does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer. Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality — such as confidential journalistic material — is being transferred. Finally, the Court considers that the transfer of material to foreign intelligence partners should also be subject to independent control.

363. For the reasons identified at paragraph 342 above, the Court is not persuaded that the acquisition of related communications data through bulk interception is necessarily less intrusive than the acquisition of content. It therefore considers that the interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content.

364. That being said, while the interception of related communications data will normally be authorised at the same time the interception of content is authorised, once obtained they may be treated differently by the intelligence services (see, for example, paragraphs 153–154 above). In view of the different character of related communications data and the different ways in which they are used by the intelligence services, as long as the aforementioned safeguards are in place, the Court is of the opinion that the legal provisions governing their treatment may not necessarily have to be identical in every respect to those governing the treatment of content.

(iv) The Court's assessment of the case at hand

(α) Preliminary remarks

365. At the relevant time bulk interception had a legal basis in Chapter I of RIPA. Moreover, the Court is satisfied that the said regime pursued the legitimate aims of protecting national security, preventing disorder and crime and protecting the rights and freedoms of others. Therefore, following the approach outlined in paragraph 334 above, it remains to be considered whether the domestic law was accessible and contained adequate and effective safeguards and guarantees to meet the requirements of 'foreseeability' and 'necessity in a democratic society'.

366. The relevant legislative provisions governing the operation of the bulk interception regime were undoubtedly complex; indeed, most of the reports into the United Kingdom's secret surveillance regimes criticised their lack of clarity (see paragraphs 143, 152 and 157 above). However, those provisions were elucidated in the accompanying Interception of Communications Code of Practice ('the IC Code' — see paragraph 96 above). Paragraph 6.4 of the IC Code made it clear that bulk interception was taking place and provided further details of how this particular surveillance regime operated in practice (see paragraph 96 above). The IC Code is a public document approved by both Houses of Parliament, which is published by the Government online and in print version, and which has to be taken into account both by persons exercising interception duties and the courts (see paragraphs 93–94 above). As a consequence, this Court has accepted that its provisions could be taken into account in assessing the foreseeability of RIPA (see *Kennedy*, cited above, § 157). Accordingly, the Court would accept that domestic law was adequately 'accessible'.

367. Turning next to the question whether the law contained adequate and effective safeguards and guarantees to meet the requirements of 'foreseeability' and 'necessity in a democratic society', the Court will address in subsection (β;) each of the

eight requirements set out in paragraph 361 above with respect to the interception of the contents of electronic communications. In sub-section (γ) it will examine more specifically the interception of related communications data.

(β) Interception of the contents of communications

— 1. The grounds on which bulk interception may be authorised

368. Under section 5(3) of RIPA and paragraph 6.11 of the IC Code (see paragraphs 62 and 96 above), the Secretary of State could only issue a bulk interception warrant if he or she was satisfied that it was necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom so far as those interests were also relevant to the interests of national security.

369. These grounds were subject to the following limitations. First of all, the IC Commissioner had clarified that in practice 'national security' allowed surveillance of activities which threatened the safety or well-being of the State and activities which were intended to undermine or overthrow parliamentary democracy by political, industrial or violent means (see *Kennedy*, cited above, § 333). Secondly, serious crime was defined in section 81(2)(b) of RIPA as a crime for which the perpetrator (assuming he or she was over the age of twenty-one and had no previous convictions) could reasonably be expected to be sentenced to imprisonment for a term of three years or more; or where the conduct involved the use of violence, resulted in substantial financial gain or was conducted by a large number of persons in pursuit of a common purpose (see paragraph 63 above). Thirdly, section 17 of RIPA and paragraph 8.3 of the IC Code provided that as a general rule neither the possibility of interception, nor intercepted material itself, could play any part in legal proceedings (see paragraphs 83 and 96 above). Therefore, while interception could be used for the purposes of preventing or detecting serious crime, intercept material could not be used in the prosecution of a criminal offence. In addition, paragraph 6.8 of the IC Code provided that the purpose of a section 8(4) warrant would 'typically reflect one or more of the intelligence priorities set by the National Security Council' (see paragraphs 96 and 98 above).

370. In principle, the wider the grounds are, the greater the potential for abuse. However, narrower and/or more tightly defined grounds would only provide an effective guarantee against abuse if there were sufficient other safeguards in place to ensure that bulk interception was only authorised for a permitted ground and that it was necessary and proportionate for that purpose. The closely related issue of whether there existed sufficient guarantees to ensure that the interception was necessary or justified is therefore as important as the degree of precision with which the grounds on which authorisation may be given are defined. Consequently, in the Court's view, a regime which permits bulk interception to be ordered on relatively wide grounds may still comply with Article 8 of the Convention, provided that, when viewed as a whole, sufficient guarantees against abuse are built into the system to compensate for this weakness.

371. In the United Kingdom, while the grounds on which bulk interception could be authorised were formulated in relatively broad terms, they still focused on national security as well as serious crime and the economic well-being of the country so far as those interests were also relevant to the interests of national security (see paragraph 368 above). The Court will therefore turn to consider the other safeguards built in to the section 8(4) regime in order to determine whether, when viewed as a whole, it was compliant with Article 8 of the Convention.

— 2. The circumstances in which an individual's communications may be intercepted

372. Paragraph 6.2 of the IC Code (see paragraph 96 above) clearly stated that '[i]n contrast to section 8(1), a section 8(4) warrant does not name or describe the interception subject or set of premises in relation to which the interception is to take place. Neither does section 8(4) impose an express limit on the number of external communications which may be intercepted'. In other words, the communications bearers were targeted rather than the devices from which the communications were sent, or the senders or recipients of the communications. In the absence of any limit on the number of communications which could have been intercepted, it would appear that all packets of communications flowing across the targeted bearers while the warrant was in force were intercepted.

373. That being said, a section 8(4) warrant was a warrant for the interception of external communications (see paragraph 72 above) and paragraph 6.7 of the IC Code (see paragraph 96 above) required the intercepting agency conducting interception under a section 8(4) warrant to use its knowledge of the way in which international communications were routed, combined with regular surveys of relevant communications links, to identify those individual communications bearers that were most likely to contain external communications that met the description of material certified by the Secretary of State. The intercepting agency was also required to conduct the interception in ways that limited the collection of non-external communications to the minimal level compatible with the objective of intercepting wanted external communications. The bearers were not, therefore, chosen at random. On the contrary, they were selected because they were believed to be the most likely to carry external communications of intelligence interest.

374. Paragraph 6.5 of the IC Code defined 'external communications' as communications which were either sent or received outside the British Is-

lands (see paragraph 96 above). Where both the sender and recipient were within the British Islands, the communication was internal. Whether or not a communication was 'external' therefore depended on the geographic location of the sender and recipient and not on the route the communication took to its destination. Communications which crossed the United Kingdom's borders (international communications) could still be 'internal', since a communication (or packets of a communication) both sent from and received in the United Kingdom could nevertheless be routed through one or more third countries.

375. The distinction between internal and external communications did not, therefore, prevent the interception of internal communications travelling across the United Kingdom's borders, and in fact the 'by-catch' of such communications was expressly permitted by section 5(6) of RIPA, which provided that the conduct authorised by an interception warrant included the interception of communications not identified by the warrant if necessary to do what was expressly authorised by the warrant (see paragraph 68 above). In addition, the definition of 'external' was itself sufficiently broad to include cloud storage and the browsing and social media activities of a person in the United Kingdom (see paragraphs 75 and 76 above). Nevertheless, as the Chamber acknowledged, the 'external communications' safeguard had a role to play at the macro level of selecting the bearers for interception (see paragraph 337 of the Chamber judgment); as the intercepting agency had to use its knowledge of the way in which international communications were routed to identify those communications bearers most likely to contain external communications of value to the operation, the safeguard did, albeit to a limited extent, circumscribe the categories of people liable to have their communications intercepted. It was also relevant to the question of proportionality, since States might have less intrusive measures available to them to obtain the communications of persons within their territorial jurisdiction.

376. In light of the foregoing, the Court considers it clear that under the section 8(4) regime international communications (that is, communications crossing State borders) could be intercepted; and that the intelligence services would only use the power to intercept those bearers most likely to be carrying external communications of intelligence interest. In the bulk interception context it is difficult, in the abstract, to imagine how the circumstances in which an individual's communications might be intercepted could be further delimited. In any event, as neither the sender nor the recipient of an electronic communication could control the route it took to its destination, in practice any further restrictions on the choice of bearers would not have made domestic law any more foreseeable as to its effects. The Court would therefore accept that the circumstances in which an individual's communications could be intercepted under the section 8(4) regime were sufficiently 'foreseeable' for the purposes of Article 8 of the Convention.

— 3. The procedure to be followed for granting authorisation

377. An application for a section 8(4) warrant was made to the Secretary of State, who alone had the power to issue such a warrant. Prior to submission, each application was subject to a review within the agency making it. This involved scrutiny by more than one official, who had to consider whether the application was made for a purpose falling within section 5(3) of RIPA and whether the proposed interception satisfied the Convention standards of necessity and proportionality (see paragraph 6.9 of the IC Code, at paragraph 96 above). This additional level of internal scrutiny was no doubt valuable, but it remained the case that at the relevant time bulk interception conducted under the section 8(4) regime was authorised by the Secretary of State and not by a body independent of the executive. Consequently, the section 8(4) regime lacked one of the fundamental safeguards; namely, that bulk interception should be subject to independent authorisation at the outset (see paragraph 350 above).

378. As for the level of scrutiny provided by the Secretary of State, paragraph 6.10 of the IC Code set out in detail the information which had to be included in the application (see paragraph 96 above). This included a description of the communications to be intercepted, details of the communications service provider(s) and an assessment of the feasibility of the operation, where relevant; a description of the conduct to be authorised; the certificate that would regulate examination of intercept material (see paragraphs 378 and 379 below); an explanation of why the interception was considered necessary for one or more of the section 5(3) purposes; a consideration of why the conduct was proportionate to what was sought to be achieved; an assurance that intercept material would be read, looked at or listened to only so far as it was certified and met the conditions of sections 16(2) to 16(6) of RIPA; and an assurance that intercept material would be handled in accordance with the section 15 and section 16 safeguards.

379. The Secretary of State was therefore informed of the purpose of the operation (which had to be one of the section 5(3) purposes) and, before issuing a warrant, had to be satisfied that it was necessary for that purpose, and that it was proportionate to what it sought to achieve (see paragraphs 6.11 and 6.13 of the IC Code at paragraph 96 above). In assessing proportionality the Secretary of State had to consider whether the warrant was excessive in the overall circumstances of the case and whether the information sought could reasonably have been obtained by less intrusive means (see paragraph 3.6 of the IC Code at paragraph 96 above). In particular, the size and scope of the interference had to be balanced against what was sought to be

achieved; an explanation had to be given of how and why the methods would cause the least possible intrusion on the subject and others; consideration had to be given as to whether the activity was an appropriate way of achieving the necessary result, having considered all reasonable alternatives; and, as far as reasonably practicable, evidence had to be given of other methods considered but assessed as insufficient to fulfil operational objectives (see paragraph 3.7 of the IC Code at paragraph 96 above).

380. Although the application for a section 8(4) warrant had to include 'a description of the communications to be intercepted' and 'details of the Communications Service Provider(s)', the Government confirmed at the hearing that the warrant did not specify particular bearers, because there would be 'serious impracticalities and difficulties' if that were to be a requirement. Nevertheless, there had to be a proper description of what the interception would involve and details of the 'sorts of bearers' that would be intercepted. This information informed the Secretary of State's assessment of the necessity and proportionality of the conduct described in the application. Furthermore, the Government confirmed in their submissions to the Grand Chamber that the IC Commissioner was briefed regularly by GCHQ about the basis on which bearers were selected for interception (see paragraph 290 above).

381. The application for a section 8(4) warrant also did not have to include an indication of the categories of selectors to be employed. As a consequence, there was no possibility for their necessity and proportionality to be assessed at the authorisation stage, although the choice of selectors was thereafter subject to independent supervision. In their submissions before the Grand Chamber the Government confirmed that whenever a new selector was added to the system, the analyst adding it had to complete a written record, explaining why it was necessary and proportionate to apply the selector for the purposes within the Secretary of State's certificate. This was done by the selection of text from a drop down menu, followed by the addition, by the analyst, of free text explaining why it was necessary and proportionate to make the search. Furthermore, the use of selectors had to be recorded in an approved location that enabled them to be audited; created a searchable record of selectors in use; and enabled oversight by the IC Commissioner (see paragraphs 291–292 above). The choice of selectors was therefore subject to oversight by the IC Commissioner and in his 2016 annual report he 'was impressed by the quality of the statements' prepared by analysts explaining the necessity and proportionality of adding a new selector (see paragraph 177 above).

382. Given that the choice of selectors and query terms determined which communications would be eligible for examination by an analyst, the Court has indicated that it is of fundamental importance for at least the categories of selectors to be identified in the authorisation and for those strong selectors linked to identifiable individuals to be subject to prior internal authorisation providing for separate and objective verification of whether the justification conforms to the aforementioned principles (see paragraphs 353–355 above).

383. In the present case, the absence of any oversight of the categories of selectors at the point of authorisation was a deficiency in the section 8(4) regime. Neither did the subsequent control of all individual selectors satisfy the requirement for enhanced safeguards for the use of strong selectors linked to identifiable individuals and the need to have in place a process of prior internal authorisation providing for separate and objective verification of whether the justification conforms to the above mentioned principles (see paragraph 355 above). Although analysts had to record and justify the use of every selector with regard to the Convention principles of necessity and proportionality and that justification was subjected to independent supervision by the IC Commissioner, strong selectors linked to identifiable individuals were nevertheless not subject to prior internal authorisation.

— 4. The procedures to be followed for selecting, examining, and using intercept material

384. Paragraph 6.4 of the IC Code stipulated that where a section 8(4) warrant resulted in the acquisition of large volumes of communications, authorised persons within the intercepting agency could apply strong selectors and complex queries to generate an index (see paragraph 96 above). This selection process was circumscribed by section 16(2) of RIPA and paragraph 7.19 of the IC Code, which provided that a selector could not refer to an individual known to be in the British Islands, and have as a purpose the identification of material contained in communications sent by or intended for him or her, unless the Secretary of State had personally authorised the use of the selector, having first been satisfied that it was necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom so far as those interests were also relevant to the interests of national security; and was proportionate (see paragraphs 85 and 96 above).

385. Only material on the index could be viewed by an analyst (see paragraphs 96 and 289 above); and no intelligence report could be made of any communications or communications data unless they had been viewed by an analyst (see paragraph 289 above). Moreover, paragraph 7.13 of the IC Code provided that only material described in the Secretary of State's certificate was available for human examination, and no official was permitted to gain access to the material other than as permitted by the certificate (see paragraph 96 above). Paragraph 6.4 further provided that before a particular communication could be accessed by an authorised per-

son within the intercepting agency, the person had to explain why it was necessary for one of the reasons set out in the accompanying certificate, and why it was proportionate in the particular circumstances, having regard to whether the information could reasonably have been obtained by less intrusive means (see paragraph 96 above).

386. The Secretary of State's certificate was issued when he or she granted the warrant and was intended to ensure that a selection process was applied to the intercepted material so that only material described in the certificate was made available for human examination (see paragraphs 6.3 and 6.14 of the IC Code at paragraph 96 above). Although the certificate played an important role in regulating access to intercept material, the reports of the ISC and the Independent Reviewer of Terrorism Legislation both criticised the fact that the material identified in these certificates was couched in very general terms (for example, 'material providing intelligence on terrorism as defined in the Terrorism Act 2000 (as amended)') (see paragraph 342 of the Chamber judgment and paragraphs 146 and 155 above). The Court agrees with the Chamber that this was a deficiency in the system of safeguards available under the section 8(4) regime.

387. Nonetheless, according to the ISC, although the certificate set out the general categories of information which could be examined, in practice it was the selection of the bearers, the application of simple selectors and initial search criteria, and then complex searches which determined what communications were examined (see paragraphs 146–147 above). In other words, while the certificates regulated the analyst's selection of material from a computer generated index, it was the choice of bearers and selectors/search terms which determined which communications were on that index (and therefore eligible for examination) in the first place. However, the Court has already held that both the failure to identify the categories of selectors in the application for a warrant and the absence of prior internal authorisation of those strong selectors linked to an identifiable individual represented deficiencies in the section 8(4) regime (see paragraph 382 above). These deficiencies would have been exacerbated by the general nature of the Secretary of State's certificate. Not only was there no prior independent authorisation of the categories of selectors used to generate the index, and no internal authorisation of those strong selectors linked to an identifiable individual, but the certificate regulating access to material on that index was drafted in insufficiently precise terms to provide any meaningful restriction.

388. Paragraph 7.16 of the IC Code further required an analyst seeking access to material on the index to indicate any circumstances likely to give rise to a degree of collateral infringement of privacy, together with the measures taken to reduce the extent of that intrusion (see paragraph 96 above). Any subsequent access by the analyst was limited to a defined period of time, and if that period of time was renewed, the record had to be updated giving reasons for renewal (see paragraph 7.17 of the IC Code, at paragraph 96 above). According to paragraph 7.18 of the IC Code, regular audits were carried out which included checks to ensure that the records requesting access to material were compiled correctly, and that the material requested fell within the matters certified by the Secretary of State (see paragraph 96 above).

389. Furthermore, according to paragraph 7.15, material gathered under a section 8(4) warrant could only be read, looked at or listened to by authorised persons (analysts) who had received regular mandatory training regarding the provisions of RIPA and the requirements of necessity and proportionality, and who had been appropriately vetted (see paragraph 96 above). Pursuant to paragraph 7.10, the vetting of each individual member of staff was periodically reviewed (see paragraph 96 above).

390. Paragraph 7.6 of the IC Code provided that intercept material could only be copied to the extent necessary for the authorised purposes and subject to a strict application of the 'need to know' principle, including providing extracts or summaries where this was sufficient to satisfy the user's need to know. Section 15(5) of RIPA required arrangements to be in place for securing that every copy of the material or data that was made was stored, for as long as it was retained, in a secure manner (see paragraph 81 above); and paragraph 7.7 further required that prior to its destruction, intercept material, and all copies, extracts and summaries of it, had to be stored securely and could not be accessible to persons without the required level of security clearance (see paragraph 96 above).

391. Subject to the aforementioned deficiencies relating to the authorisation of the selectors (see paragraphs 381 and 382 above) and the general nature of the Secretary of State's certificate (see paragraph 386 above), the Court considers that the circumstances in which intercept material could be selected, examined, used and stored under the section 8(4) regime were sufficiently 'foreseeable' for the purposes of Article 8 of the Convention, and that they provided adequate safeguards against abuse.

— 5. The precautions to be taken when communicating the material to other parties

392. Section 15(2) of RIPA required that the following be limited to the minimum necessary for the 'authorised purposes': the number of persons to whom the material or data were disclosed or made available; the extent to which the material or data were disclosed or made available; the extent to which the material or data were copied; and the number of copies that were made (see paragraphs 78 above). Pursuant to section 15(4) and paragraph 7.2 of the IC Code, something was necessary for the authorised purposes if, and only if, it continued to be, or was likely to become, necessary for the pur-

poses mentioned in section 5(3) of RIPA; for facilitating the carrying out of any of the interception functions of the Secretary of State; for facilitating the carrying out of any functions of the IC Commissioner or of the IPT; to ensure that a person conducting a criminal prosecution had the information he or she needed to determine what was required by the duty to secure the fairness of the prosecution (although the intercept material could not itself be used in the prosecution of a criminal offence — see paragraph 8.3 of the IC Code at paragraph 96 above); or for the performance of any duty imposed on any person under public records legislation (see paragraphs 80 and 96 above).

393. Paragraph 7.3 of the IC Code prohibited disclosure to persons who had not been appropriately vetted and also by the 'need-to-know' principle: intercepted material could not be disclosed to any person unless that person's duties, which had to relate to one of the authorised purposes, were such that he or she 'needed to know' about the intercept material to carry out those duties. In the same way, only so much of the intercept material could be disclosed as the recipient needed (see paragraph 96 above). Paragraph 7.3 applied equally to disclosure to additional persons within an agency, and to disclosure outside the agency (see paragraph 96 above). Pursuant to paragraph 7.4, it also applied not just to the original interceptor, but also to anyone to whom the intercept material was subsequently disclosed (see paragraph 96 above).

394. As the Chamber observed, since 'likely to become necessary' was not further defined in RIPA or the IC Code, or indeed anywhere else, section 15(4) and paragraph 7.2 could in practice have given the authorities a broad power to disclose and copy intercept material. Nevertheless, the material could still only be disclosed to a person with the appropriate level of security clearance, who had a 'need to know', and only so much of the intercept material as the individual needed to know could be disclosed. The Court therefore agrees with the Chamber that the inclusion of 'likely to become necessary' did not significantly reduce the safeguards for the protection of data obtained by bulk interception (see paragraphs 368 and 369 of the Chamber judgment).

395. Turning, then, to the transfer of intercept material outside the United Kingdom, where material has been intercepted in accordance with domestic law, the Court considers that the transfer of that material to a foreign intelligence partner or international organisation would only give rise to an issue under Article 8 of the Convention if the intercepting State did not first ensure that its intelligence partner, in handling the material, had in place safeguards capable of preventing abuse and disproportionate interference, and in particular, could guarantee the secure storage of the material and restrict its onward disclosure (see paragraph 362 above).

396. In the United Kingdom it would appear that Five Eyes partners could access elements of the product of GCHQ's interception warrants on their own systems (see paragraph 180 above). In such cases, the interception of the material by the United Kingdom intelligence services would have been conducted in accordance with domestic law including, in so far as is relevant in the present case, section 8(4) of RIPA. According to paragraph 7.5 of the IC Code, where intercept material was disclosed to the authorities of a country or territory outside the United Kingdom, the intelligence services had to take reasonable steps to ensure that the authorities in question had and would maintain the necessary procedures to safeguard the intercept material, and to ensure that it was disclosed, copied, distributed and retained only to the minimum extent necessary. The intercept material could not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency and it had to be returned to the issuing agency or securely destroyed when no longer needed (see paragraph 96 above). Section 15(7) of RIPA further provided that restrictions should be in force which would prevent the doing of anything in connection with legal proceedings outside the United Kingdom which would disclose the content or related communications data of an intercepted communication where such a disclosure could not have been made in the United Kingdom (see paragraph 82 above).

397. In respect of confidential material, paragraph 4.30 of the IC Code provided that where confidential information was disseminated to an outside body, reasonable steps had to be taken to mark the information as confidential. Where there was any doubt as to the lawfulness of the proposed dissemination of confidential information, advice had to be sought from a legal adviser within the relevant intercepting agency and before any further dissemination of the material could take place (see paragraph 96 above).

398. There were therefore safeguards in place to ensure that intelligence partners would guarantee the secure storage of transferred material and restrict its onward disclosure. A final safeguard, to which the Court attaches particular weight, is the oversight provided by the IC Commissioner and the IPT (see paragraphs 411 and 414 below).

399. In light of the foregoing, the Court considers that the precautions to be taken when communicating intercept material to other parties were sufficiently clear and afforded sufficiently robust guarantees against abuse.

— 6. The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased or destroyed

400. As regards the duration of section 8(4) warrants issued for reasons of national security or the economic well-being of the United Kingdom so far as those interests were also relevant to the interests of national security, pursuant to section 9 of RIPA these ceased to have effect after six months, unless they were renewed. Section 8(4) warrants issued by

the Secretary of State for the purposes of preventing serious crime ceased to have effect after three months, unless renewed. These warrants were renewable for periods of six and three months respectively, and could be renewed at any point before their expiry date by application to the Secretary of State. That application had to contain the same information as the original application, together with an assessment of the value of the interception up to that point and an explanation of why its continuation was necessary, within the meaning of section 5(3), and proportionate (see section 9 of RIPA at paragraph 67 above and paragraphs 6.22–6.24 of the IC Code at paragraph 96 above). The Secretary of State had to cancel a warrant — even before the original expiry date — if satisfied that it was no longer necessary on section 5(3) grounds (see section 9 of RIPA at paragraph 67 above).

401. In view of the clear limitation on the duration of section 8(4) warrants, and the requirement that they be kept under continuous review, the Court considers that the rules in respect of the duration of interception under the section 8(4) regime were sufficiently clear and provided adequate safeguards against abuse.

402. Paragraph 7.9 of the IC Code provided that where an intelligence service received unanalysed intercept material and related communications data from interception under a section 8(4) warrant, it had to specify maximum retention periods for different categories of material which reflected its nature and intrusiveness. Those specified periods would normally be no longer than two years, and had to be agreed with the IC Commissioner. So far as possible, all retention periods had to be implemented by a process of automated deletion, triggered once the applicable maximum retention period had been reached (see paragraph 96 above). Pursuant to paragraph 7.8 of the IC Code retained intercept material had to be reviewed at appropriate intervals to confirm that the justification for its retention was still valid under section 15(3) of RIPA (see paragraph 96 above).

403. In their submissions to the Grand Chamber, the Government provided further information about the retention periods. Communications to which only the 'strong selector' process was applied were discarded immediately unless they matched the strong selector. Communications to which the 'complex query' process was also applied were retained for a few days, in order to allow the process to be carried out, and were then deleted automatically unless they had been selected for examination. Communications which had been selected for examination could be retained only where it was necessary and proportionate to do so. The default position was that the retention period for selected communications was no longer than a few months, after which they were automatically deleted (although if the material had been cited in intelligence reporting, the report would be retained), but in exceptional circumstances a case could be made to retain selected communications for longer (see paragraph 293 above). In practice, therefore, it would appear that the retention periods were significantly shorter than the two-year maximum retention period.

404. Finally, section 15(3) of RIPA and paragraph 7.8 of the IC Code required that every copy of intercept material (together with any extracts and summaries) be destroyed securely as soon as retention was no longer necessary for any of the section 5(3) purposes (see paragraphs 79 and 96 above).

405. In the *Liberty* proceedings, the IPT considered the arrangements for the retention of material and its destruction and found them to be adequate (see paragraph 50 above). The Court also considers that the 'above the waterline' arrangements setting out the circumstances in which intercept material had to be erased or destroyed were sufficiently clear. However, in its view it would have been desirable for the shorter retention periods identified by the Government in the course of the present proceedings to have been reflected in the appropriate legislative and/or other general measures.

— 7. Supervision

406. Supervision of the section 8(4) regime was primarily carried out by the IC Commissioner, although according to that Commissioner a 'critical quality assurance function [was] initially carried out by the staff and lawyers within the intercepting agency or the warrant-granting department', who provided independent advice to the Secretary of State and performed important pre-authorisation scrutiny of warrant applications and renewals to ensure that they were (and remained) necessary and proportionate (see paragraph 170 above).

407. The IC Commissioner was independent of the executive and the legislature, and had to have held high judicial office. His principal duty was to review the exercise and performance, by the relevant Secretaries of State and public authorities, of the powers under Part 1 (and to a limited extent Part 3) of RIPA and he oversaw an inspection regime that enabled him to carry out independent oversight of how the law was applied. He regularly reported on his activities, on a half-yearly basis, to the Prime Minister, and prepared an annual report which was placed before both Houses of Parliament. In addition, after each inspection a report was sent to the head of the inspected agency which contained formal recommendations and which required the agency to report back within two months to confirm whether the recommendations had been implemented or what progress had been made. His periodic reports have been published from 2002, and from 2013 they were published in full with no confidential annexes. Furthermore, section 58(1) of RIPA imposed a statutory obligation on every public official in an organisation within the IC Commissioner's remit to disclose or to provide to him all documents or information as might be required to

enable him to carry out his functions (see paragraphs 135 and 136 above).

408. The IC Commissioner's 2016 report provides evidence of the extent of his oversight powers. In summary, during inspections he evaluated the systems in place for the interception of communications and ensured that all relevant records had been kept; examined selected interception applications to assess whether they met the necessity and proportionality requirements; interviewed case officers and analysts to assess whether interceptions and the justifications for acquiring all of the material were proportionate; examined any urgent oral approvals to check that the process was justified and used appropriately; reviewed those cases where communications subject to legal privilege or otherwise confidential information had been intercepted and retained, and any cases where a lawyer was the subject of an investigation; reviewed the adequacy of the safeguards and arrangements under sections 15 and 16 of RIPA; investigated the procedures in place for the retention, storage and destruction of intercepted material and related communications data; and reviewed reported errors and the sufficiency of any measures put in place to prevent recurrence (see paragraph 171 above).

409. During 2016, the IC Commissioner's office inspected all nine interception agencies once and the four main warrant-granting departments twice. Nine hundred and seventy warrants were inspected, representing sixty-one percent of the number of warrants in force at the end of the year and thirty-two percent of the total of new warrants issued in 2016 (see paragraphs 173 and 175 above).

410. Inspections usually involved a three-stage process. First, to achieve a representative sample of warrants, inspectors selected them across different crime types and national security threats, focusing on those of particular interest or sensitivity. Secondly, inspectors scrutinized the selected warrants and associated documentation in detail during reading days which preceded the inspections. At this stage, inspectors examined the necessity and proportionality statements made by analysts when adding a selector to the collection system for examination. Each statement had to stand on its own and had to refer to the overall requirement of priorities for intelligence collection. Thirdly, they identified those warrants, operations or areas of the process which required further information or clarification and arranged to interview relevant operational, legal or technical staff. Where necessary, they examined further documentation or systems relating to those warrants (see paragraph 174 above).

411. The IC Commissioner also had oversight of the sharing of intercept material with intelligence partners. In his 2016 report he indicated that GCHQ had provided his inspectors with 'comprehensive details of the sharing arrangements whereby Five Eyes partners can access elements of the product of GCHQ's interception warrants on their own systems'. In addition, his inspectors were able to meet with representatives of the Five Eyes community and they received a demonstration of how other Five Eyes members could request access to GCHQ's intercept material. He observed that 'access to GCHQ systems was tightly controlled and had to be justified in accordance with the laws of the host country and handling instructions of section 15/16 safeguards.' He further observed that before getting any access to GCHQ's intercept material, Five Eyes analysts had to complete the same legalities training as GCHQ staff (see paragraph 180 above).

412. In light of the foregoing, the Court is satisfied that the IC Commissioner provided independent and effective supervision of the operation of the section 8(4) regime. In particular, he and his inspectors were able to assess the necessity and proportionality of a significant number of warrant applications and the subsequent choice of selectors, and to investigate the procedures in place for the retention, storage and destruction of intercepted communications and related communications data. They were also able to make formal recommendations to the head of the public authorities concerned and those authorities were required to report back, within two months, on the progress they had made in implementing those recommendations. Furthermore, the Government confirmed in their submissions to the Grand Chamber that the IC Commissioner was also briefed regularly by GCHQ about the basis on which bearers were selected for interception (see paragraphs 136 and 290 above). The intelligence services were required to keep records at each stage of the bulk interception process and they were obliged to grant inspectors access to those records (see paragraphs 6.27 and 6.28 of the IC Code at paragraph 96 above). Finally, he also had oversight of the sharing of intercept material with intelligence partners (see paragraph 180 above).

— 8. Ex post facto review

413. *Ex post facto* review was provided by the IPT which in the present case was presided over at all relevant times by a High Court Judge. The Chamber found — and the applicants have not disputed — that the IPT provides an effective remedy for applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes (see paragraph 265 of the Chamber judgment). In this regard, the Chamber found it significant that the IPT had extensive jurisdiction to examine any complaint of unlawful interception which was not dependent on notification of the interception to its subject (see paragraph 122 above). Consequently, any person who believed that he or she had been subject to secret surveillance could make an application to it. Its members had to have held high judicial office or be a qualified lawyer of at least ten years' standing (see paragraph 123 above). Those involved in the authorisation and execution of an intercept warrant were required to disclose to it all the documents it might require, including 'below the waterline' documents which could

not be made public for reasons of national security (see paragraph 125 above). Furthermore, it had discretion to hold oral hearings, in public, where possible (see paragraph 129 above); in closed proceedings it could ask Counsel to the Tribunal to make submissions on behalf of claimants who could not be represented (see paragraph 132 above); and when it determined a complaint it had the power to award compensation and make any other order it saw fit, including quashing or cancelling any warrant and requiring the destruction of any records (see paragraph 126 above). Finally, its legal rulings were published on its own dedicated website, thereby enhancing the level of scrutiny afforded to secret surveillance activities in the United Kingdom (see *Kennedy*, cited above, § 167).

414. In addition, the IPT had jurisdiction to consider any complaint about the Convention compliance either of the transfer of intercept material to third parties, or about the regime governing the transfer of intercept material. In the present case, however, the applicants in the third of the joined cases did not make any specific complaint in this respect in the course of the domestic proceedings. Rather, their complaints about intelligence sharing focused solely on the regime governing the receipt of intelligence from third countries (see paragraphs 467–516 below).

415. The Court is therefore satisfied that the IPT provided a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services.

(γ) Related communications data

416. The Court has indicated that in the context of bulk interception the interception, retention and searching of related communications data should be analysed by reference to the same safeguards applicable to content, but that the legal provisions governing the treatment of related communications data do not necessarily have to be identical in every respect to those governing the treatment of content (see paragraphs 363–364 above). In the United Kingdom section 8(4) warrants authorised the interception of both content and related communications data. The latter were, in most respects, treated identically under the section 8(4) regime. Thus, the deficiencies already identified in respect of that regime governing the interception of content (see paragraphs 377, 381 and 382 above) applied equally to related communications data, namely: the absence of independent authorisation (see paragraph 377 above); the failure to identify the categories of selectors in the application for a warrant (see paragraphs 381 and 382 above) and the failure to subject those selectors linked to identifiable individuals to prior internal authorisation; and the lack of foreseeability of the circumstances in which communications could be examined (see paragraph 391 above), having regard both to the failure to identify the categories of selectors in the application for a warrant (see paragraphs 381 and 382 above) and to the general nature of the Secretary of State's certificate (see paragraph 386 above).

417. At the same time, the treatment of communications data benefitted in most part from the same safeguards as applied to content. Like the latter, the former were subject to an automated filtering process in near-real time, with a substantial proportion of them being instantly deleted at this stage; and they were also subject to simple or complex queries in order to draw out the material that was of potential intelligence value. Moreover, the selectors used in respect of related communications data were subject to the same safeguards as content; most notably, analysts had to complete a written record explaining why each new selector added to the system was necessary and proportionate, that record was subject to audit by the IC Commissioner, selectors had to be removed if it was established that they were not being used by their intended target, and there was a maximum time during which selectors could remain in use before a review was necessary (see paragraph 298 above).

418. Content and related communications data were also subject to many of the same procedures for storage, access, examination and use, the same precautions for communication to third parties, and the same procedures for erasure and destruction. In this regard, both content and related communications data were subject to the safeguards in section 15 of RIPA; analysts wishing to access related communications data had to complete an auditable record explaining why access was necessary and proportionate; and no intelligence reporting could be made on the basis of related communications data unless and until they had been examined.

419. There were, however, two principal ways in which the bulk interception regime treated content and related communications data differently: related communications data were excluded from the section 16(2) safeguard, meaning that if an analyst wished to use a selector referable to an individual known for the time being to be in the British Islands, he or she was not required to have the use of that selector certified as necessary and proportionate by the Secretary of State; and related communications data which did not match either a strong selector or a complex query were not destroyed immediately, but were instead stored for a maximum period of up to several months (see paragraphs 296–298 above). The Court will therefore examine whether domestic law clearly defined the procedures to be followed for selecting related communications data for examination, and the limits on the duration of the storage of related communications data.

420. Under the section 8(4) regime, section 16(2) was the principal statutory safeguard circumscribing the process of selecting intercept material for examination. However, it was not the only safeguard. As already noted at paragraph 417 above, all new selectors had to be justified by analysts through the creation of a written record explaining why the choice of selector was both necessary and propor-

tionate (see paragraphs 291–292 and 298 above); analysts wishing to examine related communications data had to complete a further record explaining why it was necessary and proportionate to do so, in pursuit of GCHQ's statutory functions (see paragraph 6.4 of the IC Code, at paragraph 96 above); and these records were subject to audit and oversight by the IC Commissioner (see paragraphs 135–136 and 381 above). According to the Government, it would not have been feasible to extend the section 16(2) safeguard to related communications data, since this would have required the Secretary of State to certify the necessity and proportionality of targeting the individual concerned in every case. The number of queries made against communications data was significantly higher than the number of queries made against content (possibly many thousands in any given week in relation to individuals known or believed to be in the United Kingdom), and in many of these cases the identity of the individual would not be known. In addition, the Government pointed out that related communications data had a temporal quality, and having to delay the conducting of searches pending acquisition of an individual authority would seriously risk undermining their use in intelligence terms (see paragraph 296 above).

421. The Court accepts that related communications data are an essential tool for the intelligence services in the fight against terrorism and serious crime, and that there would be circumstances in which it was both necessary and proportionate to search for and access the related communications data of persons known to be in the United Kingdom. Moreover, while section 16(2) contains an important safeguard governing the process of selecting intercept material for examination, it is noteworthy that in assessing the regime governing the bulk interception of content, the Court placed considerably more weight on the existence or otherwise of an effective mechanism to ensure that the choice of selectors was both subject to the Convention requirements of necessity and proportionality; and subject to both internal and external oversight. Therefore, while the Court would echo the concerns raised in respect of the choice and oversight of selectors at paragraphs 381 and 382 above, it does not consider that the exclusion of related communications data from the section 16(2) safeguard should carry decisive weight in the overall assessment.

422. As for the duration of storage, the Government contended that related communications data 'require more analytical work, over a lengthy period, to discover 'unknown unknowns". That discovery could involve an exercise of piecing together disparate small items of communications data to form a 'jigsaw' revealing a threat, and would include the possible examination of items that initially appeared to be of no intelligence interest. Discarding unselected communications data immediately, or even after a few days, would render that exercise impossible (see paragraph 297 above).

423. In light of the foregoing, and in view of the fact that there was a maximum retention period, which did not exceed 'several months', and the difference in treatment was objectively and reasonably justified, the Court would accept that the storage provisions concerning related communications data were sufficiently robust, even though they differed in substance from the provisions relating to content. However, these retention periods were only disclosed in the proceedings before this Court. Consequently, the shorter retention periods were not evident to anyone reading the IC Code; nor was there any indication in the IC Code that the retention periods for related communications data were different from those in respect of content. In the Court's view, in order to meet the Article 8 requirement of 'foreseeability', the retention periods disclosed in the proceedings before it should be included in appropriate legislative and/or other general measures.

(δ) Conclusion

424. The Court accepts that bulk interception is of vital importance to Contracting States in identifying threats to their national security. This has been recognised by the Venice Commission (see paragraph 196 above) and was the position adopted by the respondent Government as well as the Governments of France and the Netherlands in their third party interventions (see paragraphs 300 and 303 above). It was also the conclusion of the Independent Reviewer of Terrorism Legislation, who, having examined a great deal of closed material, concluded that bulk interception was an essential capability: first, because terrorists, criminals and hostile foreign intelligence services had become increasingly sophisticated at evading detection by traditional means; and secondly, because the nature of the global Internet meant that the route a particular communication would travel had become hugely unpredictable. Although he and his team considered alternatives to bulk interception (including targeted interception, the use of human sources and commercial cyber-defence products), they concluded that no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power (see paragraph 166 above).

425. Nonetheless, the Court recalls that there is considerable potential for bulk interception to be abused in a manner adversely affecting the rights of individuals to respect for private life (see paragraph 347 above). Therefore, in a State governed by the rule of law, which is expressly mentioned in the Preamble to the Convention and is inherent in the object and purpose of Article 8 (see *Roman Zakharov*, cited above, § 228), the Court considers that, when viewed as a whole, the section 8(4) regime, despite its safeguards, including some robust ones as highlighted above (see, for example, paragraphs 412 and 415 above), did not contain sufficient 'end-to-end' safeguards to provide adequate and effective guarantees against arbitrariness and the risk of abuse. In particular, it has identified the following fundamental de-

ficiencies in the regime: the absence of independent authorisation, the failure to include the categories of selectors in the application for a warrant, and the failure to subject selectors linked to an individual to prior internal authorisation (see paragraphs 377–382 above). These weaknesses concerned not only the interception of the contents of communications but also the interception of related communications data (see paragraph 416 above). While the IC Commissioner provided independent and effective oversight of the regime, and the IPT offered a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services, these important safeguards were not sufficient to counterbalance the shortcomings highlighted at paragraphs 377–382 above.

426. In view of the aforementioned shortcomings, the Court finds that section 8(4) did not meet the 'quality of law' requirement and was therefore incapable of keeping the 'interference' to what was 'necessary in a democratic society'.

427. There has accordingly been a violation of Article 8 of the Convention.

C. The alleged violation of Article 10 of the Convention

428. The applicants in both the second and the third of the joined cases complained under Article 10 of the Convention about the section 8(4) regime, arguing that the protection afforded by Article 10 to privileged communications was of critical importance to them as journalists and NGOs respectively. However, as the Chamber declared the complaint by the applicants in the third of the joined cases inadmissible for failure to exhaust domestic remedies, only the Article 10 complaint relating to journalists is within the scope of the case referred to the Grand Chamber.

429. Article 10 of the Convention provides:

> '1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.'

1. The Chamber judgment

430. The Chamber found that as the surveillance measures under the section 8(4) regime were not aimed at monitoring journalists or uncovering journalistic sources, the interception of such communications could not, by itself, be characterised as a particularly serious interference with freedom of expression. However, it considered that the interference would be greater if those communications were selected for examination. If that were the case the interference could only be 'justified by an overriding requirement in the public interest' if it was accompanied by sufficient safeguards. In particular, the circumstances in which such communications could be selected intentionally for examination would have to be set out sufficiently clearly in domestic law, and there would have to be adequate measures in place to ensure the protection of confidentiality where such communications had been selected, either intentionally or otherwise, for examination. In the absence of any publicly available arrangements limiting the intelligence services' ability to search and examine confidential journalistic material other than where it was justified by an overriding requirement in the public interest, the Chamber found that there had also been a violation of Article 10 of the Convention.

2. The parties' submissions

(a) The applicants

431. The applicants in the second of the joined cases argued that the bulk interception regime was in breach of Article 10 because the large scale interception and the maintaining of large databases of information had a chilling effect on freedom of communication for journalists.

432. In view of the fundamental importance of press freedom, the applicants submitted that any interference with journalistic freedom, and in particular the right to maintain confidentiality of sources, had to be attended with legal procedural safeguards commensurate with the importance of the principle at stake. In particular, the notion of 'in accordance with the law' required that where a measure was capable of identifying journalistic sources or revealing journalistic material it had to have been authorised by a judge or other independent and impartial decision-making body; the review had to be *ex ante*; and the authorising body had to be invested with the power to determine whether it was 'justified by an overriding requirement in the public interest' and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest (see *Sanoma Uitgevers B.V. v. the Netherlands* [GC], no. 38224/03, 14 September 2010). None of these safeguards were present in the section 8(4) regime.

(b) The Government

433. The Government argued first, that there was no authority in the Court's case-law for the proposition that prior judicial (or independent) au-

thorisation was required for the operation of a strategic monitoring regime by virtue of the fact that some journalistic material might be intercepted in the course of that regime's operation. Rather, the Court had drawn a sharp distinction between the strategic monitoring of communications and/or communications data, which might inadvertently 'sweep up' some journalistic material, and measures that targeted journalistic material (see *Weber and Saravia*, cited above, § 151, and contrast *Sanoma Uitgevers B.V.*, cited above, and *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, 22 November 2012). A requirement of prior judicial authorisation would make no sense in the context of bulk interception, since the judge could only be told that there was a possibility that the execution of the warrant might result in the interception of some confidential journalistic material.

434. That being said, the Government accepted the Chamber's conclusion that further protection was required at the point of selection for examination. It therefore confirmed that the IC Code had been amended to provide that '[p]articular consideration should be given to the interception of communications or the selection for examination of content containing information where individuals might reasonably assume a high degree of confidentiality. This includes where the communications contain information that is legally privileged; confidential journalistic material or where communications identify a journalist's source'.

(c) The third party interveners

(i) The Government of France

435. The Government of France argued that the surveillance of journalists was permissible under Article 10 of the Convention if it pursued a legitimate aim and was necessary, and if the measure did not target the journalists and was not aimed at identifying their sources. No parallel could be drawn between the situation where journalists' communications were intercepted by chance, and where a decision of the national authorities required a journalist to reveal his or her sources.

(ii) The Government of the Kingdom of Norway

436. The Norwegian Government submitted that the wide margin of appreciation allowed under Article 8 with regard to the decision to introduce a bulk interception regime also logically applied when the decision was scrutinised from the point of view of Article 10. It would defeat the nature and purpose of a bulk interception regime if the Court were to subject the decision to set it up to the 'justified by an overriding requirement in the public interest' test simply because some of the intercepted communications might involve contact with journalists.

(iii) The United Nations' Special Rapporteur on the promotion of the right to freedom of opinion and expression

437. The Special Rapporteur argued that surveillance measures interfered with the right to freedom of expression and therefore had to comply with Article 19(3) of the ICCPR, which required restrictions on expression to 'only be such as are provided by law and are necessary' for the protection of the rights and reputations of others, national security, public order, or public health or morals. Mass surveillance programmes provided significant challenges to the requirement of accessible legislation, due to the complexity of how surveillance technologies functioned, vague legal standards for intercepting communications, and complicated and often classified administrative frameworks. In addition, there was a serious proportionality concern relating to interference with the work of journalists and protection of their sources. As human rights law afforded confidentiality a high standard of protection, restrictions should be exceptional and implemented by judicial authorities only and circumventions not authorised by judicial authorities according to clear and narrow legal rules should not be used to undermine source confidentiality. In this regard, the scope of the protection of confidential communications had to take account of the broad understanding of 'journalist' under the ICCPR.

(iv) Article 19

438. Article 19 urged the Court to extend the same protection to NGOs as it normally extended to journalists.

(v) The Helsinki Foundation for Human Rights

439. The Helsinki Foundation submitted that the protection of journalistic sources was undermined not only by the surveillance of the content of journalists' communications, but also by the surveillance of related metadata which could, by itself, allow for the identification of sources and informants. It was especially problematic that confidential information could be acquired without the journalists' knowledge or control, thereby depriving them of their right to invoke confidentiality, and their sources of their ability to rely on guarantees of confidentiality.

(vi) The Media Lawyers' Association ('MLA')

440. The MLA expressed concern that mass surveillance regimes were capable of intercepting journalistic communications and communications data which could identify sources. In their view, the mere interception of journalistic material could interfere with Article 10 of the Convention, even if the material was not actually analysed. It was therefore imperative that appropriate safeguards were in place to protect the confidentiality of journalistic sources, regardless of the purpose for which information was collected. Moreover, a regime permitting States

to intercept journalists' communications without prior judicial authorisation was more likely to affect journalism that was in the public interest because the nature of such stories meant that the State would have a particular interest in identifying the sources. The risk would be particularly grave where the source was a government whistle-blower. The chilling effect of the mere potential that such sources would be identified was significant. As a consequence, the MLA argued that at a minimum Article 10 required prior independent judicial oversight of any attempt to obtain journalistic material or identify journalistic sources, and that the judicial process be *inter partes*.

(vii) The National Union of Journalists ('NUJ') and the International Federation of Journalists ('IFJ')

441. The NUJ and the IFJ submitted that the confidentiality of sources was indispensable for press freedom. They also expressed concern about the possible sharing of data retained by the United Kingdom with other countries. If confidential journalistic material were to be shared with a country which could not be trusted to handle it securely, it could end up in the hands of people who would harm the journalist or his or her source. In the interveners' view, the safeguards in the updated IC Code and the Acquisition of Communications Data Code of Practice were not adequate, especially where the journalist or the identification of his or her source was not the target of the surveillance measure.

3. The Court's assessment

(a) General principles on the protection of journalists' sources

442. As freedom of expression constitutes one of the essential foundations of a democratic society, the Court has always subjected the safeguards for respect of freedom of expression in cases under Article 10 of the Convention to special scrutiny. 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. As a result the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information may be affected adversely (see, *inter alia, Goodwin v. the United Kingdom*, no. 17488/90, § 39, 27 March 1996; *Sanoma Uitgevers B.V.*, cited above, § 50; and *Weber and Saravia*, cited above, § 143).

443. Orders to disclose sources potentially have a detrimental impact, not only on the source, whose identity may be revealed, but also on the newspaper or other publication against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources by the disclosure; and on members of the public, who have an interest in receiving information imparted through anonymous sources. There is, however, 'a fundamental difference' between the authorities ordering a journalist to reveal the identity of his or her sources, and the authorities carrying out searches at a journalist's home and workplace with a view to uncovering his or her sources (compare *Goodwin*, cited above, § 39, with *Roemen and Schmit v. Luxembourg*, no. 51772/99, § 57, ECHR 2003-IV). The latter, even if unproductive, constitutes a more drastic measure than an order to divulge a source's identity, since investigators who raid a journalist's workplace have access to all the documentation held by the journalist (see *Roemen and Schmit*, cited above, § 57).

444. 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 (see *Sanoma Uitgevers B.V.*, cited above, § 51; *Goodwin*, cited above, § 39; *Roemen and Schmit*, cited above, § 46; and *Voskuil v. the Netherlands*, no. 64752/01, § 65, 22 November 2007). Furthermore, any interference with the right to protection of journalistic sources must be attended with legal procedural safeguards commensurate with the importance of the principle at stake (see *Sanoma Uitgevers B.V.*, cited above, §§ 88–89). First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making 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 and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not (see *Sanoma Uitgevers B.V.*, cited above, §§ 88–90).

445. Given the preventive nature of such review the judge or other independent and impartial body must be in a position to carry out this weighing of the potential risks and respective interests prior to any disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be assessed properly. The decision to be taken should be governed by clear criteria, including whether a less intrusive measure can suffice to serve the overriding public interests established. It should be open to the judge or other authority to refuse to make a disclosure order or to make a limited or qualified order so as to protect sources from being revealed, whether or not they are specifically named in the withheld material, on the grounds that the communication of such material creates a serious risk of compromising the identity of journalist's sources (see *Sanoma Uitgevers B.V.*, cited above, § 92 and *Nordisk Film & TV A/S v. Denmark* (dec.), no. 40485/02, ECHR 2005-XIII). In situations of urgency, a procedure should exist to identify and isolate, prior to the exploitation of the material by the authorities, information that could lead to the identification of sources from information that carries no such risk (see, *mutatis mutandis, Wieser and*

Bicos Beteiligungen GmbH v. Austria, no. 74336/01, §§ 62–66, ECHR 2007-XI).

(b) Article 10 in the bulk interception context

446. In *Weber and Saravia* the Court recognised that the 'strategic monitoring' regime had interfered with the first applicant's freedom of expression as a journalist. However, in so finding it considered it decisive that the surveillance measures were not aimed at monitoring journalists or uncovering journalistic sources. As such, it found that the interference with the first applicant's freedom of expression could not be characterised as particularly serious and, in view of the attendant safeguards, it declared her complaints inadmissible as manifestly ill-founded (see *Weber and Saravia*, cited above, §§ 143–145 and 151).

(c) The approach to be adopted in the present case

447. Under the section 8(4) regime, confidential journalistic material could have been accessed by the intelligence services either intentionally, through the deliberate use of selectors or search terms connected to a journalist or news organisation, or unintentionally, as a 'bycatch' of the bulk interception operation.

448. Where the intention of the intelligence services is to access confidential journalistic material, for example, through the deliberate use of a strong selector connected to a journalist, or where, as a result of the choice of such strong selectors, there is a high probability that such material will be selected for examination, the Court considers that the interference will be commensurate with that occasioned by the search of a journalist's home or workplace; regardless of whether or not the intelligence services' intention is to identify a source, the use of selectors or search terms connected to a journalist would very likely result in the acquisition of significant amounts of confidential journalistic material which could undermine the protection of sources to an even greater extent than an order to disclose a source (see *Roemen and Schmit*, cited above, § 57). Therefore, the Court considers that before the intelligence services use selectors or search terms known to be connected to a journalist, or which would make the selection of confidential journalistic material for examination highly probable, the selectors or search terms must have been authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether they were 'justified by an overriding requirement in the public interest' and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest (see *Sanoma Uitgevers B.V.*, cited above, §§ 90–92).

449. Even where there is no intention to access confidential journalistic material, and the selectors and search terms used are not such as to make the selection of confidential journalistic material for examination highly probable, there will nevertheless be a risk that such material could be intercepted, and even examined, as a 'bycatch' of a bulk interception operation. In the Court's view, this situation is materially different from the targeted surveillance of a journalist through either the section 8(1) or the section 8(4) regimes. As the interception of any journalistic communications would be inadvertent, the degree of interference with journalistic communications and/or sources could not be predicted at the outset. Consequently, it would not be possible at the authorisation stage for a judge or other independent body to assess whether any such interference would be 'justified by an overriding requirement in the public interest' and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest.

450. In *Weber and Saravia* the Court held that the interference with freedom of expression caused by strategic monitoring could not be characterised as particularly serious as it was not aimed at monitoring journalists and the authorities would know only when examining the intercepted telecommunications, if at all, that a journalist's communications had been monitored (see *Weber and Saravia*, cited above, § 151). Therefore, it accepted that the initial interception, without examination of the intercepted material, did not constitute a serious interference with Article 10 of the Convention. Nevertheless, as the Court has already observed, in the current, increasingly digital, age technological capabilities have greatly increased the volume of communications traversing the global Internet, and as a consequence surveillance which is not targeted directly at individuals has the capacity to have a very wide reach indeed, both within and without the territory of the surveilling State (see paragraphs 322–323 above). As the examination of a journalist's communications or related communications data by an analyst would be capable of leading to the identification of a source, the Court considers it imperative that domestic law contain robust safeguards regarding the storage, examination, use, onward transmission and destruction of such confidential material. Moreover, even if a journalistic communication or related communications data have not been selected for examination through the deliberate use of a selector or search term known to be connected to a journalist, if and when it becomes apparent that the communication or related communications data contain confidential journalistic material, their continued storage and examination by an analyst should only be possible if authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether continued storage and examination is 'justified by an overriding requirement in the public interest'.

(d) Application of the aforementioned test to the facts of the present case

451. In *Weber and Saravia* the Court expressly recognised that the impugned surveillance regime had interfered with the first applicant's right to freedom of expression as a journalist (see *Weber and Saravia*, cited above, §§ 143–145). In the present case, the Court has accepted that the operation of the section 8(4) regime interfered with all of the applicants' rights under Article 8 of the Convention (see paragraphs 324–331 above). As the applicants in the second of the joined cases' were a newsgathering organisation and a journalist respectively, the Court would accept that the section 8(4) regime also interfered with their right under Article 10 of the Convention to freedom of expression as journalists.

452. As already noted, the section 8(4) regime had a clear basis in domestic law (see paragraphs 365 and 366 above). However, in assessing foreseeability and necessity under Article 8 of the Convention, the Court identified the following deficiencies in the regime and its attendant safeguards: the absence of independent authorisation (see paragraph 377 above); the failure to identify the categories of selectors in the application for a warrant (see paragraphs 381–382 above); and the absence of prior internal authorisation for selectors linked to an identifiable individual (see paragraph 382 above).

453. Nonetheless, some additional safeguards in respect of confidential journalistic material were set out in paragraphs 4.1–4.3 and 4.26–4.31 of the IC Code (see paragraph 96 above). According to paragraph 4.1, 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. However, paragraph 4.1 only required the Secretary of State to take these circumstances and measures into account when considering an application for a section 8(1) warrant, that is, a warrant authorising targeted interception. Paragraph 4.2 further provided that 'particular consideration should also be given' in cases where confidential journalistic material might have been involved, and paragraph 4.26 stated that 'particular consideration' had to be given to the interception of communications that involved confidential journalistic material.

454. According to the Government paragraph 4.28 also applied to confidential journalistic material. Where the intention was to acquire confidential *personal* information, paragraph 4.28 indicated that the reasons and the specific necessity and proportionality of doing so had to be documented clearly. If the acquisition of such material was likely but not intended, any possible mitigation steps had to be considered and, if none were available, consideration had to be given to whether special handling arrangements were required within the intercepting agency (see paragraph 96 above). The Court notes, however, that in paragraph 4.26 of the IC Code, 'confidential personal information' appeared to be something distinct from 'confidential journalistic material' (see paragraph 96 above).

455. As for the storage of confidential material, paragraph 4.29 of the IC Code provided that such material could only be retained where it was necessary and proportionate for one of the authorised purposes in section 15(4) of RIPA, and it had to be destroyed securely when it was no longer needed for one of those purposes (see paragraph 96 above). Furthermore, according to paragraph 4.30, if it was retained or disseminated to an outside body, reasonable steps had to be taken to mark the information as confidential. Where there was any doubt as to the lawfulness of the proposed dissemination of confidential information, advice had to be sought from a legal adviser within the relevant intercepting agency and before any further dissemination of the material could take place (see paragraph 96 above). Finally paragraph 4.31 required that the IC Commissioner be notified of the retention of such material as soon as reasonably practicable, and that such material be made available to him on request (see paragraph 96 above).

456. In light of the above, the Court would accept that the safeguards in the IC Code concerning the storage, onward transmission and destruction of confidential journalistic material were adequate. However, the additional safeguards in the IC Code did not address the weaknesses identified by the Court in its analysis of the regime under Article 8 of the Convention, nor did they satisfy the requirements identified by the Court at paragraphs 448–450 above. In particular, there was no requirement that the use of selectors or search terms known to be connected to a journalist be authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether it was 'justified by an overriding requirement in the public interest' and whether a less intrusive measure might have sufficed to serve the overriding public interest. On the contrary, where the intention was to access confidential journalistic material, or that was highly probable in view of the use of selectors connected to a journalist, all that was required was that the reasons for doing so, and the necessity and proportionality of doing so, be documented clearly.

457. Moreover, there were insufficient safeguards in place to ensure that once it became apparent that a communication which had not been selected for examination through the deliberate use of a selector or search term known to be connected to a journalist nevertheless contained confidential journalistic material, it could only continue to be stored and examined by an analyst if authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether its continued storage and examination was 'justified by an overriding requirement in the public interest'. Instead, all that was required by paragraph 4.2 of the IC Code was that 'particular

consideration' be given to any interception which might have involved the interception of confidential journalistic material, including consideration of any possible mitigation steps (see paragraph 96 above).
458. In view both of these weakness, and those identified by the Court in its consideration of the complaint under Article 8 of the Convention, it finds that there has also been a breach of Article 10 of the Convention by virtue of the operation of the section 8(4) regime.

III. The receipt of intelligence from foreign intelligence services
A. Article 8 of the Convention
459. The applicants in the first of the joined cases complained about the receipt by the United Kingdom authorities of material from foreign intelligence services. The applicants in the third of the joined cases complained more specifically that the respondent State's receipt of material intercepted by the NSA under PRISM and Upstream was in breach of their rights under Article 8 of the Convention.

1. Scope of the complaint before the Grand Chamber
460. In the *Liberty* proceedings the IPT identified three categories of material which could be received from foreign intelligence partners: unsolicited intercept material; solicited intercept material; and non-intercept material. As the Government informed the Chamber that it was 'implausible and rare' for intercept material to be obtained 'unsolicited', the Chamber did not examine material falling into this category (see paragraph 417 of the Chamber judgment). The Chamber also declined to examine the receipt of non-intercept material, since the applicants had not specified the kind of material foreign intelligence services might obtain by methods other than interception and, as such, it was not satisfied that they had demonstrated that its acquisition would interfere with their Article 8 rights (see paragraph 449 of the Chamber judgment). The applicants have not contested either of these findings.
461. Furthermore, as the *Liberty* proceedings were brought by the applicants in the third of the joined cases, the IPT only considered the receipt of intelligence from the NSA. In their submissions before the Chamber and the Grand Chamber, the parties also focused on the receipt of material from the NSA.
462. The Grand Chamber will therefore limit its examination to the complaint about the receipt of solicited intercept material from the NSA.

2. The Government's preliminary objection
463. The Government argued that the applicants in the first and third of the joined cases could not claim to be victims of the alleged violation because neither of the two conditions in *Roman Zakharov* (cited above, §171) were met (namely, the applicants could not possibly have been affected by the legislation permitting secret surveillance measures, and remedies were available at the national level). In particular, they argued that the applicants had put forward no basis on which they were at realistic risk either of having their communications intercepted under PRISM or Upstream, or of having their communications requested by the United Kingdom intelligence services. In addition, they submitted that the applicants had available to them an effective domestic remedy to discover whether they were the subject of unlawful intelligence sharing.

(a) The Chamber judgment
464. As the Chamber accepted that the IPT had afforded the applicants an effective remedy for their Convention complaint, it considered that they could only claim to be 'victims' on account of the mere existence of the intelligence sharing regime if they were able to show that they were potentially at risk of having their communications obtained by the United Kingdom authorities through a request to a foreign intelligence service (see paragraphs 392–393 of the Chamber judgment, referring to *Roman Zakharov*, cited above, § 171).
465. On the basis of the information submitted to it, the Chamber found that the applicants were potentially at risk both of having their communications obtained by a foreign intelligence service, and requested from a foreign intelligence service by the United Kingdom authorities (see paragraph 395 of the Chamber judgment). Although they could only have had their communications requested if there was either an Article 8(1) or 8(4) warrant in place which covered their communications, it was clear from the *Liberty* proceedings that at least two of the applicants in the third of the joined cases had their communications lawfully intercepted and selected for examination by the United Kingdom intelligence services under the section 8(4) regime. While the Chamber found no reason to believe that these applicants were themselves of interest to the intelligence services, it observed that their communications could have been obtained lawfully under the section 8(4) regime if, as they claimed, they were in contact with persons who were. Similarly, their communications could have been requested lawfully from a third country under the intelligence sharing regime if they were in contact with an individual who was the subject of a request.
466. As Upstream functioned in a similar manner to the section 8(4) regime, the Chamber also accepted that the applicants' communications could potentially have been obtained by the NSA.

(b) The Court's assessment
467. The applicants have not challenged the Chamber's finding that the IPT offered an effective domestic remedy for Convention complaints about the operation of a surveillance regime, and, for the reasons expounded in paragraphs 413–415 above, the Grand Chamber agrees with that finding. Therefore, as the Chamber observed, the applicants could only claim to be 'victims' on account of the

mere existence of the intelligence sharing regime if they were able to show that they were potentially at risk of having their communications obtained by the United Kingdom authorities through a request to a foreign intelligence service (see *Roman Zakharov*, cited above, § 171). This would only be the case if they were potentially at risk both of having their communications intercepted by a foreign intelligence service and of having those communications requested by GCHQ.

468. The Government, focusing on the receipt of intelligence from the United States, argued that the applicants were not potentially at risk of having their communications intercepted under Upstream, as it was a targeted interception regime. However, according to the NSA, prior to April 2017 Upstream acquired communications to, from or about a section 702 selector (such as an email address); and only from April 2017 onwards it acquired communications to or from a section 702 selector (see paragraph 263 above). Given that section 702 selectors were applied to all communications flowing over specified cables, it would appear that Upstream was not so very different to the section 8(4) regime, which also intercepted all communications flowing over a number of cables and filtered them using selectors. The only apparent difference between the two regimes was that from April 2017 the NSA could only search for communications to or from a strong selector, while GCHQ retained the ability to perform searches by way of complex queries.

469. In the course of the *Liberty* proceedings the IPT confirmed that at least two of the applicants in the third of the joined cases had not only had some of their communications intercepted pursuant to a section 8(4) warrant, but had also had those communications lawfully and proportionately retained pursuant to that warrant (see paragraphs 58–60 above). In order to have been retained lawfully those communications must have matched either a 'strong selector' (pertaining either to the applicants or someone they were in contact with) or a 'complex query'. The Court would accept that if some of the applicants' communications matched a 'strong selector' used by GCHQ, they would also have been potentially at risk of being intercepted and retained by the NSA under Upstream on the basis that they were 'to' or 'from' a section 702 selector. Even if they did not match a strong selector, some of the applicants' communications must nevertheless have been of intelligence interest. Prior to April 2017 they could also have been intercepted and retained under Upstream if they were 'about' a section 702 selector. If this was the case, at the relevant time (that is, 7 November 2017) those communications may still have been held by the NSA since, following the change in policy in April 2017, it only indicated that it would delete previously acquired Upstream Internet communications 'as soon as practicable' (see paragraph 263 above). Therefore, communications acquired before that date which were 'about' a strong selector might have continued to be stored by the NSA for some time thereafter.

470. Consequently, the Court would accept that at the relevant time (that is, 7 November 2017) the applicants in the first and third of the joined cases were potentially at risk of having had at least some of their communications intercepted and retained under Upstream.

471. Nevertheless, the applicants could still only be victims for the purposes of the intelligence sharing regime if they were also potentially at risk of having their communications requested by GCHQ, and such a request could only have been made where a warrant was already in place for the material sought. However, as the Court has already noted, the fact that the communications of at least two of the applicants in the third of the joined cases were retained by GCHQ suggests that at least some of their communications were covered by a section 8(4) warrant. Consequently, the Court would accept that the applicants in the first and third of the joined cases were potentially at risk of also having their communications requested by GCHQ.

472. Accordingly, it finds that the applicants in the first and third of the joined cases can claim to be victims in respect of their complaints about the intelligence sharing regime. The Government's preliminary objection is therefore dismissed.

3. The merits

(a) The Chamber judgment

473. In considering the Article 8 compliance of the regime governing the receipt of intercept material from foreign intelligence services such as the NSA, the Chamber applied a modified version of the six minimum safeguards (see paragraph 275). Since the first two requirements could not apply to the act of requesting intercept material from foreign governments, the Chamber instead asked whether the circumstances in which intercept could be requested was circumscribed sufficiently to prevent States from using the power to circumvent domestic law or their Convention obligations. It then applied the final four requirements to the treatment of intercept material once it had been obtained by the United Kingdom intelligence services.

474. The Chamber considered that the domestic law, together with the clarifications brought by the amendment of the IC Code, indicated with sufficient clarity the procedure for requesting either interception or the conveyance of intercept material from foreign intelligence services. Moreover, the Chamber found no evidence of any significant shortcomings in the application and operation of the regime. It therefore held, by a majority, that there had been no violation of Article 8 of the Convention.

(b) The parties' submissions

475. The applicants submitted that the safeguards in place in respect of the intelligence sharing regime were inadequate. In particular, they argued that the problems which had led the Chamber to

find a violation of Article 8 of the Convention in respect of the bulk interception regime (that is, the lack of oversight of the use of selectors and the inadequate safeguards in respect of related communications data) applied equally to the intelligence sharing regime.

476. The Government, on the other hand, submitted that the intelligence sharing regime had a clear basis in domestic law, being set down in statute supplemented by Chapter 12 of the IC Code; and that law had been accessible. With regard to foreseeability, the Government argued that instead of applying a modified version of the six minimum safeguards, the Chamber should instead have applied the more general test — commonly applied in intelligence gathering cases which did not involve the interception of communications — of whether the law indicated the scope of any discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. In any event, the Government contended that the intelligence sharing regime satisfied the six minimum safeguards. The IC Code clearly described the nature of offences which could lead to intelligence being obtained; the limits on the duration of such obtaining; the process for examining, using and storing the intelligence obtained; and the circumstances in which the intelligence was to be erased or destroyed.

477. Finally, in the Government's view there was no good reason to single out intercepted communications and related communications data from other types of information that might in principle be obtained from a foreign intelligence service, such as intelligence from covert human intelligence sources, or covert audio/visual surveillance. Indeed, in many cases the intelligence services might not even know whether communications provided to them by a foreign intelligence service had been obtained as a result of interception.

(c) The third parties' submissions

(i) The Government of France

478. The French Government pointed out that intelligence sharing between partner services — either on an *ad hoc* or regular basis — was vitally important, especially in the fight against the increasingly transnational and diffusive threats which States had to prevent, primarily by identifying suspects before they acted. That fight justified the development of an intelligence community, without which intelligence services, with their limited ability to act overseas, would be unable to accomplish the task assigned to them.

479. The French Government further submitted that in the context of intelligence sharing the interference occurred not with the interception but rather with the obtaining of information, even if the material was intercepted at the behest of the receiving State. It noted the approach taken by the Chamber in analysing the United Kingdom intelligence sharing regime and invited the Grand Chamber to adopt the same approach.

480. In the Government's view, the reliability of the receiving service was one of the main criteria on which the sending State based its decision to exchange data, and as a consequence the receiving State had to guarantee the strict confidentiality of the information communicated to it. Therefore, the guarantees required for the handling of intelligence collected through an exchange of data with a partner service had to be in keeping with the 'third party rule', which prohibited an agency which had received information from a foreign partner from sharing it with a third party without the consent of the originator. Without such an assurance, States might refuse to transfer information.

(ii) The United Nations' Special Rapporteur on the promotion of the right to freedom of opinion and expression

481. The Special Rapporteur argued that the same standards should apply to the acquisition of data from foreign intelligence services as applied when the domestic authorities acquired data themselves. A contrary position could lead State authorities to *de facto* outsource surveillance operations circumventing the protections afforded in the ICCPR.

(iii) Access Now

482. Access Now contended that while Mutual Legal Assistance Treaties ('MLATs') offered a transparent and formal process for one State party to request intelligence from another, the operation of secret signals intelligence programmes (for example, the Five Eyes intelligence sharing network of which the United Kingdom, the United States of America, Australia, Canada and New Zealand were members) were not transparent and were prohibited by international human rights standards. Such secret programmes were not necessary, since the relevant intelligence could be obtained under MLATs.

(iv) Dutch Against Plasterk ('Burgers tegen Plasterk')

483. Dutch Against Plasterk, a coalition of five individuals and four associations, were applicants in a case against the Netherlands in which they sought to challenge the exchange of data between the Dutch authorities and their foreign intelligence partners (including the United States and the United Kingdom).

484. In their third party intervention before this Court, the coalition argued that the sharing of intelligence should only be permitted if it was accompanied by sufficient safeguards and the foreign authority had a sound legal basis for capturing the material. Otherwise, there could be a circumvention of the protection provided by Article 8 of the Convention. States should not be allowed to obtain material from foreign authorities that they could not lawfully capture themselves.

(v) Center for Democracy and Technology ('CDT') and Pen American Center ('PEN America')

485. CDT and PEN America argued that the circumstances of international cooperation in bulk data and communications surveillance required that at least three conditions were met: that States actively assessed and satisfied themselves as to the adequacy of their foreign partners' legal and administrative framework governing interception, and set out these adequacy measures in domestic law; that there was independent — preferably judicial — authorisation, based on a finding of reasonable suspicion, for the use of selectors identifiable to specific targets to query information obtained from foreign partners; and that there was a requirement of subsequent notification to the surveillance subjects.

486. CDT and PEN America submitted that the interception regimes operated by the NSA — most notably, under section 702 of FISA and Executive Order 12333 — would satisfy neither the 'in accordance with the law' nor the 'proportionality' requirements of Article 8 of the Convention, and these deficiencies tainted the lawfulness of the United Kingdom's intelligence sharing regime.

(vi) European Network of National Human Rights Institutions ('ENNHRI')

487. The ENNHRI provided examples from Contracting States which in their view showed that the nature of international intelligence sharing had changed significantly so that it had become difficult to distinguish between 'solicited' and 'unsolicited' data. Historically, international intelligence sharing had involved the transfer of evaluated data, or finished intelligence. However, the advent of new technology had resulted in the increasing exchange of unevaluated 'raw' data. Even where there was an agreement governing bilateral or multilateral intelligence co-operation the advent of automation and big data made it much more challenging to evaluate what one party received from another, including whether the information remained within the parameters of the original request. Consequently, there was a need for robust independent oversight of international intelligence sharing without distinction between solicited and unsolicited data. Oversight bodies should be legally mandated to oversee all matters of international cooperation by their intelligence services; cooperate with independent oversight bodies from the third States involved in the intelligence sharing; and hire independent specialists, with expertise in modern information and communications technology, where required.

(vii) Human Rights Watch ('HRW')

488. Although the present applications focused on the receipt of foreign intelligence from the United States, HRW believed that the network of States with which communications intelligence was shared was vastly larger. For example the 'Five Eyes Alliance' comprised the United Kingdom, the United States, Australia, Canada and New Zealand, and there were also thought to be other, more restricted intelligence sharing coalitions (for example, the 'Nine Eyes', adding Denmark, France, the Netherlands and Norway; the 'Fourteen Eyes', adding Germany, Belgium, Italy, Spain and Sweden; and the 'Forty-One Eyes', adding in others in the allied coalition in Afghanistan).

(viii) Open Society Justice Initiative ('OSJI')

489. OSJI argued that States should not receive or request data from a third party in a manner that circumvented individuals' Article 8 rights. To ensure that this did not happen, safeguards were required at the point when the material was first gathered, including prior scrutiny of the human rights record and interception laws and practices in the foreign State, and independent, preferably judicial, *a posteriori* oversight of any sharing arrangements to ensure that the safeguards were in place and enforced.

(ix) The Electronic Privacy Information Center ('EPIC')

490. EPIC submitted that United States' law authorised mass, indiscriminate surveillance of non-US persons. This surveillance took place pursuant to section 702 of FISA and Executive Order 12333. Surveillance under section 702 took place in the United States with the compelled assistance of service providers and it targeted non-US persons reasonably believed to be located outside the United States. There was no prior judicial review of surveillance activity; no reasonable suspicion was required; and there was no statutory obligation to notify subjects of surveillance. All that was required was that the FISC annually review the targeting and minimization procedures aimed at limiting the acquisition of the communications of US persons or persons located in the United States.

491. Executive Order 12333 authorised the NSA to acquire foreign intelligence and counterintelligence. The order provided broad authority to conduct signals intelligence surveillance from a wide variety of sources, including fibre optic networks. Collection occurred outside the territory of the United States. There were no reports or official disclosures concerning the scope of surveillance under the order, which was not subject to judicial oversight.

492. In EPIC's view, surveillance by the NSA would violate Article 8 of the Convention for failure to limit the scope of application and duration, and the failure to provide adequate supervision, notice and remedies.

(x) The International Commission of Jurists ('ICJ')

493. The ICJ referred the Court to Articles 15 and 16 of the Articles of State Responsibility of the International Law Commission ('the ILC Articles'). They contended that, pursuant to Article 15, a Contracting State could be responsible for mass surveillance conducted by a non-Contracting State if they

were acting in organised and structured forms of co-operation; and that, pursuant to Article 16, a Contracting State could be responsible for mass surveillance conducted by a non-Contracting State if it contributed to the surveillance programme and had actual or constructive knowledge of the breaches of international human rights obligations inherent in the system. The ICJ further submitted that Contracting States participating in or contributing to a mass surveillance programme were obliged to establish a system of safeguards for the protection of Article 8 rights, and were also under a duty to protect persons within their jurisdiction from violations of Article 8 rights caused by mass surveillance programmes.

(xi) The Law Society of England and Wales

494. The Law Society submitted that the section 8(4) regime and associated Codes provided no robust or transparent safeguards for legally privileged material. Since the same safeguards applied to privileged material obtained by foreign States and disclosed to the intelligence services of the United Kingdom, the same deficiencies also tainted that regime.

(d) The Court's assessment

(i) The applicable test

495. In the Chamber's view, the interception of communications by foreign intelligence services could not engage the responsibility of a receiving State, or fall within that State's jurisdiction within the meaning of Article 1 of the Convention, even if the interception was carried out at that State's request (see paragraph 420 of the Chamber judgment). First of all, in so far as some of the third parties had invoked the ILC Articles, the Chamber considered that these would only be relevant if the foreign intelligence services were placed at the disposal of the receiving State and were acting in exercise of elements of the governmental authority of that State (Article 6); if the receiving State aided or assisted the foreign intelligence services in intercepting the communications where that amounted to an internationally wrongful act for the State responsible for the services, the receiving State was aware of the circumstances of the internationally wrongful act, and the act would have been internationally wrongful if committed by the receiving State (Article 16); or if the receiving State exercised direction or control over the foreign Government (Article 17). Secondly, according to the Court's case-law the interception of communications by a foreign intelligence service could only fall within the receiving State's jurisdiction if that State was exercising authority or control over the foreign intelligence service (see, for example, *Al-Skeini and Others v. the United Kingdom* [GC], no. 55721/07, §§ 130–139, ECHR 2011 and *Jaloud v. the Netherlands* [GC], no. 47708/08, §§ 139 and 151 ECHR 2014).

496. The Grand Chamber agrees with the Chamber that none of these elements were present in the situation under consideration and, indeed, in their pleadings before the Grand Chamber the applicants have not suggested that they were. Therefore, any interference with Article 8 of the Convention could only lie in the initial request and the subsequent receipt of intercept material, followed by its subsequent storage, examination and use by the intelligence services of the receiving State.

497. The protection afforded by the Convention would be rendered nugatory if States could circumvent their Convention obligations by requesting either the interception of communications by, or the conveyance of intercepted communications from, non-Contracting States; or even, although not directly in issue in the cases at hand, by obtaining such communications through direct access to those States' databases. Therefore, in the Court's view, where a request is made to a non-contracting State for intercept material the request must have a basis in domestic law, and that law must be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov*, cited above, § 228). It will also be necessary to have clear detailed rules which give citizens an adequate indication of the circumstances in which and the conditions on which the authorities are empowered to make such a request (see *Roman Zakharov*, cited above, § 229; *Malone*, cited above, § 67; *Leander*, cited above, § 51; *Huvig*, cited above, § 29; *Kruslin*, cited above, § 30; *Valenzuela Contreras*, cited above, § 46; *Rotaru*, cited above, § 55; *Weber and Saravia*, cited above, § 93; and *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 75) and which provide effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the Convention.

498. Upon receipt of the intercept material, the Court considers that the receiving State must have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction. These safeguards, first developed by the Court in its case-law on the interception of communications by Contracting States, are equally applicable to the receipt, by a Contracting State, of solicited intercept material from a foreign intelligence service. If, as the Government contend, States do not always know whether material received from foreign intelligence services is the product of interception, then the Court considers that the same standards should apply to all material received from foreign intelligence services that could be the product of intercept.

499. Finally, the Court considers that any regime permitting the intelligence services to request either interception or intercept material from non-Contracting States, or to directly access such material, should be subject to independent supervision, and there should also be the possibility for independent *ex post facto* review.

(ii) Application of that test to the case at hand

500. The British-US Communication Intelligence Agreement of 5 March 1946 specifically permitted the exchange of material between the United States and the United Kingdom (see paragraph 103 above). However, details of the intelligence services' internal (or 'below the waterline') arrangements were only disclosed during the *Liberty* proceedings (see paragraphs 33–36 above). This new information was later incorporated into Chapter 12 of the IC Code (see paragraph 116 above) which, as already noted, was a public document, subject to the approval of both Houses of Parliament, and which had to be taken into account both by those exercising interception duties and by courts and tribunals (see paragraph 93–94 above). The Court has accepted that the provisions of the IC Code could be taken into consideration in assessing the foreseeability of the RIPA regime (see *Kennedy*, cited above, § 157 and paragraph 366 above) and the same must necessarily be true for the intelligence sharing regime.

501. Accordingly, the Court considers that the regime for requesting and receiving intelligence from non-Contracting States had a clear basis in domestic law and, following the amendment to the IC Code, that law was adequately accessible. As it undoubtedly pursued the legitimate aims of protecting national security, preventing disorder and crime and protecting the rights and freedoms of others, the Court will now — in line with its usual methodology (see paragraph 334 above) — assess, jointly, the foreseeability and necessity of the intelligence sharing regime.

502. Chapter 12 of the IC Code (see paragraph 116 above) follows the same approach as the one adopted by domestic legislation in respect of bulk interception. According to Chapter 12 the intelligence services could only make a request to a foreign government for unanalysed intercepted communications and/or associated communications data if a relevant interception warrant under RIPA had already been issued by the Secretary of State, the assistance of the foreign government was necessary to obtain the particular communications because they could not be obtained under the existing warrant (see paragraph 12.2 of the IC Code at paragraph 116 above), and it was necessary and proportionate for the intercepting agency to obtain those communications. For these purposes, a relevant RIPA interception warrant meant either a section 8(1) warrant in relation to the subject at issue; a section 8(4) warrant and an accompanying certificate which included one or more 'descriptions of intercepted material' covering the subject's communications; or, where the subject was known to be within the British Islands, a section 8(4) warrant and an accompanying certificate which included one or more 'descriptions of intercepted material' covering his or her communications, together with an appropriate section 16(3) modification.

503. Where exceptional circumstances existed, a request for communications could be made in the absence of a relevant RIPA interception warrant only if it did not amount to a deliberate circumvention of RIPA or otherwise frustrate its objectives (for example, because it was not technically feasible to obtain the communications via RIPA interception), and it was necessary and proportionate for the intercepting agency to obtain those communications. In such a case the request had to be considered and decided on by the Secretary of State personally, and, pursuant to the revised IC Code, notified to the IC Commissioner. According to information disclosed during the *Liberty* proceedings, and confirmed in the Government's submissions before both the Chamber and Grand Chamber, no request for intercept material had ever been made in the absence of an existing RIPA warrant (see paragraph 42 above).

504. In light of the foregoing, the Court considers that domestic law set down clear legal rules giving citizens an adequate indication of the circumstances in which and the conditions on which the authorities could request intercept material from a foreign State.

505. Where either a relevant section 8(1) or a section 8(4) warrant was already in place, that warrant would have been authorised by the Secretary of State. More specifically, it would appear from paragraph 12.5 of the IC Code, read together with the accompanying footnote, that where a request was based on an existing warrant that request would be made to, from or about specific selectors (that is, relating to a specific individual or individuals) and the Secretary of State would already have approved the request for the communications of those individuals. While, in exceptional circumstances, a request could be made in the absence of a relevant warrant, the Secretary of State personally had to approve the request and, if based on specific selectors, he or she personally had to consider and approve the examination of those communications by reference to such factors (see paragraph 116 above).

506. As the domestic legislation followed, with respect to such requests for intelligence sharing, the same approach as in bulk interception, and as national law explicitly provided that there should be no circumvention, there is no need for the Court to look separately at the authorisation procedure.

507. As for the safeguards for the examination, use, storage, onward transmission, erasure and destruction of the solicited intercept material, it was clear from paragraph 12.6 of the IC Code that intercepted content or related communications data obtained by the United Kingdom intelligence services from another State, which identified themselves as the product of intercept, had to be subject to the same internal rules and safeguards that applied to the same categories of content or data when they were obtained directly by the intercepting agencies as a result of interception under RIPA. Consequently, the safeguards in sections 15 and 16 of RIPA, as supplemented by the IC Code, applied equally to inter-

cepted communications and communications data obtained from foreign intelligence services, provided that the material 'identified itself as the product of intercept'.

508. The Court has examined the section 15 and section 16 safeguards in respect of the bulk interception regime and it was satisfied that the procedures for storing, accessing, examining and using the material obtained; for communicating the material to other parties; and for the erasure and destruction of the material obtained were sufficiently clear and afforded adequate protection against abuse (see paragraphs 384–405 above). In light of the Court's findings at paragraph 498 above, it notes that paragraph 12.6 of the IC does not extend the safeguards in sections 15 and 16 of RIPA, as supplemented by the IC Code, to all material received from foreign intelligence services that could be the product of intercept, limiting these safeguards only to material that identified itself as such; however, the Court does not consider this fact alone to be fatal to the Article 8 compliance of the intelligence sharing regime.

509. In the context of the section 8(4) regime, the Court had concerns about the exemption of related communications data from the section 16 safeguard. However, under the section 8(4) regime the State was able to intercept, store and search all packets of communications travelling across certain bearers. The blanket exemption of related communications data from the section 16 safeguard therefore meant that all of these data, regardless of whether they were of any intelligence interest, could be searched by the intelligence services apparently without restriction. Under Chapter 12 of the IC Code, on the other hand, content and related communications data were not requested by the intelligence services in bulk. Paragraph 12.5 of the IC Code, together with its accompanying footnote, indicated that where a request was based on an existing warrant that request would be made to, from or about specific selectors (that is, specified individuals) and the Secretary of State would already have approved the request for the communications of those individuals. While in exceptional circumstances a request could be made in the absence of a warrant, the Secretary of State personally had to approve the request and, if based on specific selectors, he or she personally had to consider and approve the examination of those communications by reference to such factors. If the request was not for specific selectors, any communications subsequently obtained could not be examined according to a factor referable to a person known to be in the British Islands unless the Secretary of State had approved the examination of those communications (see paragraph 116 above). In other words, the intelligence services either requested intelligence relating to an individual for whom the Secretary of State had already considered the necessity and proportionality of obtaining his or her communications; or the section 16 safeguard was applicable to the material obtained. As no request has yet been made without a warrant, it would seem that, to date, all requests have fallen into the first category.

510. Therefore, the Court considers that the United Kingdom had in place adequate safeguards for the examination, use and storage of the content and communications data received from intelligence partners; for the onward transmission of this material; and for its erasure and destruction.

511. Finally, the Court observes that a further layer of protection was provided by the IC Commissioner and the IPT (see paragraph 41 above). The IC Commissioner had oversight of the intelligence sharing regime: paragraph 12.7 of the IC Code (see paragraph 116 above) required him to be notified of all requests made in the absence of a warrant, and he already supervised the granting of warrants and the storage of material by the intelligence services.

512. In addition to the oversight of the IC Commissioner, the IPT provided *ex post facto* review of the intelligence sharing regime. As can be seen from the *Liberty* proceedings, it was open to anyone wishing to make either a specific or general complaint about the intelligence sharing regime to complain to the IPT; and, in response, the IPT was able to examine both the 'above the waterline' and 'below the waterline' arrangements in order to assess the Convention compliance of the regime.

513. Consequently, the Court considers that the regime for requesting and receiving intercept material was compatible with Article 8 of the Convention. There existed clear detailed rules which gave citizens an adequate indication of the circumstances in which and the conditions on which the authorities were empowered to make a request to a foreign intelligence service; domestic law contained effective guarantees against the use of such requests to circumvent domestic law and/or the United Kingdom's obligations under the Convention; the United Kingdom had in place adequate safeguards for the examination, use, storage, onward transmission, erasure and destruction of the material; and the regime was subject to independent oversight by the IC Commissioner and there was a possibility for *ex post facto* review by the IPT.

514. Accordingly, there has been no violation of Article 8 of the Convention.

B. Article 10 of the Convention

515. The applicants in the third of the joined cases also complained that the intelligence sharing regime had breached their rights under Article 10 of the Convention. In so far as that complaint related to their activities as NGOs, the Chamber declared it inadmissible for non-exhaustion of domestic remedies as the applicants had raised it too late in the domestic proceedings for it to be considered (see paragraph 473 of the Chamber judgment). This aspect of the complaint is therefore outwith the scope of the Grand Chamber's examination.

516. The applicants in the third of the joined cases also complained more generally about the Ar-

ticle 10 compliance of the intelligence sharing regime. Although this argument was raised before the IPT in good time, the Court would agree with the Chamber that it gives rise to no separate issue over and above that arising out of Article 8 of the Convention (see paragraph 474 of the Chamber judgment). It therefore considers that there has also been no violation of Article 10 of the Convention.

IV. Acquisition of communications data from communications service providers

A. Article 8 of the Convention

517. The applicants in the second of the joined cases complained that the regime for the acquisition of communications data under Chapter II of RIPA was incompatible with their rights under Article 8 of the Convention.

1. The Chamber judgment

518. At the date of the Chamber's examination of the case the Government of the United Kingdom was in the process of replacing the existing legal framework for conducting secret surveillance with the new IPA. The provisions in the new legislation governing the retention of communications data by CSPs were subject to a domestic legal challenge by Liberty. In the course of those proceedings, the Government conceded that the relevant provision was inconsistent with the requirements of EU law. Consequently, the High Court found Part 4 to be incompatible with fundamental rights in EU law since, in the area of criminal justice, access to retained data was not limited to the purpose of combating 'serious crime'; nor was it subject to prior review by a court or an independent administrative body (see paragraph 190 above).

519. In view of both the primacy of EU law over United Kingdom law, and the Government's concession in the domestic proceedings that the provisions of IPA governing the retention of communications data by CSPs was incompatible with EU law, the Chamber considered it 'clear' that domestic law required that any regime permitting the authorities to access data retained by CSPs should limit access to the purpose of combating 'serious crime', and that access should be subject to prior review by a court or independent administrative body. As the predecessor regime suffered from the same 'flaws' as its successor, the Chamber found that it could not be in accordance with the law within the meaning of Article 8 of the Convention (see paragraphs 465–468 of the Chamber judgment).

2. The parties' submissions

520. The parties made no further submissions before the Grand Chamber in respect of this complaint.

3. The Court's assessment

521. The Government did not contest the Chamber's findings before the Grand Chamber. Furthermore, the latter finds no ground on which to disagree with the Chamber's conclusions.

522. Accordingly, the Court considers that in the present case there was a violation of Article 8 of the Convention on account of the fact that the operation of the regime under Chapter II of RIPA was not 'in accordance with the law'.

B. Article 10 of the Convention

523. The applicants in the second of the joined cases also complained under Article 10 of the Convention about the regime for the acquisition of communications data from CSPs.

1. The Chamber judgment

524. The Chamber acknowledged that the Chapter II regime afforded enhanced protection where data were sought for the purpose of identifying a journalist's source. In particular, paragraph 3.77 of the Acquisition of Communications Data Code of Practice provided that where an application was intended to determine the source of journalistic information, there had to be an overriding requirement in the public interest, and such applications had to use the procedures of the Police and Criminal Evidence Act 1984 ('PACE') to apply to a court for a production order to obtain these data. Pursuant to Schedule 1 to PACE, an application for a production order was made to a judge and, where the application related to material that consisted of or included journalistic material, the application had to be made *inter partes*. Internal authorisation could only be used if there was believed to be an immediate threat of loss of human life, and that person's life could be endangered by the delay inherent in the process of judicial authorisation (see paragraph 498 of the Chamber judgment).

525. Nevertheless, these provisions only applied where the purpose of the application was to determine a source; they did not apply in every case where there was a request for the communications data of a journalist, or where such collateral intrusion was likely. Furthermore, in cases concerning access to a journalist's communications data there were no special provisions restricting access to the purpose of combating 'serious crime'. Consequently, the Chamber considered that the regime was not 'in accordance with the law' for the purpose of the Article 10 complaint (see paragraphs 496–499 of the Chamber judgment).

2. The parties' submissions

526. The parties made no further submissions before the Grand Chamber in respect of this complaint.

3. The Court's assessment

527. The Government did not contest the Chamber's findings before the Grand Chamber. Furthermore, the latter finds no ground on which to disagree with the Chamber's conclusions.

528. Accordingly, the Court considers that in the present case there has also been a violation of Article 10 of the Convention on account of the fact that the operation of the regime under Chapter II of RIPA was not 'in accordance with the law'.

V. Application of Article 41 of the Convention

529. Article 41 of the Convention provides:

'If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party.'

A. Damage

530. The applicants did not submit any claim in respect of pecuniary or non-pecuniary damage. Accordingly, the Court considers that there is no call to award them any sum on that account.

B. Costs and expenses

Enz. (*red.*)

For these reasons, the Court

1. *Holds*, unanimously, that there has been a violation of Article 8 of the Convention in respect of the section 8(4) regime;
2. *Holds,* unanimously, that there has been a violation of Article 8 of the Convention in respect of the Chapter II regime;
3. *Holds*, by twelve votes to five, that there has been no violation of Article 8 of the Convention in respect of the receipt of intelligence from foreign intelligence services;
4. *Holds,* unanimously, that, in so far as it was raised by the applicants in the second of the joined cases, there has been a violation of Article 10 of the Convention in respect of the section 8(4) regime and the Chapter II regime.
5. *Holds*, by twelve votes to five, that there has been no violation of Article 10 of the Convention in respect of the receipt of intelligence from foreign intelligence services;
6. *Holds*, unanimously,

(a) that the respondent State is to pay the applicants, within three months, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
(i) to the applicants in the first of the joined cases: € 227,500 (two hundred and twenty-seven thousand five hundred euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;
(ii) to the applicants in the second of the joined cases: € 90,000 (ninety thousand euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;
(iii) to the applicants in the third of the joined cases: € 36,000 (thirty-six thousand euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;
(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;
7. *Dismisses*, unanimously, the remainder of the applicants' claim for just satisfaction.

Done in English and in French, and delivered at a hearing on 25 May 2021, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Søren Prebensen
Deputy to the Registrar
Robert Spano
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:
(a) Joint partly concurring opinion of Judges Lemmens, Vehabović and Bošnjak;
(b) Partly concurring and partly dissenting opinion of Judge Pinto de Albuquerque [niet opgenomen; *red.*];
(c) Joint partly dissenting opinion of Judges Lemmens, Vehabović, Ranzoni and Bošnjak [niet opgenomen; *red.*].

R.S.O.
S.C.P.

Joint partly concurring opinion of Judges Lemmens, Vehabović and Bošnjak

1. In the present case, we agree with the majority on all counts in the operative part of the judgment, except for operative points 3 (no violation of Article 8 of the Convention in respect of the receipt of intelligence from foreign intelligence services) and 5 (no violation of Article 10 of the Convention in respect of the receipt of intelligence from foreign intelligence services). To show where we disagree with the outcome of the case, we are submitting a dissenting opinion jointly with our colleague Judge Ranzoni. In addition, we are submitting this concurring opinion to underline that while the present judgment as a whole is elegantly structured and largely clear in its message, it has also missed an excellent opportunity to fully uphold the importance of private life and correspondence when faced with interference in the form of mass surveillance.

I. Introductory remarks

2. This case is about a balancing exercise in which legitimate interests pursued by the Contracting States have to be weighed against human rights and fundamental freedoms, notably those protected by Article 8 of the Convention. At the start of its assessment (paragraphs 322 and 323 of the judgment), the Grand Chamber extensively describes the nature of the modern threats facing the Contracting States and recognises how valuable bulk interception can be in identifying and preventing

those threats. Furthermore, the judgment underlines a need for secrecy of operations in this domain which it considers to be legitimate, meaning that little if any information about a given scheme will be available to the public. While one may subscribe, to a certain extent, to this description of the legitimate interest in operating a bulk interception regime, there is no similar emphasis on the importance of privacy or any other private interest in those same preliminary remarks. Although this has no direct bearing upon the assessment of the bulk interception system under scrutiny, we would have preferred a more balanced introduction to this assessment.

3. Before embarking on an analysis of what we consider to be the weak points of the present judgment, it is worthwhile remembering that privacy is a fundamental precondition for a variety of fundamental individual interests, but also for the existence of a democratic society. It is essential for a person's well-being, autonomy, self-development, and ability to enter into meaningful relationships with other persons. It is also a necessary precondition for the enjoyment of civil rights and consequently for a person's status as a free and equal member of a democratic society. Encroachments on privacy do not merely diminish individual autonomy and mental and physical health, they also inhibit democratic self-governance.

4. First, privacy is important for a person's mental and physical health. The mere feeling that one is constantly being observed and evaluated by others can have serious effects on one's mental and physical well-being. It makes individuals internalise too much of their social behaviour, so that they feel guilty or ashamed because of any feelings or thoughts, desires or practices that they would not want to express publicly. Such tensions between the demands of their inner life and the pressures of self-presentation can lead to serious health problems.

5. Second, external observation and the pressures on self-presentation may obstruct 'the promotion of liberty, autonomy, selfhood, human relations, and furthering the existence of a free society'[3]. Surveillance is inhibiting because it diminishes the extent to which we can spontaneously and wholeheartedly relate to other people and engage in certain activities. A lack of privacy would have a stifling effect on our inner life, our relationships and ultimately our autonomy. 'Thus will be lost … the inner personal core that is the source of criticism of convention, of creativity, rebellion and renewal'[4].

6. Third, privacy is essential for democratic self-governance. Mass surveillance exerts internal and external pressures to conform, making individuals submissive and deferential. In order to avoid outright oppression and give itself the varnish of legitimacy, there is an inherent danger that the State will utilise surveillance to ensure compliance and conformism. As George Orwell described in the novel *Nineteen Eighty-Four*:

> 'There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live — did live, from habit that became instinct — in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.'[5]

7. In securing a realm for unobserved activity, privacy fosters and encourages the moral autonomy of citizens, a central requirement of self-governance in democracies[6]. Only autonomous beings can truly govern themselves and only autonomous beings can truly enjoy all the civil rights, such as the right to vote, freedom of association and participation in civil society, the freedoms of thought and conscience, speech and expression, and freedom of religion, that are essential for self-governance. We cannot be said to fully enjoy the freedoms that these rights are supposed to afford us if our inner freedom is compromised.

8. But surveillance does not merely exert internal pressures on freedom. To the extent that citizens retain their autonomy, it also exerts external pressures on their freedom to exercise their civil rights. Just as living under constant social control makes us less likely to act according to our feelings and thoughts for fear of ostracism, living under constant government surveillance can make citizens just a little more cautious when engaging with their political convictions, a little less likely to freely associate, a little less likely to speak freely, a little less likely to dissent, a little less likely to run for public office. The aggregate effect of often merely marginal inhibitions can stifle what was once a free society, especially as people grow up in an environment of increased conformism and moral cowardice. US Supreme Court Justice William O. Douglas, writing the dissent in *Osborn v. United States*, impressionably describes as follows the threat that mass surveillance poses to our democratic freedoms:

> '… The time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that his most secret thoughts are no longer his own, but belong to the Government; when the most confidential and intimate conversations are always open to eager, prying ears. When that time

3 Ruth Gavison (1980), 'Privacy and the Limits of Law', *Yale Law Journal* 89, p. 347.

4 Jeffrey Reiman (1995), 'Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Technology of the Future', *Santa Clara High Technology Law Journal* 11:1, p. 42.

5 George Orwell (2008), *Nineteen Eighty-Four* (London: Penguin), pp. 4–5.

6 Daniel Solove (2008), *Understanding Privacy* (Cambridge, MA: Harvard University Press), p. 98.

> comes, privacy, and with it liberty, will be gone. If a man's privacy can be invaded at will, who can say he is free? If his every word is taken down and evaluated, or if he is afraid every word may be, who can say he enjoys freedom of speech? If his every association is known and recorded, if the conversations with his associates are purloined, who can say he enjoys freedom of association? When such conditions obtain, our citizens will be afraid to utter any but the safest and most orthodox thoughts; afraid to associate with any but the most acceptable people. Freedom as the Constitution envisages it will have vanished.'[7]

9. To conclude, the development of new technologies enabling mass surveillance and more effective use of the information collected has increased threats to privacy as well as the risk of abuse of personal data. It is not our intention to assert that these threats and risks have already materialised on a large scale or have brought about the consequences discussed above. However, one should be properly aware of their existence when designing a system capable of preventing, detecting and sanctioning any abuse that might occur.

10. In our opinion, these considerations should have led the Court to attach significantly more weight to private life in general, and to confidentiality of correspondence in particular, when weighing them in the balance against the legitimate interests of the respondent State in operating its bulk interception scheme. Consequently, the Grand Chamber should have (a) accurately identified and attached proper weight to interferences with private life and correspondence; (b) introduced clear minimum safeguards capable of protecting individuals against arbitrary or excessive interference; and consequently (c) assessed the impugned bulk interception scheme in a stricter manner.

II. Interferences with private life and correspondence

11. In paragraph 325 of the judgment, the majority describe the stages of the bulk interception system. They consider that the initial stage, described as the interception and initial retention of communications and related communications data, followed by the immediate discarding of parts of the communications, 'does not constitute a particularly significant interference' (paragraph 330 of the judgment). We respectfully disagree. It is our belief that at this stage already, the interference is significant. First, by interception and initial retention, all communications of any individual flowing through selected bearers and all related communications data come into the hands of State authorities. Secondly, while it is true that at this stage, the content of those communications has not yet been analysed or brought to the attention of decision makers and thus cannot yet lead to any action being taken against a particular individual, the first stage is a *sine qua non* for any further stage. The exact extent of the communications and related data thereby gathered by the intelligence services is unknown. But there are reasons to believe that, on a regular basis, a large part of the communications of millions of individuals is intercepted. This situation is aggravated by the fact that the individuals concerned will, as a rule, not be aware of this interference. In such a situation, when people cannot know whether their communications are being targeted, but are aware that there exists a strong probability that this is happening, a third element of interference arises: people may adapt their behaviour, with many a serious consequence, as described above in paragraphs 3–8 of this separate opinion.

12. According to paragraph 330 of the judgment, parts of intercepted communications are discarded immediately. The Court is not in possession of any information as to how this 'discarding' is performed. One may reasonably assume that it is not conducted randomly without any internal logic and that in this exercise, intelligence services apply certain criteria which separate rubbish from possibly useful material. The very fact that this act is performed in obscurity and on an unknown basis should, in our opinion, be a matter of serious concern. Such 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. Yet the majority fail to address this particular step in the bulk interception process in any way. We consider this to be an important shortcoming of the judgment.

III. Minimum safeguards protecting individuals against arbitrary or excessive interference

13. In paragraph 335, the judgment outlines the Court's case-law on six minimum requirements that should be set out in domestic law in order to avoid abuses of power in cases of interception of communications for the purposes of criminal investigation. It further explains that, in *Roman Zakharov v. Russia* ([GC], no. 47143/06, ECHR 2015), the Court held that the same six minimum safeguards also applied in cases where the interception was performed for reasons of national security. In the next step, the Grand Chamber identifies a need to develop and adapt these requirements to the specificities of bulk interception and, finally, outlines a list of eight criteria which the domestic legal framework must clearly define in order to comply with Article 8 of the Convention (paragraph 361 of the judgment).

14. That list is very well supported by arguments and can certainly serve as protection against arbitrariness and abuse. However, the criteria included in this list:

(a) do not clearly serve as self-standing minimum standards, as any lack of compliance with any of

7 *Osborn v. United States*, 385 U.S. 323 (1966).

those standards appears to be 'reparable' in the process of a global assessment;
(b) require clear definition of particular safeguards in domestic law, but do not set any minimum safeguards themselves; and
(c) do not provide for any clear substantive protection of an individual against disproportionate interference, in particular at the stage of application of strong selectors to the material gathered, and the procedural protection provided by these criteria is also insufficient.

15. As to (a), we would like to turn the reader's attention to paragraph 360 of the judgment, announcing a need for a global assessment of a particular bulk interception regime. While this may sound appealing, it necessarily erodes the importance of each safeguard. By contrast, we believe that each safeguard labelled as a minimum one can never be offset by any counterbalancing factors provided in respect of some other criterion. In other words, lack of compliance with a safeguard which is considered to be a minimum one should automatically lead to a finding of a violation of Article 8 of the Convention, regardless of whether a global assessment might reveal a more positive picture. Regrettably, the majority do not appear to have opted for such an approach. We would add that an approach setting minimum standards as absolute limits, as thick red lines that may not be crossed, would provide for a stricter and more foreseeable protection, which is of utmost importance in a field where the action of the State authorities is conducted with a high level of secrecy, as a result of which, in the words of the present judgment (see paragraph 322), little if any information about the operation of the scheme is available and such information as is available may be couched in terminology which is obscure.

16. In respect of (b), the majority state that the eight criteria outlined in paragraph 361 need to be clearly defined in the domestic legal framework. While this is a requirement to be welcomed, in particular from the point of view of foreseeability of the law, these criteria in themselves do not lay down minimum requirements in respect of the substantive or procedural conditions that need to be complied with in order to operate the bulk interception regime and to pass from its initial stage to the more intrusive ones. This flaw is partly remedied by the fact that certain (but not all) of those elements discussed in paragraphs 348–360 of the judgment are set out not only in descriptive passages referring to the existing case-law but also in prescriptive wording laying down certain requirements, particularly in respect of the authorisation of bulk interception in its specific stages. However, we argue that the requirements set by the majority do not go far enough in protecting an individual against arbitrary, excessive or abusive interferences with his or her private life and correspondence.

17. This brings us to our point (c). In the context of targeted interception, mostly for purposes of detecting and investigating criminal activity, the Court has referred to certain substantive safeguards against abuse. Thus, the Court has required that the nature of the offences which may give rise to an interception order be defined together with the categories of people liable to have their communications intercepted. Furthermore, on numerous occasions, the Court has had recourse to the requirement of reasonable suspicion. The majority simply consider that these safeguards are not readily applicable to bulk interception. While we can agree that they cannot be directly transposable, there remains a need for robust substantive protection to be developed, whereby safeguards developed in the framework of targeted interception for the purpose of combatting crime can serve as an excellent source of inspiration, as we will seek to explain below.

18. First, in contrast to targeted interception in crime prevention, bulk interception is largely used for purposes of national security. It is difficult to see why one should not expect the domestic legislation to clearly define the possible national security threats and the circumstances in which those threats may trigger bulk interception.

19. In respect of the second substantive requirement attached to targeted interception, namely the definition of categories of people liable to have their communications intercepted, one can acknowledge that a similar requirement would make little sense in the first stage of bulk interception, when all communications running through certain bearers are intercepted indiscriminately. Yet the breadth of the interference should not be an excuse for abandoning a particular safeguard. Additionally, at later stages of bulk interception, particularly when strong selectors are applied for the purpose of singling out and analysing the communications of an identified individual, the situation becomes largely comparable to that of targeted interception. Expecting the legal framework to define the categories of people that can be targeted by the application of strong selectors would not be an excessive, but rather a fully appropriate, requirement.

20. Third, the requirement of reasonable suspicion is an important protection against arbitrary and disproportionate interferences with several Convention rights. It refers to the probability that a criminal offence giving rise to an interference has been committed or is about to be committed. While bulk interception should not be used in crime investigation, but rather confined to national security purposes, we believe that a standard similar to reasonable suspicion should pertain to the grounds on which bulk interception may be authorised. This is particularly true when bulk interception starts targeting an identified individual through the application of strong selectors. To be clear, we consider that in a democratic society intelligence services may only inspect communications and related communication data of an individual once they can demonstrate to an objective observer that that individual may be engaged or is about to engage in activities

infringing a specific national security interest, or is a person who is or may be in contact with individuals engaged in, or about to engage, in such activities. No such or similar requirement has been introduced by the majority in the present judgment.

21. Instead of these three safeguards, the majority have set an overly broad substantive requirement, namely that the grounds on which bulk interception may be authorised and the circumstances in which an individual's communications may be intercepted must be clearly defined in the domestic legal framework. Unfortunately, the reference to 'grounds' and 'circumstances' is rather vague, particularly in the absence of any reference to what such grounds and circumstances may or may not be. Furthermore, according to the language used in paragraph 361 of the judgment, the specific requirement relating to the grounds only applies to the stage of authorisation of bulk interception and not to any subsequent stage, thereby giving no indication as to whether any substantive requirement is attached, for example, to the application of strong selectors targeting the communications of an identified individual.

22. The lack of appropriate substantive protection has an important bearing upon the effectiveness of procedural protection. The main element of procedural protection is the requirement of prior authorisation, which the present judgment introduces both at the first stage of bulk interception and before the application of strong selectors. The crucial point of any prior authorisation is to verify whether the envisaged interference complies with the substantive criteria for such an interference. However, if the substantive criteria are vague, overly broad or even non-existent, the requirement of prior authorisation will necessarily fail to provide for sufficiently effective protection against arbitrariness and abuse.

23. In respect of the prior authorisation requirement, the judgment requires such authorisation to be exercised at the initial stage by a body that is independent from the executive. We can agree. However, we respectfully but strongly disagree that it suffices for the application of strong selectors relating to identifiable individuals to be subjected to a prior *internal* authorisation alone. Instead, we argue that at this stage, prior judicial control would be needed. While the existing case-law of the Court does not necessarily require judicial authorisation for targeted interception of communications of individuals, we believe that there are reasons for a reinforced standard of protection in cases of application of strong selectors in bulk interception. These reasons are as follows:

(a) Bulk interception, in contrast to targeted interception, is not limited to a specific category of people, and thus a much larger pool of communications is liable to be examined than in a case of targeted communications.

(b) Furthermore, a strong selector pertaining to an identified individual can, when applied, open the door to a much larger number of communications, namely wherever that specific individual is referred to, even if he or she has not engaged in those communications (as opposed to communicating over the communication means that he or she personally uses).

(c) In targeted interception for the purposes of law enforcement, a form of judicial control will usually occur somewhere down the line. For example, when evidence is obtained by targeted interception, it will be submitted in subsequent criminal proceedings, such that a court conducting those proceedings will be able to verify whether the targeted interception in that case complied with legal requirements. No such subsequent judicial control will normally occur in cases of bulk interception coupled with the application of strong selectors.

24. In stark contrast with this view, the majority consider that prior internal authorisation is sufficient. In our opinion, internal authorisation cannot provide for a level of protection against arbitrariness and abuse comparable to the protection offered by independent scrutiny. In particular, it is hard to imagine how a person having an organisational and, possibly, collegial connection with the requesting authority could properly assess a request in a fair and disinterested manner. It is probable that authorisation requirements will not be fully respected and, thus, the very purpose of this safeguard will not be met. This is even more likely in those High Contracting Parties where no long-standing tradition of democratic oversight of intelligence services exists.

25. We note that the Governments of the United Kingdom and the Netherlands have submitted that any requirement to explain or substantiate selectors or search criteria would seriously restrict the effectiveness of bulk interception (paragraph 353 of the judgment) and that the majority show some sympathy for this argument (paragraph 354 of the judgment). We cannot subscribe to this argument. We believe that in a democratic society, communications and related communications data of an identified individual may not be singled out and examined without that individual's consent unless very convincing reasons exist to do so. If an intelligence service or other authority is not able to articulate such reasons and demonstrate them before an independent institution, this should simply mean that it ought not to have any access to such communications. We acknowledge that occasionally a situation may arise where the regular authorisation process is too cumbersome to effectively neutralise a threat to national security, and that other solutions should be provided in this respect. However, if a robust authorisation system designed to properly protect human rights is perceived as an unnecessary hurdle, democratic society should be put on notice.

IV. Assessment of the bulk interception regime at hand

26. We agree with the other members of the Grand Chamber in their findings in points 1, 2 and 4

of the operative part of the judgment. That said, we believe that the assessment of certain features of the impugned regime does not go far enough and fails to properly identify some of its shortcomings.

27. As an example, we wish to direct the reader's attention to the grounds on which bulk interception could be authorised under the UK system (paragraphs 368–371 of the judgment). A bulk interception warrant could be issued if this was necessary (a) in the interests of national security; (b) for the purpose of preventing or detecting serious crime; or (c) for the purpose of safeguarding the economic well-being of the United Kingdom in so far as those interests were also relevant to the interests of national security.

28. The purposes under (a) and (c) both made reference to interests of national security. It appears that neither national security nor its interests were anywhere defined. While we take note of the judgment's reference to the IC Commissioner's clarification of how practice perceived the term 'national security' (paragraph 369 of the judgment), we argue that this clarification remained insufficient from the point of view of the foreseeability requirement. Furthermore, we have doubts as to whether the IC Commissioner's clarification can be assimilated to well established case-law which, according to the Court's jurisprudence, may compensate for vagueness in legislation. As a consequence of the absence of a clear definition, an individual could not be sure, even with the help of qualified advice, on what exact grounds his or her communications were liable to be intercepted and analysed by the intelligence services.

29. The purpose under (b) did not have the above-mentioned flaws of the purposes under (a) and (c). Serious crime was defined as an offence for which the perpetrator (assuming he or she was over the age of twenty-one and had no previous convictions) could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or where the conduct involved the use of violence, resulted in substantial financial gain or was conducted by a large number of persons in pursuit of a common purpose (see paragraph 369 of the judgment). 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.[8] The explanation of the respondent Government, namely that information obtained by bulk interception could not be used in the prosecution of a criminal offence, is in our opinion unconvincing. It appears that on the basis of the information thus obtained, law enforcement agencies could act, for example, by proceeding to conduct investigative measures or even arrests, this in turn producing evidence for the purpose of prosecution. It is likely that in a not so distant future, by exploring this particular ground, crime investigation might move from targeted surveillance to bulk interception of data.

V. Conclusion

30. 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. The Grand Chamber has partly seized the opportunity and outlined a comprehensive set of principles which are aimed at protecting human rights and fundamental freedoms, notably those enshrined in Articles 8 and 10 of the Convention. However, for the reasons explained in this separate opinion, in performing the balancing exercise, the majority have failed to assign proper weight to private life and correspondence, which in several respects remain insufficiently protected in the face of interference by bulk interception. One may hope that in future cases raising questions of concrete interference with the rights of specific individuals, the Court will interpret and further develop the principles in a way which will properly uphold democratic society and the values it stands for.

8 See, e.g., Recommendation 1402 (1999) of the Parliamentary Assembly of the Council of Europe on the control of internal security services in Council of Europe member states, in particular Guideline A (ii). This Recommendation addresses activities of internal security services, but we see it as perfectly applicable to foreign intelligence also.

Noot

Zie noot onder *NJ* 2021/362.

E.J. Dommering

NJ 2021/362

HOF VAN JUSTITIE VAN DE EUROPESE UNIE
6 oktober 2020, nr. C-511/18, nr. C-512/18, nr. C-520/18
(K. Lenaerts, R. Silva de Lapuerta, J.-C. Bonichot, A. Arabadjiev, A. Prechal, M. Safjan, P.G. Xuereb, L.S. Rossi, J. Malenovský, L. Bay Larsen, T. von Danwitz, C. Toader, K. Jürimäe, C. Lycourgos, N. Piçarra; A-G M. Campos Sánchez-Bordona)
m.nt. E.J. Dommering

Art. 1 lid 3, art. 3, 5, 15 lid 1 Richtlijn 2002/58; art. 4, 6 t/m 8, 11, 52 lid 1 Handvest van de grondrechten van de Europese Unie; art. 4 lid 2 VEU; art. 23 lid 1 Verordening 2016/679; Richtlijn 2000/31

RvdW 2021/387
Computerrecht 2021/62
ECLI:EU:C:2020:7
ECLI:EU:C:2020:791
ECLI:EU:C:2020:6

Verzoeken om een prejudiciële beslissing ingediend door de Conseil d'État (hoogste bestuursrechter, Frankrijk) bij beslissingen van 26 juli 2018 (C-511/18 en C-512/18), en door het Grond-

wettelijk Hof (België) bij beslissing van 19 juli 2018 (C-520/18).

Verwerking van persoonsgegevens in de sector elektronische communicatie. Aanbieders van elektronische communicatiediensten. Aanbieders van opslagdiensten en aanbieders van toegang tot het internet. Algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. Geautomatiseerde analyse van de gegevens. Toegang in real time tot de gegevens. Bescherming van de nationale veiligheid en bestrijding van terrorisme. Bestrijding van criminaliteit. Vertrouwelijk karakter van elektronische communicatie. Bescherming.

1) Artikel 15, lid 1, van Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), zoals gewijzigd bij Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie, moet aldus worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in die bepaling genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. Artikel 15, lid 1, van Richtlijn 2002/58, zoals gewijzigd bij Richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, verzet zich daarentegen niet tegen wettelijke maatregelen

- die het mogelijk maken om ten behoeve van de bescherming van de nationale veiligheid van aanbieders van elektronischecommunicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;

- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;

- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;

- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen, en

- die het mogelijk maken om ten behoeve van de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode,

mits die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik.

2) Artikel 15, lid 1, van Richtlijn 2002/58, zoals gewijzigd bij Richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, moet aldus worden uitgelegd dat het zich niet verzet tegen een nationale regeling die aanbieders van elektronischecommunicatiediensten verplicht om, ten eerste, met name verkeers- en locatiegegevens op geautomatiseerde wijze te analyseren en in real time op te vragen, en, ten tweede, technische gegevens over de locatie van de gebruikte eindapparatuur in real time op te vragen, wanneer

- die geautomatiseerde analyse beperkt is tot situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en de toepassing van die analyse effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of er sprake is van een situatie die de genoemde maatregel rechtvaardigt en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer

- het in real time opvragen van verkeers- en locatiegegevens beperkt is tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten, en is onderworpen aan voorafgaande toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, om ervoor te zorgen dat een dergelijke maatregel slechts wordt toegestaan binnen de grenzen van het

strikt noodzakelijke. In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden.
3) Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('richtlijn inzake elektronische handel') moet aldus worden uitgelegd dat zij niet van toepassing is op de bescherming van het vertrouwelijke karakter van communicatie en van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de diensten van de informatiemaatschappij. Deze bescherming wordt, naargelang van het geval, beheerst door Richtlijn 2002/58, zoals gewijzigd bij Richtlijn 2009/136, of door Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming). Artikel 23, lid 1, van Verordening 2016/679, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd.
4) Een nationale rechterlijke instantie mag geen bepaling van haar nationale recht toepassen die haar machtigt om de werking in de tijd te beperken van de door haar op grond van dit recht uit te spreken onwettigverklaring van een nationale wettelijke regeling waarbij ten behoeve van met name de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die onverenigbaar is met artikel 15, lid 1, van Richtlijn 2002/58, zoals gewijzigd bij Richtlijn 2009/136, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten. Op grond van artikel 15, lid 1, uitgelegd in het licht van het doeltreffendheidsbeginsel, dient de nationale strafrechter informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten.

La Quadrature du Net (C-511/18 en C-512/18), French Data Network (C-511/18 en C-512/18), Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 en C- 512/18) en Igwan.net (C-511/18), Ordre des barreaux francophones et germanophone (C-520/18), Académie Fiscale ASBL (C-520/18), Liga voor Mensenrechten VZW (C-520/18), Ligue des Droits de l'Homme ASBL e.a (C-520/18)
tegen
Premier ministre (C-511/18 en C-512/18), Garde des Sceaux, ministre de la Justice (C-511/18 en C-512/18), Ministre de l'Intérieur (C-511/18), Ministre des Armées (C-511/18) en Ministerraad (C-520/18)

Hof van Justitie EU:

Arrest

1 De verzoeken om een prejudiciële beslissing betreffen de uitlegging van artikel 15, lid 1, van richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (*PB* 2002, L 201, blz. 37), zoals gewijzigd bij richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 (*PB* 2009, L 337, blz. 11) (hierna: 'richtlijn 2002/58'), en van de artikelen 12 tot en met 15 van richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('richtlijn inzake elektronische handel') (*PB* 2000, L 178, blz. 1), gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 4, 6 tot en met 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie (hierna: 'Handvest').
2 Het verzoek in zaak C-511/18 is ingediend in het kader van gedingen tussen La Quadrature du Net, French Data Network, de Fédération des fournisseurs d'accès à Internet associatifs en Igwan.net, enerzijds, en de Premier ministre (eerste minister, Frankrijk), de Garde des Sceaux, ministre de la Justice (minister van Justitie, Frankrijk), de ministre de l'Intérieur (minister van Binnenlandse Zaken, Frankrijk) en de ministre des Armées (minister van de Strijdkrachten, Frankrijk), anderzijds, over de rechtmatigheid van décret nº 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement (decreet nr. 2015-1185 van 28 september 2015 houdende aanwijzing van de gespecialiseerde inlichtingendiensten) (JORF van 29 september 2015, tekst 1 van 97; hierna: 'decreet nr. 2015-1185'), décret nº 2015-1211, du 1er octobre 2015, relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État (decreet nr. 2015-1211 van 1 oktober 2015 betreffende geschillen inzake het gebruik van aan machtiging onderworpen inlichtingentechnieken en van voor

de staatsveiligheid relevante bestanden) (JORF van 2 oktober 2015, tekst 7 van 108; hierna: 'decreet nr. 2015-1211'), décret nº 2015-1639, du 11 décembre 2015, relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'article L. 811-4 du code de la sécurité intérieure (decreet nr. 2015-1639 van 11 december 2015 tot aanwijzing van de andere diensten dan de gespecialiseerde inlichtingendiensten, die gemachtigd zijn om gebruik te maken van de in boek VIII, titel V, van de code de la sécurité intérieure genoemde technieken, vastgesteld op grond van artikel L. 811-4 van de code de la sécurité intérieure) (JORF van 12 december 2015, tekst 28 van 127; hierna: 'decreet nr. 2015-1639'), en décret nº 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement (decreet nr. 2016-67 van 29 januari 2016 betreffende de technieken voor het inwinnen van inlichtingen) (JORF van 31 januari 2016, tekst 2 van 113; hierna: 'decreet nr. 2016-67').

3 Het verzoek in zaak C-512/18 is ingediend in het kader van gedingen tussen French Data Network, La Quadrature du Net en de Fédération des fournisseurs d'accès à Internet associatifs, enerzijds, en de Premier ministre (eerste minister, Frankrijk) en de Garde des Sceaux, ministre de la justice (minister van Justitie, Frankrijk), anderzijds, over de rechtmatigheid van artikel R. 10-13 van de code des postes et des communications électroniques (wetboek post en elektronische communicatie; hierna: 'CPCE') en van décret nº 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne (decreet nr. 2011-219 van 25 februari 2011 betreffende de bewaring en mededeling van gegevens die het mogelijk maken om personen te identificeren die hebben bijgedragen aan de creatie van online geplaatste inhoud) (JORF van 1 maart 2011, tekst 32 van 170; hierna: 'decreet nr. 2011-219').

4 Het verzoek in zaak C-520/18 is ingediend in het kader van gedingen tussen de Ordre des barreaux francophones et germanophone, de Académie Fiscale ASBL, UA, de Liga voor Mensenrechten VZW, de Ligue des Droits de l'Homme ASBL, VZ, WY en XX, enerzijds, en de Ministerraad (België), anderzijds, over de rechtmatigheid van de Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie (*Belgisch Staatsblad*, 18 juli 2016, blz. 44717; hierna: 'wet van 29 mei 2016').

Toepasselijke bepalingen

Unierecht

Richtlijn 95/46

5 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (*PB* 1995, L 281, blz. 31) is met ingang van 25 mei 2018 ingetrokken bij verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46 (algemene verordening gegevensbescherming) (*PB* 2016, L 119, blz. 1). Artikel 3, lid 2, van richtlijn 95/46 luidde als volgt:

'De bepalingen van deze richtlijn zijn niet van toepassing op de verwerking van persoonsgegevens:

- die met het oog op de uitoefening van niet binnen de werkingssfeer van het gemeenschapsrecht vallende activiteiten geschiedt zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie en in ieder geval verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de staat (waaronder de economie van de staat, wanneer deze verwerkingen in verband staan met vraagstukken van staatsveiligheid), en de activiteiten van de staat op strafrechtelijk gebied;
- die door een natuurlijk persoon in activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden wordt verricht.'

6 Artikel 22 van richtlijn 95/46, dat was opgenomen in hoofdstuk III ('Beroep op de rechter, aansprakelijkheid en sancties') van deze richtlijn, bepaalde:

'Onverminderd de administratieve voorziening die met name bij de in artikel 28 bedoelde toezichthoudende autoriteit kan worden getroffen voordat de zaak aanhangig wordt gemaakt voor de rechter, bepalen de lidstaten dat eenieder zich tot de rechter kan wenden wanneer de rechten die hem worden gegarandeerd door het op de betrokken verwerking toepasselijke nationale recht geschonden worden.'

Richtlijn 97/66

7 Artikel 5 van richtlijn 97/66/EG van het Europees Parlement en de Raad van 15 december 1997 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector (*PB* 1997, L 24, blz. 1), met het opschrift 'Vertrouwelijk karakter van de oproepen', luidde als volgt:

'1. De lidstaten garanderen in hun nationale reglementering het vertrouwelijk karakter van oproepen via het openbare telecommunicatienetwerk en via algemeen beschikbare telecommunicatiediensten. Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van gesprekken door anderen dan de gebruikers, indien de betrokken gebruikers daarmee niet hebben ingestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 14, lid 1.

2. Lid 1 is niet van toepassing op de wettelijk toegestane registratie van oproepen in het legale zakelijke verkeer ten bewijze van een commerciële transactie of van enigerlei andere zakelijke oproep.'

Richtlijn 2000/31

8 In de overwegingen 14 en 15 van richtlijn 2000/31 staat te lezen:

'(14) De bescherming van individuen met betrekking tot de verwerking van persoonsgegevens is alleen geregeld bij [richtlijn 95/46] en bij [richtlijn 97/66], die volledig van toepassing zijn op diensten van de informatiemaatschappij. Die richtlijnen vormen reeds een communautair wettelijk kader op het gebied van persoonsgegevens, en het is daarom niet nodig die kwestie in deze richtlijn op te nemen om een soepele werking van de interne markt te garanderen, met name wat betreft het vrije verkeer van persoonsgegevens tussen lidstaten. Deze richtlijn moet worden uitgevoerd en toegepast met volledige inachtneming van de beginselen inzake de bescherming van persoonsgegevens, met name wat ongevraagde commerciële communicatie en de aansprakelijkheid van tussenpersonen betreft. Deze richtlijn kan het anonieme gebruik van open netwerken zoals Internet niet voorkomen.

(15) De vertrouwelijkheid van berichten wordt gewaarborgd door artikel 5 van [richtlijn 97/66]. Op basis van die richtlijn moeten de lidstaten iedere vorm van onderschepping of bewaking van deze berichten door andere personen dan de verzender en de adressaat verbieden, tenzij dit wettelijk toegestaan is.'

9 Artikel 1 van richtlijn 2000/31 bepaalt:

'1. Deze richtlijn heeft tot doel bij te dragen aan de goede werking van de interne markt door het vrije verkeer van de diensten van de informatiemaatschappij tussen lidstaten te waarborgen.

2. Voor zover voor de verwezenlijking van de in lid 1 genoemde doelstelling nodig, worden met deze richtlijn bepaalde nationale bepalingen nader tot elkaar gebracht die van toepassing zijn op de diensten van de informatiemaatschappij en betrekking hebben op de interne markt, de vestiging van de dienstverleners, de commerciële communicatie, langs elektronische weg gesloten contracten, de aansprakelijkheid van tussenpersonen, gedragscodes, de buitengerechtelijke geschillenregeling, rechtsgedingen en de samenwerking tussen lidstaten.

3. Deze richtlijn vormt een aanvulling op het communautaire recht dat van toepassing is op de diensten van de informatiemaatschappij en doet niet af aan het in de communautaire besluiten en nationale wetgeving ter uitvoering daarvan vastgelegde niveau van bescherming, inzonderheid van de volksgezondheid en de consumentenbelangen, voor zover de vrijheid om diensten van de informatiemaatschappij te verlenen daardoor niet beperkt wordt.

[…]

5. Deze richtlijn is niet van toepassing op:

[…]

b) kwesties in verband met diensten van de informatiemaatschappij die onder [richtlijn 95/46] en [richtlijn 97/66] vallen;

[…]'

10 Artikel 2 van richtlijn 2000/31 luidt als volgt:

'Voor de doeleinden van deze richtlijn wordt verstaan onder:

a) 'diensten van de informatiemaatschappij': diensten zoals omschreven in artikel 1, lid 2, van richtlijn 98/34/EG [van het Europees Parlement en de Raad van 22 juni 1998 betreffende een informatieprocedure op het gebied van normen en technische voorschriften (*PB* 1998, L 204, blz. 37)], zoals gewijzigd bij richtlijn 98/48/EG [van het Europees Parlement en de Raad van 20 juli 1998 (*PB* 1998, L 217, blz. 18)];

[…]'

11 Artikel 15 van richtlijn 2000/31 bepaalt:

'1. Met betrekking tot de levering van de in de artikelen 12, 13 en 14 bedoelde diensten leggen de lidstaten de dienstverleners geen algemene verplichting op om toe te zien op de informatie die zij doorgeven of opslaan, noch om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden.

2. De lidstaten kunnen voorschrijven dat dienstverleners de bevoegde autoriteiten onverwijld in kennis dienen te stellen van vermeende onwettige activiteiten of informatie door afnemers van hun dienst, alsook dat zij de bevoegde autoriteiten op hun verzoek informatie dienen te verstrekken waarmee de afnemers van hun dienst met wie zij opslagovereenkomsten hebben gesloten, kunnen worden geïdentificeerd.'

Richtlijn 2002/21

12 In overweging 10 van richtlijn 2002/21/EG van het Europees Parlement en de Raad van 7 maart 2002 inzake een gemeenschappelijk regelgevingskader voor elektronischecommunicatienetwerken en -diensten (kaderrichtlijn) (*PB* 2002, L 108, blz. 33) wordt verklaard:

'De definitie van 'dienst van de informatiemaatschappij' in artikel 1 van [richtlijn 98/34, zoals gewijzigd bij richtlijn 98/48,] bestrijkt een breed scala van economische activiteiten die online plaatsvinden; de meeste van deze activiteiten vallen niet binnen de werkingssfeer van de onderhavige richtlijn omdat zij niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronischecommunicatienetwerken; spraaktelefonie en de diensten voor het overbrengen van elektronische post vallen onder deze richtlijn; dezelfde onderneming, bijvoorbeeld een verstrekker van internetdiensten, kan een elektronischecommunicatiedienst aanbie-

den, zoals de toegang tot internet, en diensten die niet onder deze richtlijn vallen, zoals de levering van internet-inhoud.'

13 Artikel 2 van richtlijn 2002/21 bepaalt:

'Voor de toepassing van deze richtlijn wordt verstaan onder:

[…]

c) 'elektronischecommunicatiedienst': een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronischecommunicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch niet de dienst waarbij met behulp van elektronischecommunicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd. Hij omvat niet de diensten van de informatiemaatschappij zoals omschreven in artikel 1 van [richtlijn 98/34], die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronischecommunicatienetwerken;

[…]'

Richtlijn 2002/58

14 In de overwegingen 2, 6, 7, 11, 22, 26 en 30 van richtlijn 2002/58 staat te lezen:

'(2) Deze richtlijn strekt tot eerbiediging van de grondrechten en beginselen die tot uitdrukking zijn gebracht in met name het [Handvest]. In het bijzonder strekt deze richtlijn tot volledige eerbiediging van de in de artikelen 7 en 8 [van het Handvest] bedoelde rechten.

[…]

(6) Het internet vervangt traditionele marktstructuren door te voorzien in een gemeenschappelijke, wereldwijde infrastructuur voor de levering van een breed scala van elektronischecommunicatiediensten. Algemeen beschikbare elektronischecommunicatiediensten via het internet bieden de gebruikers nieuwe mogelijkheden, maar houden ook nieuwe gevaren in voor de bescherming van hun persoonsgegevens en persoonlijke levenssfeer.

(7) Voor openbare communicatienetwerken moeten specifieke wettelijke, bestuursrechtelijke en technische bepalingen worden vastgesteld teneinde de fundamentele rechten en vrijheden van natuurlijke personen en de rechtmatige belangen van rechtspersonen te beschermen tegen met name de steeds grotere mogelijkheden in verband met de geautomatiseerde opslag en verwerking van gegevens met betrekking tot de abonnees en de gebruikers.

[…]

(11) Deze richtlijn is evenmin als [richtlijn 95/46] van toepassing op vraagstukken met betrekking tot de bescherming van fundamentele rechten en vrijheden in verband met niet onder het [Unierecht] vallende activiteiten. Zij verandert bijgevolg niets aan het bestaande evenwicht tussen het recht van personen op persoonlijke levenssfeer en de mogelijkheid voor de lidstaten om de in artikel 15, lid 1, van deze richtlijn bedoelde maatregelen te nemen, die nodig zijn voor de bescherming van de openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economisch welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de wetshandhaving op strafrechtelijk gebied. Bijgevolg doet deze richtlijn geen afbreuk aan de mogelijkheid voor de lidstaten om wettelijk toegestane interceptie van elektronische communicatie uit te voeren of andere maatregelen vast te stellen, wanneer dat voor één van voornoemde doeleinden noodzakelijk is, mits zij daarbij het [op 4 november 1950 te Rome ondertekende] Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, zoals geïnterpreteerd in de uitspraken van het Europees Hof voor de rechten van de mens, in acht nemen. Zulke maatregelen dienen passend te zijn voor, en strikt evenredig met, het beoogde doel en noodzakelijk in een democratische samenleving en moeten adequate waarborgen bevatten overeenkomstig het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.

[…]

(22) Het verbod op het opslaan van communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers of zonder hun toestemming is niet bedoeld om de automatische, tussentijdse en tijdelijke opslag van die informatie te verbieden, voor zover deze opslag uitsluitend dient voor het doorzenden in het elektronischecommunicatienetwerk en mits de informatie niet langer wordt opgeslagen dan nodig voor het doorzenden en het beheer van het verkeer, en het vertrouwelijk karakter tijdens de opslag gewaarborgd blijft. […]

[…]

(26) De gegevens over abonnees die in elektronischecommunicatienetwerken worden verwerkt om verbindingen tot stand te brengen en informatie over te dragen, bevatten informatie over het privéleven van natuurlijke personen en betreffen het recht op respect voor hun correspondentie of de rechtmatige belangen van rechtspersonen. Dergelijke gegevens mogen slechts worden opgeslagen voor zover dat nodig is voor het leveren van de dienst, voor facturering en voor interconnectiebetalingen, en slechts gedurende een beperkte tijd. Elke verdere verwerking van dergelijke gegevens […] is slechts toegestaan indien de abonnee daarmee heeft ingestemd op basis van precieze en volledige informatie van de aanbieder van de openbare elektronischecommunicatiedienst over de door hem geplande verdere verwerking van de gegevens en over het recht van de abonnee een dergelijke verwerking niet toe te staan of de toestemming daartoe in te trekken. Verkeersgegevens die worden gebruikt voor de marketing van communicatiediensten

[…] moeten ook worden gewist of anoniem gemaakt […].

[…]

(30) Systemen voor elektronischecommunicatienetwerken en -diensten moeten op dusdanige wijze worden ontworpen dat het aantal persoonsgegevens tot het strikt noodzakelijke minimum wordt beperkt. […]'

15 Artikel 1 ('Werkingssfeer en doelstelling') van richtlijn 2002/58 bepaalt:

'1. Deze richtlijn voorziet in de harmonisering van de regelgeving van de lidstaten die nodig is om een gelijk niveau van bescherming van fundamentele rechten en vrijheden — met name het recht op een persoonlijke levenssfeer en vertrouwelijkheid — bij de verwerking van persoonsgegevens in de sector elektronische communicatie te waarborgen en om te zorgen voor het vrij verkeer van dergelijke gegevens en van elektronischecommunicatieapparatuur en diensten in de [Europese Unie].

2. Voor de doelstellingen van lid 1 vormen de bepalingen van deze richtlijn een specificatie van en een aanvulling op [richtlijn 95/46]. Bovendien voorzien zij in bescherming van de rechtmatige belangen van abonnees die rechtspersonen zijn.

3. Deze richtlijn is niet van toepassing op activiteiten die niet onder het [VWEU] vallen, zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie, en in geen geval op activiteiten die verband houden met de openbare veiligheid, defensie, staatsveiligheid (met inbegrip van het economische welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid) en de activiteiten van de staat op strafrechtelijk gebied.'

16 Artikel 2 ('Definities') van richtlijn 2002/58 luidt:

'Tenzij anders is bepaald, zijn de definities van [richtlijn 95/46] en [richtlijn 2002/21] van toepassing.

Daarnaast wordt in deze richtlijn verstaan onder:

a) 'gebruiker': natuurlijke persoon die gebruikmaakt van een openbare elektronischecommunicatiedienst voor particuliere of zakelijke doeleinden zonder noodzakelijkerwijze op die dienst te zijn geabonneerd;

b) 'verkeersgegevens': gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronischecommunicatienetwerk of voor de facturering ervan;

c) 'locatiegegevens': gegevens die in een elektronischecommunicatienetwerk of door een elektronischecommunicatiedienst worden verwerkt, waarmee de geografische positie van de eindapparatuur van een gebruiker van een openbare elektronischecommunicatiedienst wordt aangegeven;

d) 'communicatie': informatie die wordt uitgewisseld of overgebracht tussen een eindig aantal partijen door middel van een openbare elektronischecommunicatiedienst. Dit omvat niet de informatie die via een omroepdienst over een elektronischecommunicatienetwerk wordt overgebracht, behalve wanneer de informatie kan worden gerelateerd aan de identificeerbare abonnee of gebruiker die de informatie ontvangt;

[…]'

17 Artikel 3 ('Betrokken diensten') van richtlijn 2002/58 bepaalt:

'Deze richtlijn is van toepassing op de verwerking van persoonsgegevens in verband met de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de [Unie], met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen.'

18 In artikel 5 ('Vertrouwelijk karakter van de communicatie') van die richtlijn staat:

'1. De lidstaten garanderen via nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronischecommunicatiediensten. Zij verbieden met name het afluisteren, aftappen, opslaan of anderszins onderscheppen of controleren van de communicatie en de daarmee verband houdende verkeersgegevens door anderen dan de gebruikers, indien de betrokken gebruikers daarin niet hebben toegestemd, tenzij dat bij wet is toegestaan overeenkomstig artikel 15, lid 1. Dit lid laat de technische opslag die nodig is voor het overbrengen van informatie onverlet, onverminderd het vertrouwelijkheidsbeginsel.

[…]

3. De lidstaten dragen ervoor zorg dat de opslag van informatie of het verkrijgen van toegang tot informatie die reeds is opgeslagen in de eindapparatuur van een abonnee of gebruiker, alleen is toegestaan op voorwaarde dat de betrokken abonnee of gebruiker toestemming heeft verleend, na te zijn voorzien van duidelijke en volledige informatie overeenkomstig [richtlijn 95/46], onder meer over de doeleinden van de verwerking. Zulks vormt geen beletsel voor enige vorm van technische opslag of toegang met als uitsluitend doel de uitvoering van de verzending van een communicatie over een elektronisch communicatienetwerk, of, indien strikt noodzakelijk, om ervoor te zorgen dat de aanbieder van een uitdrukkelijk door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij deze dienst levert.'

19 Artikel 6 ('Verkeersgegevens') van richtlijn 2002/58 bepaalt:

'1. Verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen door de aanbieder van een openbaar elektronischecommunicatienetwerk of -dienst, moeten, wanneer ze niet langer nodig zijn voor

het doel van de transmissie van communicatie, worden gewist of anoniem gemaakt, onverminderd de leden 2, 3 en 5, alsmede artikel 15, lid 1.

2. Verkeersgegevens die noodzakelijk zijn ten behoeve van de facturering van abonnees en interconnectiebetalingen mogen worden verwerkt. Die verwerking is slechts toegestaan tot aan het einde van de termijn waarbinnen de rekening in rechte kan worden aangevochten of de betaling kan worden afgedwongen.

3. De aanbieder van een openbare elektronischecommunicatiedienst mag ten behoeve van de marketing van elektronischecommunicatiediensten of voor de levering van diensten met toegevoegde waarde de in lid 1 bedoelde gegevens verwerken voor zover en voor zolang dat nodig is voor dergelijke diensten of marketing, indien de abonnee of de gebruiker waarop de gegevens betrekking hebben daartoe zijn voorafgaande toestemming heeft gegeven. Gebruikers of abonnees kunnen hun toestemming voor de verwerking van verkeersgegevens te allen tijde intrekken.

[…]

5. De verwerking van verkeersgegevens overeenkomstig de leden 1 tot en met 4 mag alleen worden uitgevoerd door personen die werkzaam zijn onder het gezag van de aanbieders van de openbare communicatienetwerken of -diensten voor facturering of verkeersbeheer, behandeling van verzoeken om inlichtingen van klanten, opsporing van fraude en marketing van elektronischecommunicatiediensten van de aanbieder of de levering van diensten met toegevoegde waarde, en moet beperkt blijven tot hetgeen noodzakelijk is om die activiteiten te kunnen uitvoeren.'

20 Artikel 9 ('Andere locatiegegevens dan verkeersgegevens') van die richtlijn bepaalt in lid 1:

'Wanneer andere locatiegegevens dan verkeersgegevens die betrekking hebben op gebruikers of abonnees van elektronischecommunicatienetwerken of -diensten verwerkt kunnen worden, mogen deze gegevens slechts worden verwerkt wanneer zij anoniem zijn gemaakt of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven, voor zover en voor zolang zulks nodig is voor de levering van een dienst met toegevoegde waarde. De dienstenaanbieder moet de gebruikers of abonnees, voorafgaand aan het verkrijgen van hun toestemming, in kennis stellen van de soort locatiegegevens anders dan verkeersgegevens, die zullen worden verwerkt, en van de doeleinden en de duur van die verwerking, en hun meedelen of deze gegevens aan een derde zullen worden doorgegeven ten behoeve van de levering van de dienst met toegevoegde waarde. […]'

21 Artikel 15 ('Toepassing van een aantal bepalingen van [richtlijn 95/46]') van richtlijn 2002/58 bepaalt:

'1. De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, d.w.z. de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronischecommunicatiesysteem als bedoeld in artikel 13, lid 1, van [richtlijn 95/46]. Daartoe kunnen de lidstaten o.a. wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. Alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het [Unierecht], met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie.

[…]

2. Het bepaalde in hoofdstuk III van [richtlijn 95/46] inzake beroep op de rechter, aansprakelijkheid en sancties geldt voor de nationale bepalingen die uit hoofde van deze richtlijn worden aangenomen en ten aanzien van de individuele rechten die uit deze richtlijn voortvloeien.

[…]'

Verordening 2016/679

22 In overweging 10 van verordening 2016/679 wordt verklaard:

'Teneinde natuurlijke personen een consistent en hoog beschermingsniveau te bieden en de belemmeringen voor het verkeer van persoonsgegevens binnen de Unie op te heffen, dient het niveau van bescherming van de rechten en vrijheden van natuurlijke personen op het vlak van verwerking van deze gegevens in alle lidstaten gelijkwaardig te zijn. Er moet gezorgd worden voor een in de gehele Unie coherente en homogene toepassing van de regels inzake bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens. […]'

23 Artikel 2 van die verordening bepaalt:

'1. Deze verordening is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

2. Deze verordening is niet van toepassing op de verwerking van persoonsgegevens:

a) in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen;

b) door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU vallen;

[…]

d) door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

[…]

4. Deze verordening laat de toepassing van [richtlijn 2000/31], en met name van de regels in de artikelen 12 tot en met 15 van die richtlijn betreffende de aansprakelijkheid van als tussenpersoon optredende dienstverleners onverlet.'

24 Artikel 4 van verordening 2016/679 luidt als volgt:

'Voor de toepassing van deze verordening wordt verstaan onder:

1) 'persoonsgegevens': alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('de betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

2) 'verwerking': een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

[…]'

25 Artikel 5 van die verordening bepaalt:

'1. Persoonsgegevens moeten:

a) worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is ('rechtmatigheid, behoorlijkheid en transparantie');

b) voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd ('doelbinding');

c) toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt ('minimale gegevensverwerking');

d) juist zijn en zo nodig worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren ('juistheid');

e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen ('opslagbeperking');

f) door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier worden verwerkt dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging ('integriteit en vertrouwelijkheid').

[…]'

26 Artikel 6 van verordening 2016/679 luidt als volgt:

'1. De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan:

[…]

c) de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;

[…]

3. De rechtsgrond voor de in lid 1, [onder] c) en e), bedoelde verwerking moet worden vastgesteld bij:

a) Unierecht; of

b) lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is.

Het doel van de verwerking wordt in die rechtsgrond vastgesteld […]. Die rechtsgrond kan specifieke bepalingen bevatten om de toepassing van de regels van deze verordening aan te passen, met inbegrip van de algemene voorwaarden inzake de rechtmatigheid van verwerking door de verwerkingsverantwoordelijke; de types verwerkte gegevens; de betrokkenen; de entiteiten waaraan en de doeleinden waarvoor de persoonsgegevens mogen worden verstrekt; de doelbinding; de opslagperioden; en de verwerkingsactiviteiten en -procedures, waaronder maatregelen om te zorgen voor een rechtmatige en behoorlijke verwerking, zoals die voor andere specifieke verwerkingssituaties als bedoeld in hoofdstuk IX. Het Unierecht of het lidstatelijke

recht moet beantwoorden aan een doelstelling van algemeen belang en moet evenredig zijn met het nagestreefde gerechtvaardigde doel.
[…]'

27 Artikel 23 van die verordening bepaalt:

'1. De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan, voor zover de bepalingen van die artikelen overeenstemmen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met [22], worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van:

a) de nationale veiligheid;

b) landsverdediging;

c) de openbare veiligheid;

d) de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid;

e) andere belangrijke doelstellingen van algemeen belang van de Unie of van een lidstaat, met name een belangrijk economisch of financieel belang van de Unie of van een lidstaat, met inbegrip van monetaire, budgettaire en fiscale aangelegenheden, volksgezondheid en sociale zekerheid;

f) de bescherming van de onafhankelijkheid van de rechter en gerechtelijke procedures;

g) de voorkoming, het onderzoek, de opsporing en de vervolging van schendingen van de beroepscodes voor gereglementeerde beroepen;

h) een taak op het gebied van toezicht, inspectie of regelgeving die verband houdt, al is het incidenteel, met de uitoefening van het openbaar gezag in de in de punten a), tot en met e) en punt g) bedoelde gevallen;

i) de bescherming van de betrokkene of van de rechten en vrijheden van anderen;

j) de inning van civielrechtelijke vorderingen.

2. De in lid 1 bedoelde wettelijke maatregelen bevatten met name specifieke bepalingen met betrekking tot, in voorkomend geval, ten minste:

a) de doeleinden van de verwerking of van de categorieën van verwerking,

b) de categorieën van persoonsgegevens,

c) het toepassingsgebied van de ingevoerde beperkingen,

d) de waarborgen ter voorkoming van misbruik of onrechtmatige toegang of doorgifte,

e) de specificatie van de verwerkingsverantwoordelijke of de categorieën van verwerkingsverantwoordelijken,

f) de opslagperiodes en de toepasselijke waarborgen, rekening houdend met de aard, de omvang en de doeleinden van de verwerking of van de categorieën van verwerking,

g) de risico's voor de rechten en vrijheden van de betrokkenen, en

h) het recht van betrokkenen om van de beperking op de hoogte te worden gesteld, tenzij dit afbreuk kan doen aan het doel van de beperking.'

28 Artikel 79, lid 1, van dezelfde verordening bepaalt:

'Onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep, waaronder het recht uit hoofde van artikel 77 een klacht in te dienen bij een toezichthoudende autoriteit, heeft elke betrokkene het recht een doeltreffende voorziening in rechte in te stellen indien hij van mening is dat zijn rechten uit hoofde van deze verordening geschonden zijn ten gevolge van een verwerking van zijn persoonsgegevens die niet aan deze verordening voldoet.'

29 In artikel 94 van verordening 2016/679 staat:

'1. [Richtlijn 95/46] wordt met ingang van 25 mei 2018 ingetrokken.

2. Verwijzingen naar de ingetrokken richtlijn gelden als verwijzingen naar deze verordening. Verwijzingen naar de groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, die bij artikel 29 van [richtlijn 95/46] is opgericht, gelden als verwijzingen naar het bij deze verordening opgerichte Europees Comité voor gegevensbescherming.'

30 Artikel 95 van die verordening bepaalt:

'Deze verordening legt natuurlijke personen of rechtspersonen geen aanvullende verplichtingen op met betrekking tot verwerking in verband met het verstrekken van openbare elektronischecommunicatiediensten in openbare communicatienetwerken in de Unie, voor zover zij op grond van [richtlijn 2002/58] onderworpen zijn aan specifieke verplichtingen met dezelfde doelstelling.'

Frans recht

CSI

31 Boek VIII van het deel 'wetgeving' van de code de la sécurité intérieure (wetboek binnenlandse veiligheid; hierna: 'CSI') bevat in de artikelen L. 801-1 tot en met L. 898-1 regels betreffende het inwinnen van inlichtingen.

32 Artikel L. 811-3 CSI bepaalt:

'Uitsluitend met het oog op de uitoefening van hun respectieve taken kunnen de gespecialiseerde inlichtingendiensten gebruikmaken van de in titel V van dit boek genoemde technieken voor

het inwinnen van inlichtingen betreffende de verdediging en bevordering van de volgende fundamentele staatsbelangen:

1o de nationale onafhankelijkheid, de integriteit van het grondgebied en de landsverdediging;

2o de zwaarwegende belangen van het buitenlands beleid, de nakoming door Frankrijk van zijn Europese en internationale verplichtingen, en de voorkoming van elke vorm van buitenlandse inmenging;

3o de zwaarwegende economische, industriële en wetenschappelijke belangen van Frankrijk;

4o de voorkoming van terrorisme;

5o de voorkoming van:

a) aanvallen op de republikeinse vorm van de instituties;

b) acties die gericht zijn op het in stand houden of opnieuw oprichten van groeperingen die overeenkomstig artikel L. 212-1 zijn ontbonden;

c) collectieve gewelddadigheden die de openbare vrede ernstig ondermijnen;

6o de voorkoming van georganiseerde misdaad;

7o de voorkoming van de verspreiding van massavernietigingswapens.'

33 Artikel L. 811-4 CSI luidt als volgt:

'Bij decreet vastgesteld na advies van de Conseil d'État [(hoogste bestuursrechter, Frankrijk)] en van de Commission nationale de contrôle des techniques de renseignement [(nationale commissie voor toezicht op inlichtingentechnieken)], worden de andere diensten dan de gespecialiseerde inlichtingendiensten — ressorterend onder de minister van Defensie, de minister van Binnenlandse Zaken of de minister van Justitie of onder de ministers belast met economische zaken, begrotingszaken en douanezaken — aangewezen waaraan machtiging kan worden verleend om onder de in dit boek vastgestelde voorwaarden gebruik te maken van de in titel V van dit boek genoemde technieken. Het decreet specificeert voor elke dienst de in artikel L. 811-3 vermelde doelstellingen en de technieken waarvoor machtiging kan worden verleend.'

34 In artikel L. 821-1, eerste alinea, CSI staat:

'De toepassing op het nationale grondgebied van de in titel V, hoofdstukken I tot en met IV, van dit boek genoemde technieken voor het inwinnen van inlichtingen is onderworpen aan voorafgaande machtiging van de eerste minister, verleend na advies van de nationale commissie voor toezicht op inlichtingentechnieken.'

35 Artikel 821-2 CSI bepaalt:

'De in artikel L. 821-1 genoemde machtiging wordt verleend op schriftelijk en met redenen omkleed verzoek van de minister van Defensie, de minister van Binnenlandse zaken, de minister van Justitie of de ministers belast met economische zaken, begrotingszaken of douanezaken.

Elke minister kan deze bevoegdheid uitsluitend delegeren aan directe medewerkers die zich mogen bezighouden met vertrouwelijke kwesties in verband met de landsverdediging.

Het verzoek vermeldt:

1o de toe te passen techniek of technieken;

2o de dienst waarvoor het wordt ingediend;

3o de nagestreefde doelstelling of doelstellingen;

4o de reden of redenen voor de maatregelen;

5o de geldigheidsduur van de machtiging;

6o de persoon of de personen, de plaats of de plaatsen dan wel het voertuig of de voertuigen waarop het verzoek betrekking heeft.

Voor de toepassing van punt 6 kunnen personen van wie de identiteit onbekend is, worden aangeduid met hun identificatiekenmerken of hun hoedanigheid, en kunnen plaatsen of voertuigen worden aangeduid door verwijzing naar de personen op wie het verzoek betrekking heeft.

[…]'

36 Artikel L. 821-3, eerste alinea, CSI luidt als volgt:

'Het verzoek wordt meegedeeld aan de voorzitter of aan een van de in van artikel L. 831-1, 2° en 3°, genoemde leden van de nationale commissie voor toezicht op inlichtingentechnieken, die binnen 24 uur advies uitbrengt aan de eerste minister. Indien het verzoek wordt beoordeeld door de commissie in beperkte dan wel in volle samenstelling, wordt de eerste minister daarvan onverwijld in kennis gesteld en wordt het advies uitgebracht binnen 72 uur.'

37 Artikel L. 821-4 CSI bepaalt:

'De machtiging om de in titel V, hoofdstukken I tot en met IV, van dit boek genoemde technieken toe te passen, wordt door de eerste minister verleend voor een periode van maximaal vier maanden. […] De machtiging bevat de in artikel L. 821-2, 1° tot en met 6°, bedoelde motieven en vermeldingen. Elke machtiging kan onder dezelfde voorwaarden als genoemd in dit hoofdstuk worden verlengd.

Wanneer de machtiging wordt verleend na een negatief advies van de commissie voor toezicht op inlichtingentechnieken, worden daarin de redenen vermeld waarom dat advies niet is opgevolgd.

[…]'

38 Artikel L. 833-4 CSI, dat is opgenomen in hoofdstuk III van diezelfde titel, bepaalt:

'Hetzij uit eigen beweging, hetzij nadat bij haar een klacht is ingediend door een persoon die zich ervan wil vergewissen dat er niet op onregelmatige wijze inlichtingentechnieken jegens hem worden toegepast, gaat de commissie na of bij de toepassing van de betrokken techniek of technieken de bepalingen van dit boek in acht zijn of worden genomen. Zij stelt de indiener van de klacht ervan in kennis de noodzakelijke on-

derzoeken te hebben uitgevoerd, zonder de toepassing van dergelijke technieken te bevestigen of te ontkennen.'

39 Artikel L. 841-1, eerste en tweede alinea, CSI luidt als volgt:

'Onverminderd de in artikel L. 854-9 van dit wetboek opgenomen bijzondere bepalingen, is de Conseil d'État bevoegd om onder de in titel VII, hoofdstuk III bis, van boek VII van de code de justice administrative [(wetboek van bestuursprocesrecht)] vastgestelde voorwaarden kennis te nemen van verzoeken betreffende de toepassing van de in titel V van de in dit boek genoemde inlichtingentechnieken.

De Conseil d'État kan worden aangezocht door:

1o eenieder die zich ervan wil vergewissen dat er niet op onregelmatige wijze inlichtingentechnieken jegens hem worden toegepast en die kan aantonen dat eerst de procedure van artikel L. 833-4 is doorlopen;

2o de commissie voor toezicht op inlichtingentechnieken, onder de in artikel L. 833-8 vastgestelde voorwaarden.'

40 Boek VIII, titel V, van het deel 'wetgeving' van de CSI, betreffende 'aan machtiging onderworpen technieken voor het inwinnen van inlichtingen', bestaat onder meer uit hoofdstuk I ('Administratieve toegang tot verbindingsgegevens'), dat de artikelen L. 851-1 tot en met 851-7 CSI omvat.

41 Artikel L. 851-1 CSI bepaalt:

'Onder de in titel II, hoofdstuk I, van dit boek vastgestelde voorwaarden kan machtiging worden verleend om bij de exploitanten van elektronischecommunicatiemiddelen, bij de in artikel L. 34-1 [CPCE] genoemde personen en bij de personen genoemd in artikel 6, lid I, punten 1 en 2, van loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [(wet nr. 2004-575 van 21 juni 2004 ter bevordering van het vertrouwen in de digitale economie; JORF van 22 juni 2004, blz. 11168)] informatie of documenten op te vragen die werden verwerkt of opgeslagen door hun netwerken of elektronischecommunicatiediensten, met inbegrip van de technische gegevens betreffende de identificatie van abonnements- of verbindingsnummers voor elektronischecommunicatiediensten, de identificatie van alle abonnements- of verbindingsnummers van een bepaalde persoon, de locatie van de gebruikte eindapparatuur en de communicatie van een abonnee bestaande uit de lijst van nummers waarheen en waarvandaan is gebeld, de duur en datum van de communicatie.

In afwijking van artikel L. 821-2 worden schriftelijke en met redenen omklede verzoeken inzake de technische gegevens betreffende de identificatie van abonnements- of verbindingsnummers voor elektronischecommunicatiediensten, of betreffende de identificatie van alle abonnements- of verbindingsnummers van een bepaalde persoon, rechtstreeks aan de commissie voor toezicht op inlichtingentechnieken doorgezonden door de individueel aangewezen en gemachtigde functionarissen van de in de artikelen L. 811-2 en L. 811-4 genoemde inlichtingendiensten. De commissie brengt haar advies uit onder de in artikel L. 821-3 vastgestelde voorwaarden.

Een onder de eerste minister ressorterende dienst is belast met het opvragen van de informatie of documenten bij de in de eerste alinea van dit artikel genoemde exploitanten en personen. De nationale commissie voor toezicht op inlichtingentechnieken heeft permanent een volledige, rechtstreekse en onmiddellijke toegang tot de verzamelde informatie of documenten.

De nadere regels voor de toepassing van dit artikel worden bepaald bij decreet, vastgesteld na advies van de Conseil d'État en van de Commission nationale de l'informatique et des libertés [(nationale commissie voor informatica en vrijheden)] en de nationale commissie voor toezicht op inlichtingentechnieken.'

42 Artikel L. 851-2 CSI bepaalt:

'I. Onder de in titel II, hoofdstuk I, van dit boek bepaalde voorwaarden kan, uitsluitend ter voorkoming van terrorisme, individueel machtiging worden verleend om op de netwerken van de in artikel L. 851–1 genoemde exploitanten en personen in real time de in ditzelfde artikel genoemde informatie of documenten op te vragen met betrekking tot een persoon die eerder is geïdentificeerd als een persoon die in verband kan worden gebracht met een dreiging. Wanneer er zwaarwegende redenen zijn om aan te nemen dat een of meer personen uit de omgeving van de persoon op wie de machtiging betrekking heeft, informatie kunnen verstrekken voor het doel waarvoor de machtiging is verleend, kan de machtiging ook individueel voor elk van die personen worden verleend.

I bis. De eerste minister stelt na advies van de nationale commissie voor toezicht op inlichtingentechnieken het maximumaantal vast van de krachtens dit artikel verleende machtigingen die tegelijkertijd van kracht kunnen zijn. De commissie wordt in kennis gesteld van het besluit waarbij dit contingent wordt vastgesteld, van de verdeling ervan over de in artikel L. 821-2, eerste alinea, genoemde ministeries en van het aantal verleende interceptiemachtigingen.

[…]'

43 Artikel L. 851-3 CSI luidt als volgt:

'I. Onder de in titel II, hoofdstuk I, van dit boek bepaalde voorwaarden kan, uitsluitend ter voorkoming van terrorisme, aan de in artikel L. 851-1 genoemde exploitanten en personen de verplichting worden opgelegd om op hun netwerken geautomatiseerde verwerkingen uit te voeren die bedoeld zijn om, in overeenstemming met in de machtiging bepaalde parameters, verbindingen op te sporen waaruit een terroristische dreiging zou kunnen blijken.

Bij die geautomatiseerde verwerkingen wordt uitsluitend gebruikgemaakt van de in artikel L. 851-1 genoemde informatie of documenten. Er mogen geen andere gegevens worden opgevraagd dan die welke beantwoorden aan de ontwerpparameters, en de personen op wie de informatie of documenten betrekking hebben, mogen niet kunnen worden geïdentificeerd.
Met inachtneming van het evenredigheidsbeginsel wordt in de door de eerste minister verleende machtiging de technische reikwijdte van de toepassing van die verwerkingen gepreciseerd.
II. De nationale commissie voor toezicht op inlichtingentechnieken brengt advies uit over het verzoek tot het verlenen van een machtiging voor geautomatiseerde verwerkingen en over de gehanteerde parameters voor het opsporen van verbindingen. Zij heeft permanent volledige en rechtstreekse toegang tot die verwerkingen en tot de opgevraagde informatie en gegevens. Zij wordt in kennis gesteld van alle wijzigingen in de verwerkingen en parameters en kan aanbevelingen doen.
De eerste machtiging voor de toepassing van geautomatiseerde verwerkingen als bedoeld in lid I van dit artikel wordt verleend voor de duur van twee maanden. De machtiging kan worden verlengd onder de in titel II, hoofdstuk I, van dit boek bepaalde voorwaarden inzake duur. De verlengingsaanvraag bevat een overzicht van het aantal identificatoren dat door middel van de automatische verwerking is gesignaleerd, alsook een analyse van de relevantie van die signaleringen.
III. De in artikel L. 871-6 bepaalde voorwaarden zijn van toepassing op de materiële verrichtingen die de in artikel L. 851-1 genoemde exploitanten en personen uitvoeren met het oog op dergelijke verwerkingen.
IV. Wanneer door middel van de in lid I van dit artikel genoemde verwerkingen gegevens worden opgespoord waaruit een terroristische dreiging zou kunnen blijken, kan de eerste minister of een van de personen aan wie deze minister zijn bevoegdheid heeft gedelegeerd, nadat de nationale commissie voor toezicht op inlichtingentechnieken overeenkomstig de in titel II, hoofdstuk I, van dit boek bepaalde voorwaarden advies heeft uitgebracht, toestemming geven om de betrokken persoon of personen te identificeren en om de betrokken gegevens op te vragen. Die gegevens worden gebruikt binnen een termijn van zestig dagen nadat zij zijn opgevraagd en worden na afloop van die termijn vernietigd, tenzij er ernstige aanwijzingen zijn voor een terroristische dreiging waarmee een of meer van de betrokken personen in verband kunnen worden gebracht.
[…]'

44 Artikel L. 851-4 CSI bepaalt:
'Onder de in titel II, hoofdstuk I, van dit boek bepaalde voorwaarden kunnen de in artikel L. 851-1 genoemde technische gegevens betreffende de locatie van de gebruikte eindapparatuur op verzoek worden opgevraagd aan het netwerk en door de exploitanten in real time worden doorgezonden aan een onder de eerste minister ressorterende dienst.'

45 Artikel R. 851-5 CSI, dat is opgenomen in het deel 'regelgeving' van dit wetboek, luidt als volgt:
'I. De in artikel L. 851-1 genoemde informatie of documenten zijn, met uitzondering van de inhoud van de correspondentie of de geraadpleegde informatie:
1o de informatie of de documenten genoemd in de artikelen R. 10-13 en R. 10-14 [CPCE] en in artikel 1 van [decreet nr. 2011-219];
2o de andere technische gegevens dan die welke worden genoemd onder 1°:
a) die het mogelijk maken de eindapparatuur te lokaliseren;
b) die betrekking hebben op de toegang van de eindapparatuur tot de netwerken of tot de openbare online communicatiediensten;
c) die betrekking hebben op het overbrengen van elektronische communicatie via de netwerken;
d) die betrekking hebben op de identificatie en authenticatie van een gebruiker, een verbinding, een netwerk of een openbare online communicatiedienst;
e) die betrekking hebben op de kenmerken van de eindapparatuur en op de configuratiegegevens van de op die apparatuur aanwezige software.
II. Enkel de in lid I, onder 1°, genoemde informatie en documenten mogen worden opgevraagd overeenkomstig artikel L. 851-1. Die opvraging geschiedt niet in real time.
De in lid I, onder 2°, genoemde informatie mag uitsluitend worden opgevraagd overeenkomstig de artikelen L. 851-2 en L. 851-3, onder de voorwaarden en binnen de grenzen die in deze artikelen zijn vastgesteld, en onverminderd de toepassing van artikel R. 851-9.'

CPCE

46 Artikel L. 34-1 CPCE bepaalt:
'I. Het onderhavige artikel is van toepassing op de verwerking van persoonsgegevens in het kader van de levering van elektronischecommunicatiediensten aan het publiek. Het is met name van toepassing op netwerken die systemen voor gegevensverzameling en identificatie ondersteunen.
II. De exploitanten van elektronischecommunicatiemiddelen, en met name de personen van wie de activiteit erin bestaat het publiek online toegang tot communicatiediensten aan te bieden, wissen of anonimiseren alle verkeersgegevens, met inachtneming van het bepaalde in de leden III, IV, V en VI.

De personen die het publiek elektronischecommunicatiediensten aan het publiek aanbieden, stellen in overeenstemming met de bepalingen van de vorige alinea interne procedures vast om gevolg te geven aan verzoeken van de bevoegde autoriteiten.
Personen van wie de hoofd- of nevenberoepsactiviteit erin bestaat het publiek een aansluiting voor online communicatie via toegang tot het netwerk aan te bieden, ook gratis, dienen de bepalingen na te leven die krachtens dit artikel van toepassing zijn op de exploitanten van elektronischecommunicatiemiddelen.
III. Met het oog op het onderzoek, de vaststelling en de vervolging van strafbare feiten of van een niet-nakoming van de in artikel L. 336-3 van de code de la propriété intellectuelle [(wetboek intellectuele eigendom)] omschreven verplichting, of met het oog op het voorkomen van aanvallen op geautomatiseerde gegevensverwerkingssystemen als bedoeld en strafbaar gesteld in de artikelen 323-1 tot en met 323-3-1 van de code pénal [(wetboek van strafrecht)], en met als enige doel, indien nodig, de gegevens ter beschikking te kunnen stellen van de rechterlijke autoriteit of van de in artikel L. 331-12 van de code de la propriété intellectuelle bedoelde hoge autoriteit, of van de in artikel L. 2321-1 van de code de la défense [(wetboek defensie)] bedoelde nationale autoriteit voor de veiligheid van de informatiesystemen, kan het wissen of anonimiseren van bepaalde categorieën technische gegevens voor een periode van maximaal één jaar worden uitgesteld. Bij decreet vastgesteld na advies van de Conseil d'État en van de commissie voor informatica en vrijheden, worden binnen de in lid VI vastgestelde grenzen deze soorten gegevens en de duur van hun bewaring vastgesteld, naargelang van de activiteit van de exploitanten en de aard van de communicatie, alsook de wijze waarop, in voorkomend geval, de aanwijsbare en specifieke extra kosten verbonden aan de in dit verband door de exploitanten op verzoek van de staat verleende diensten worden gecompenseerd.
[…]
IV. De gegevens die worden bewaard en verwerkt onder de in de leden III, IV en V vastgestelde voorwaarden, hebben uitsluitend betrekking op de identificatie van de gebruikers van de door de exploitanten verleende diensten, de technische kenmerken van de door de exploitanten verleende communicatiediensten en de locatie van de eindapparatuur.
Zij mogen in geen geval betrekking hebben op de inhoud van de correspondentie of van de informatie die in het kader van deze communicatie in welke vorm dan ook is geraadpleegd.
De gegevens worden opgeslagen en verwerkt met inachtneming van de bepalingen van loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [(wet nr. 78-17 van 6 januari 1978 betreffende informatica, bestanden en vrijheden)].
De exploitanten nemen alle maatregelen om te voorkomen dat deze gegevens voor andere dan de in dit artikel genoemde doeleinden worden gebruikt.'

47 Artikel R. 10-13 CPCE luidt als volgt:
'I. Overeenkomstig lid III van artikel L. 34-1 bewaren de exploitanten van elektronischecommunicatiemiddelen de volgende gegevens met het oog op het onderzoek, de vaststelling en de vervolging van strafbare feiten:
a) gegevens aan de hand waarvan de gebruiker kan worden geïdentificeerd;
b) gegevens betreffende de gebruikte communicatie-eindapparatuur;
c) technische kenmerken, alsmede de datum, het tijdstip en de duur van elke communicatie;
d) gegevens betreffende de gevraagde of gebruikte aanvullende diensten en hun leveranciers;
e) gegevens aan de hand waarvan de ontvanger of ontvangers van de communicatie kunnen worden geïdentificeerd.
II. In het geval van telefonieactiviteiten bewaart de exploitant naast de in lid II genoemde gegevens ook de gegevens aan de hand waarvan de oorsprong en de locatie van de communicatie kunnen worden bepaald.
III. De in dit artikel genoemde gegevens worden bewaard gedurende één jaar, te rekenen vanaf de datum van registratie ervan.
IV. De aanwijsbare en specifieke extra kosten die zijn gemaakt door exploitanten die op bevel van de rechterlijke autoriteiten gegevens hebben verstrekt die onder de in dit artikel genoemde categorieën vallen, worden gecompenseerd op de wijze als bepaald in artikel R. 213-1 van de code de procédure pénale [(wetboek van strafvordering)].'

48 Artikel R. 10-14 CPCE bepaalt:
'I. Overeenkomstig lid IV van artikel L. 34-1 is het de exploitanten van elektronischecommunicatiemiddelen toegestaan om voor facturerings- en betalingsdoeleinden de technische gegevens te bewaren aan de hand waarvan de gebruiker kan worden geïdentificeerd, alsmede de technische gegevens die worden genoemd in artikel R. 10-13, lid I, onder b), c) en d).
II. In het geval van telefonieactiviteiten mogen de exploitanten behalve de in lid I genoemde gegevens ook de technische gegevens bewaren aan de hand waarvan de locatie van de communicatie kan worden bepaald en de ontvanger of de ontvangers van de communicatie kunnen worden geïdentificeerd, alsmede de voor de facturering benodigde gegevens.
III. De in de leden I en II van dit artikel genoemde gegevens mogen slechts worden bewaard indien zij nodig zijn voor de facturering en voor de betaling van de geleverde diensten.

Zij mogen niet langer worden bewaard dan strikt noodzakelijk is voor dat doel, en in geen geval langer dan één jaar.

IV. Ten behoeve van de veiligheid van de netwerken en de faciliteiten mogen de exploitanten gedurende een periode van maximaal drie maanden de volgende gegevens bewaren:

a) gegevens aan de hand waarvan de bron van de communicatie kan worden geïdentificeerd;

b) technische kenmerken alsmede de datum, het tijdstip en de duur van elke communicatie;

c) technische gegevens aan de hand waarvan de ontvanger of ontvangers van de communicatie kunnen worden geïdentificeerd;

d) gegevens betreffende de gevraagde of gebruikte aanvullende diensten en hun leveranciers.'

LCEN

49 Artikel 6 van loi nº 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique (wet nr. 2004-575 van 21 juni 2004 ter bevordering van het vertrouwen in de digitale economie; JORF van 22 juni 2004, blz. 11168; hierna: 'LCEN') bepaalt:

'I. 1. Personen van wie de activiteit erin bestaat het publiek online toegang te verlenen tot communicatiediensten, stellen hun abonnees ervan in kennis dat er technische middelen bestaan om de toegang tot bepaalde diensten te beperken of om bepaalde diensten te selecteren, en bieden hun abonnees ten minste een van die middelen aan.

[…]

2. Natuurlijke of rechtspersonen die, zelfs gratis, zorgen voor de opslag van signalen, geschriften, beelden, geluiden of berichten van om het even welke aard die door de afnemers van openbare online communicatiediensten worden aangeleverd, om deze via deze diensten ter beschikking te stellen van het publiek, kunnen niet civielrechtelijk aansprakelijk worden gesteld voor de activiteiten of de op verzoek van een afnemer van die diensten opgeslagen informatie, indien zij niet daadwerkelijk kennis hadden van het onwettige karakter daarvan of van feiten of informatie waaruit dat onwettige karakter duidelijk bleek, of indien zij, zodra zij daadwerkelijk van het bovenbedoelde kennis hadden, prompt hebben gehandeld om die gegevens te verwijderen of de toegang daartoe onmogelijk te maken.

[…]

II. De in lid I, punten 1 en 2, genoemde personen beheren en bewaren de gegevens zodanig dat het mogelijk is eenieder te identificeren die heeft bijgedragen tot de creatie van de inhoud of een deel van de inhoud van de diensten waarvan zij aanbieder zijn.

Zij verstrekken aan de personen die een openbare online communicatiedienst verlenen, technische middelen die hen in staat stellen om aan de in lid III genoemde identificatievoorwaarden te voldoen.

De rechterlijke autoriteit kan de in lid I, punten 1 en 2, genoemde dienstverleners verzoeken om de in de eerste alinea bedoelde gegevens mee te delen.

De artikelen 226-17, 226-21 en 226-22 van de code pénal zijn van toepassing op de verwerking van die gegevens.

Bij decreet vastgesteld na advies van de Conseil d'État en van de nationale commissie voor informatica en vrijheden, worden de in de eerste alinea bedoelde gegevens gedefinieerd en wordt vastgesteld hoelang en op welke wijze zij worden bewaard.

[…]'

Decreet nr. 2011-219

50 Hoofdstuk I van decreet nr. 2011-219, dat is vastgesteld op grond van artikel 6, lid II, laatste alinea, LCEN, bevat de artikelen 1 tot en met 4 van dit decreet.

51 Artikel 1 van decreet nr. 2011-219 bepaalt:

'De in artikel 6, lid II, [LCEN] genoemde en op grond van deze bepaling te bewaren gegevens zijn:

1o voor de in artikel 6, lid I, punt 1, genoemde personen en voor elke verbinding van hun abonnees:

a) de identificator van de verbinding;

b) de door die personen aan de abonnee toegekende identificator;

c) de identificator van de voor de verbinding gebruikte eindapparatuur, wanneer deze voor die personen toegankelijk is;

d) de datum en het tijdstip van het begin en het einde van de verbinding;

e) de kenmerken van de lijn van de abonnee;

2o voor de in artikel 6, lid I, punt 2, genoemde personen en voor elke creatie:

a) de identificator van de verbinding aan de oorsprong van de communicatie;

b) de identificator die door het informatiesysteem is toegekend aan de inhoud die het voorwerp van de verrichting is;

c) de soorten protocollen die zijn gebruikt voor de verbinding met de dienst en voor de overdracht van de inhoud;

d) de aard van de verrichting;

e) de datum en het tijdstip van de verrichting;

f) de identificator die is gebruikt door de auteur van de verrichting, voor zover deze door die auteur is verstrekt;

3o voor de in artikel 6, lid I, punten 1 en 2, genoemde personen, de informatie die door een gebruiker is verstrekt bij het ondertekenen van een contract of het aanmaken van een account:

a) de identificator van de verbinding bij het aanmaken van het account;

b) de naam, achternaam of bedrijfsnaam;

c) de bijbehorende postadressen;
d) de gebruikte pseudoniemen;
e) de bijbehorende e-mail- of accountadressen;
f) de telefoonnummers;
g) het bijgewerkte wachtwoord en de bijgewerkte gegevens voor de verificatie of wijziging ervan;
4o voor de in artikel 6, lid I, punten 1 en 2, genoemde personen, wanneer voor het sluiten van het contract of het aanmaken van het account een vergoeding verschuldigd is, de volgende betalingsgegevens voor elke betalingstransactie:
a) de gebruikte betalingswijze;
b) de betalingsreferentie;
c) het bedrag;
d) de datum en het tijdstip van de transactie.
De onder 3° en 4° genoemde gegevens hoeven slechts te worden bewaard voor zover de betrokken personen deze gegevens plegen te verzamelen.'

52 Artikel 2 van decreet nr. 2011-219 luidt als volgt:
'Het bijdragen aan de creatie van inhoud omvat de volgende verrichtingen:
a) de oorspronkelijke creatie van inhoud;
b) wijzigingen van inhoud en van daarmee verband houdende gegevens;
c) verwijdering van inhoud.'

53 Artikel 3 van dat decreet bepaalt:
'De bewaartermijn voor de in artikel 1 genoemde gegevens bedraagt één jaar:
a) in het geval van de onder 1° en 2° genoemde gegevens te rekenen vanaf de dag waarop de inhoud is gecreëerd, voor elke verrichting die heeft bijgedragen aan de creatie van inhoud, zoals gedefinieerd in artikel 2;
b) in het geval van de onder 3° genoemde gegevens te rekenen vanaf de dag waarop het contract is beëindigd of het account is opgeheven;
c) in het geval van de onder 4° genoemde gegevens te rekenen vanaf de datum waarop de factuur is uitgereikt of de betalingstransactie heeft plaatsgevonden, voor elke factuur of betalingstransactie.'

Belgisch recht

54 Bij de wet van 29 mei 2016 zijn met name wijzigingen aangebracht in de wet van 13 juni 2005 betreffende de elektronische communicatie (*Belgisch Staatsblad*, 20 juni 2005, blz. 28070; hierna: 'wet van 13 juni 2005'), het Wetboek van strafvordering en de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (*Belgisch Staatsblad*, 18 december 1998, blz. 40312; hierna: 'wet van 30 november 1998').

55 Artikel 126 van de wet van 13 juni 2005, zoals gewijzigd bij de wet van 29 mei 2016, bepaalt:
'1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, dienen de aanbieders aan het publiek van telefoniediensten, via internet inbegrepen, van internettoegang, van e-mail via het internet, de operatoren die openbare elektronischecommunicatienetwerken aanbieden, alsook de operatoren die een van deze diensten verstrekken, de in paragraaf 3 bedoelde gegevens die door hen worden gegenereerd of verwerkt in het kader van de verstrekking van de betrokken communicatiediensten, te bewaren.
Dit artikel heeft geen betrekking op de inhoud van de communicatie.
De verplichting om de in paragraaf 3 bedoelde gegevens te bewaren, is ook van toepassing op oproeppogingen zonder resultaat, voor zover die gegevens in verband met de aanbieding van de bedoelde communicatiediensten:
1o wat de telefoniegegevens betreft, worden gegenereerd of verwerkt door de operatoren van openbare elektronischecommunicatiediensten of van een openbaar netwerk voor elektronische communicatie, of
2o wat de internetgegevens betreft, door deze aanbieders worden gelogd.
'2. Enkel de volgende overheden mogen op eenvoudig verzoek van de in paragraaf 1, eerste lid, bedoelde aanbieders en operatoren gegevens ontvangen die worden bewaard krachtens dit artikel om de doeleinden en volgens de hieronder opgesomde voorwaarden:
1o de gerechtelijke autoriteiten, met het oog op het opsporen, het onderzoek en de vervolging van inbreuken, voor de uitvoering van de in de artikelen 46bis en 88bis van het Wetboek van strafvordering beoogde maatregelen en volgens de voorwaarden bepaald in die artikelen;
2o de inlichtingen- en veiligheidsdiensten, teneinde de inlichtingenopdrachten met inzet van de methoden voor het vergaren van gegevens zoals bedoeld in de artikelen 16/2, 18/7 en 18/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten te vervullen en volgens de voorwaarden vastgelegd in die wet;
3o elke officier van gerechtelijke politie van het [Belgisch Instituut voor postdiensten en telecommunicatie (hierna: 'Instituut')], met het oog op het opsporen, het onderzoek en de vervolging van inbreuken op de artikelen 114, 124 en dit artikel;
4o de hulpdiensten die hulp ter plaatse bieden, wanneer ze naar aanleiding van een noodoproep, van de betrokken aanbieder of operator niet de identificatiegegevens van de oproeper ontvangen met behulp van de databank beoogd in artikel 107, § 2, derde lid, of onvolledige of onjuiste gegevens krijgen. Enkel de identificatiegegevens van de oproeper mogen worden

gevraagd en uiterlijk binnen 24 uur na de oproep;

5o de officier van gerechtelijke politie van de Cel Vermiste Personen van de federale politie, in het kader van zijn opdracht tot het verlenen van hulp aan personen in nood, opsporing van personen van wie de verdwijning onrustwekkend is en wanneer er ernstige vermoedens of aanwijzingen bestaan dat de fysieke integriteit van de vermiste persoon in onmiddellijk gevaar is. Enkel de gegevens die zijn beoogd in paragraaf 3, eerste en tweede lid, met betrekking tot de vermiste persoon en bewaard gedurende de 48 uur voorafgaand aan het verzoek om de gegevens te krijgen, mogen worden gevraagd aan de operator of de aanbieder in kwestie via een door de Koning aangewezen politiedienst;

6o de Ombudsdienst voor telecommunicatie, met het oog op de identificatie van de persoon die kwaadwillig gebruik heeft gemaakt van een elektronischecommunicatienetwerk of -dienst, conform de voorwaarden beoogd in artikel 43bis, § 3, 7°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven. Enkel de identificatiegegevens mogen worden gevraagd.

De aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, zorgen ervoor dat de in paragraaf 3 bedoelde gegevens onbeperkt toegankelijk zijn vanuit België en dat deze gegevens, en alle andere daarmee verband houdende vereiste informatie onverwijld en uitsluitend aan de in deze paragraaf bedoelde autoriteiten kunnen worden meegedeeld.

Onverminderd andere wettelijke voorschriften mogen de aanbieders en operatoren bedoeld in paragraaf 1, eerste lid, de krachtens paragraaf 3 bewaarde gegevens niet gebruiken voor andere doeleinden.

'3. De gegevens ter identificatie van de gebruiker of de abonnee en de communicatiemiddelen, met uitzondering van de gegevens waarin het tweede en derde lid specifiek voorzien, worden gedurende twaalf maanden bewaard vanaf de datum waarop communicatie voor de laatste maal mogelijk is via de gebruikte dienst.

De gegevens met betrekking tot de toegang tot en de verbinding van de eindapparatuur met het netwerk en met de dienst en met betrekking tot de plaats van die apparatuur, inclusief het netwerkaansluitpunt, worden bewaard gedurende twaalf maanden, vanaf de datum van de communicatie.

De communicatiegegevens, met uitzondering van de inhoud, met inbegrip van hun herkomst en hun bestemming, worden gedurende twaalf maanden bewaard vanaf de datum van de communicatie.

De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, op voorstel van de minister van Justitie en van de minister [die bevoegd is voor elektronische communicatie], en na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer en van het Instituut, de te bewaren gegevens per type van categorie bedoeld in het eerste tot derde lid alsook de vereisten waaraan deze gegevens moeten beantwoorden.

[…]'

Hoofdgedingen en prejudiciële vragen

Zaak C-511/18

56 Bij verzoekschriften die op 30 november 2015 en 16 maart 2016 zijn ingediend en die in de procedure in het hoofdgeding zijn gevoegd, hebben La Quadrature du Net, French Data Network, de Fédération des fournisseurs d'accès à Internet associatifs en Igwan.net bij de Conseil d'État nietigverklaring gevorderd van decreten nr. 2015-1185, nr. 2015-1211, nr. 2015-1639 en nr. 2016-67, met name omdat zij deze decreten in strijd achten met de Franse grondwet, het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: 'EVRM') en de richtlijnen 2000/31 en 2002/58, gelezen in het licht van de artikelen 7, 8 en 47 van het Handvest.

57 Wat in het bijzonder de middelen inzake schending van richtlijn 2000/31 betreft, merkt de verwijzende rechter op dat artikel L. 851-3 CSI aan exploitanten van elektronischecommunicatiemiddelen en technische dienstverleners de verplichting oplegt om 'op hun netwerken geautomatiseerde verwerkingen uit te voeren die bedoeld zijn om, in overeenstemming met in de machtiging bepaalde parameters, verbindingen op te sporen waaruit een terroristische dreiging zou kunnen blijken'. Deze techniek is volgens de verwijzende rechter bedoeld om gedurende een beperkte periode van alle door die exploitanten en dienstverleners verwerkte verbindingsgegevens de gegevens op te vragen die in verband kunnen worden gebracht met een dergelijk ernstig misdrijf. De verwijzende rechter meent dan ook dat artikel L 851-3 CSI, dat niet voorziet in een algemene verplichting om actief toezicht uit te oefenen, niet in strijd is met artikel 15 van richtlijn 2000/31.

58 Wat de middelen inzake schending van richtlijn 2002/58 betreft, is de verwijzende rechter van mening dat met name uit de bepalingen van deze richtlijn en uit het arrest van 21 december 2016, *Tele2 Sverige en Watson e.a.* (C-203/15 en C-698/15, EU:C:2016:970; hierna: 'arrest *Tele2*' (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)), volgt dat nationale bepalingen waarbij aan aanbieders van elektronischecommunicatiediensten verplichtingen worden opgelegd, zoals een verplichting tot algemene en ongedifferentieerde bewaring van de verkeers- en locatiegegevens van hun gebruikers en abonnees voor de in artikel 15, lid 1, van die richtlijn genoemde doeleinden, waaronder de bescherming van de nationale veiligheid, de landsverdediging en de openbare veiligheid, binnen de werkingssfeer van die richtlijn vallen voor zover zij de activiteit van die aanbieders regelen. Volgens de verwijzende rechter

geldt hetzelfde voor bepalingen die de toegang van de nationale autoriteiten tot de betrokken gegevens en het gebruik ervan regelen.

59 De verwijzende rechter leidt daaruit af dat zowel de uit artikel L. 851-1 CSI voortvloeiende bewaarplicht als de in de artikelen L.851-1, L.851-2 en L.851-4 van dat wetboek geregelde administratieve toegang tot die gegevens, ook in real time, binnen de werkingssfeer van richtlijn 2002/58 valt. Volgens de verwijzende rechter geldt hetzelfde voor artikel L. 851-3 CSI, dat weliswaar aan de betrokken aanbieders geen algemene bewaarplicht oplegt, maar wel van hen verlangt dat zij op hun netwerken geautomatiseerde verwerkingen uitvoeren die erop gericht zijn verbindingen op te sporen die kunnen wijzen op een terroristische dreiging.

60 De verwijzende rechter is daarentegen van mening dat richtlijn 2002/58 niet van toepassing is op de bestreden bepalingen van de CSI die betrekking hebben op technieken voor het inwinnen van inlichtingen die rechtstreeks door de staat worden toegepast en die niet de activiteiten van aanbieders van elektronischecommunicatiediensten regelen door aan deze aanbieders specifieke verplichtingen op te leggen. Die bepalingen kunnen volgens de verwijzende rechter dus niet worden geacht uitvoering te geven aan het Unierecht, zodat de middelen volgens welke die bepalingen in strijd zijn met richtlijn 2002/58, niet met succes kunnen worden aangevoerd.

61 Met het oog op de beslechting van de geschillen over de rechtmatigheid van decreten nr. 2015-1185, nr. 2015-2011, nr. 2015-1639 en nr. 2016-67 in het licht van richtlijn 2002/58, voor zover deze zijn vastgesteld ter uitvoering van de artikelen L. 851-1 tot en met 851-4 CSI, moeten volgens de verwijzende rechter dan ook drie vragen betreffende de uitlegging van het Unierecht worden beantwoord.

62 Wat de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 betreft, vraagt de verwijzende rechter zich in de eerste plaats af of een op grond van de artikelen L. 851-1 en R. 851-5 CSI aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting tot algemene en ongedifferentieerde bewaring, met name gelet op de waarborgen en controles waarmee de administratieve toegang tot verbindingsgegevens en het gebruik van die gegevens zijn omgeven, niet moet worden beschouwd als een inmenging die haar rechtvaardiging vindt in het door artikel 6 van het Handvest gewaarborgde recht op veiligheid en in de vereisten van nationale veiligheid, waarvoor de verantwoordelijkheid krachtens artikel 4 VEU uitsluitend op de lidstaten rust.

63 Wat in de tweede plaats de andere verplichtingen betreft die aan aanbieders van elektronischecommunicatiediensten kunnen worden opgelegd, merkt de verwijzende rechter op dat op grond van artikel L. 851-2 CSI de in artikel L. 851-1 van dit wetboek bedoelde informatie of documenten uitsluitend ter voorkoming van terrorisme kunnen worden opgevraagd bij dezelfde personen. Deze opvraging, die slechts betrekking heeft op een of meer personen die eerder zijn geïdentificeerd als personen die in verband kunnen worden gebracht met een terroristische dreiging, wordt in real time uitgevoerd. Dit geldt volgende verwijzende rechter ook voor artikel L. 851-4 CSI, op grond waarvan exploitanten enkel technische gegevens over de locatie van de eindapparatuur in real time mogen doorgeven. Die technieken regelen voor verschillende doeleinden en op verschillende manieren de administratieve toegang in real time tot de op grond van de CPCE en de LCEN bewaarde gegevens, zonder dat aan de betrokken aanbieders een extra bewaarplicht wordt opgelegd naast wat noodzakelijk is voor de facturering en de levering van hun diensten. Ook artikel L. 851-3 CSI, dat voorziet in een verplichting voor de betrokken aanbieders om op hun netwerken een geautomatiseerde analyse van de verbindingen uit te voeren, impliceert volgens de verwijzende rechter geen algemene en ongedifferentieerde gegevensbewaring.

64 De verwijzende rechter is van oordeel dat in een context die wordt gekenmerkt door ernstige en aanhoudende bedreigingen voor de nationale veiligheid, met name door terreurgevaar, zowel de algemene en ongedifferentieerde bewaring als de toegang in real time tot de verbindingsgegevens een ongekend operationeel nut opleveren. Dankzij de algemene en ongedifferentieerde bewaring kunnen de inlichtingendiensten immers toegang krijgen tot de communicatiegegevens van een persoon voordat de redenen zijn vastgesteld om aan te nemen dat die persoon een bedreiging vormt voor de openbare veiligheid, de landsverdediging of de staatsveiligheid, en dankzij de toegang in real time tot de verbindingsgegevens kan het gedrag van personen die een onmiddellijke bedreiging voor de openbare orde kunnen vormen, met een hoog niveau van alertheid in de gaten worden gehouden.

65 Voorts maakt de in artikel L. 851-3 CSI genoemde techniek het volgens de verwijzende rechter mogelijk om aan de hand van daartoe nauwkeurig vastgestelde criteria personen op te sporen van wie het gedrag, gelet op hun communicatiemethoden, een terroristische dreiging aan het licht kan brengen.

66 Wat in de derde plaats de toegang van de bevoegde autoriteiten tot de bewaarde gegevens betreft, vraagt de verwijzende rechter zich af of richtlijn 2002/58, gelezen in het licht van het Handvest, aldus moet worden uitgelegd dat zij de regelmatigheid van de procedures voor het opvragen van verbindingsgegevens in alle gevallen afhankelijk stelt van het vereiste om de betrokken personen te informeren wanneer een dergelijke kennisgeving het onderzoek van de bevoegde autoriteiten niet langer in gevaar kan brengen, dan wel of dergelijke procedures als regelmatig kunnen worden beschouwd gelet op alle andere procedurele waarborgen waarin het nationale recht voorziet, wanneer deze waarborgen de doeltreffendheid van het recht op beroep garanderen.

67 Met betrekking tot die andere procedurele waarborgen merkt de verwijzende rechter met name op dat eenieder die zich ervan wil vergewissen dat er niet op onregelmatige wijze inlichtingentechnieken jegens hem zijn toegepast, zich kan wenden tot een speciale formatie van de Conseil d'État, die tot taak heeft om aan de hand van de in het kader van een niet-contradictoire procedure aan hem verstrekte informatie na te gaan of jegens de verzoeker een techniek is toegepast, en zo ja, of daarbij de bepalingen van boek VIII CSI in acht zijn genomen. De bevoegdheden waarover die formatie bij de beoordeling van de ingediende verzoeken beschikt, waarborgen volgens de verwijzende rechter de doeltreffendheid van de door haar uitgevoerde rechterlijke toetsing. Zo is die formatie bevoegd om de verzoeken te onderzoeken, alle onrechtmatigheden die zij vaststelt ambtshalve op te werpen, en de autoriteiten te gelasten alle passende maatregelen te nemen om een einde te maken aan de vastgestelde onrechtmatigheden. Voorts is het de taak van de nationale commissie voor toezicht op inlichtingentechnieken om na te gaan of de technieken voor het inwinnen van inlichtingen op het nationale grondgebied worden toegepast in overeenstemming met de vereisten die voortvloeien uit de CSI. De omstandigheid dat de in het hoofdgeding aan de orde zijnde wettelijke bepalingen niet voorschrijven dat personen jegens wie surveillancemaatregelen worden toegepast, daarover worden geïnformeerd, levert volgens de verwijzende rechter dan ook op zichzelf geen buitensporige aantasting op van het recht op eerbiediging van het privéleven.

68 In deze omstandigheden heeft de Conseil d'État de behandeling van de zaak geschorst en het Hof verzocht om een prejudiciële beslissing over de volgende vragen:

'1) Moet de verplichting tot algemene en ongedifferentieerde bewaring die rust op de aanbieders op grond van de permissieve bepalingen van artikel 15, lid 1, van [richtlijn 2002/58], in een context die wordt gekenmerkt door ernstige en aanhoudende bedreigingen voor de nationale veiligheid, en met name door terreurgevaar, worden beschouwd als een inmenging die wordt gerechtvaardigd door het recht op veiligheid als gewaarborgd door artikel 6 van [het Handvest], en door de vereisten van nationale veiligheid, waarvoor de verantwoordelijkheid krachtens artikel 4 [VEU] uitsluitend op de lidstaten rust?

2) Dient [richtlijn 2002/58], gelezen in het licht van [het Handvest], aldus te worden uitgelegd dat zij het mogelijk maakt om wetgevende maatregelen te nemen, zoals maatregelen voor het in real time opvragen van verkeers- en locatiegegevens van welbepaalde personen, die weliswaar van invloed zijn op de rechten en verplichtingen van de aanbieders van een elektronischecommunicatiedienst, maar hun geen specifieke verplichting opleggen tot bewaring van hun gegevens?

3) Moet [richtlijn 2002/58], gelezen in het licht van [het Handvest], aldus worden uitgelegd dat zij de regelmatigheid van de procedures voor het opvragen van verbindingsgegevens in alle gevallen afhankelijk stelt van het vereiste om de betrokken personen te informeren wanneer dergelijke informatie het onderzoek van de bevoegde autoriteiten niet langer in gevaar kan brengen, of kunnen dergelijke procedures als regelmatig worden beschouwd gelet op alle andere bestaande procedurele waarborgen, wanneer deze waarborgen de doeltreffendheid van het recht op beroep garanderen?'

Zaak C-512/18

69 Bij een op 1 september 2015 ingediend verzoekschrift hebben French Data Network, La Quadrature du Net en de Fédération des fournisseurs d'accès à Internet associatifs bij de Conseil d'État nietigverklaring gevorderd van het stilzwijgende besluit van de eerste minister tot afwijzing van hun verzoek tot intrekking van artikel R. 10-13 CPCE en decreet nr. 2011-219, met name wegens strijdigheid met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 van het Handvest. Privacy International en het Center for Democracy and Technology zijn toegelaten tot interventie in het hoofdgeding.

70 Met betrekking tot artikel R. 10-13 CPCE en de daarin neergelegde verplichting tot algemene en ongedifferentieerde bewaring van communicatiegegevens merkt de verwijzende rechter — die vergelijkbare overwegingen formuleert als in zaak C-511/18 — op dat een dergelijke bewaring de gerechtelijke autoriteit in staat stelt toegang te krijgen tot gegevens inzake de communicatie van een persoon nog voordat deze ervan wordt verdacht een strafbaar feit te hebben gepleegd, zodat die bewaring ongekend nuttig is voor het onderzoeken, vaststellen en vervolgen van strafbare feiten.

71 Wat decreet nr. 2011-219 betreft, is de verwijzende rechter van mening dat artikel 6, punt II, LCEN, waarbij uitsluitend voor gegevens inzake de creatie van inhoud een bewaarplicht wordt opgelegd, niet binnen de werkingssfeer valt van richtlijn 2002/58, die immers volgens artikel 3, lid 1, ervan enkel van toepassing is op de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de Unie, maar binnen de werkingssfeer van richtlijn 2000/31.

72 Volgens de verwijzende rechter volgt evenwel uit artikel 15, leden 1 en 2, van richtlijn 2000/31 dat deze richtlijn geen principieel verbod stelt op het bewaren van gegevens inzake de creatie van inhoud waarvan slechts bij wijze van uitzondering zou kunnen worden afgeweken. Naar het oordeel van de verwijzende rechter rijst dan ook de vraag of de artikelen 12, 14 en 15 van richtlijn 2002/31, gelezen in het licht van de artikelen 6 tot en met 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moeten worden uitgelegd dat zij een lidstaat toestaan een nationale regeling in te voeren als die van artikel 6, lid II, LCEN, op grond waarvan de betrokken personen verplicht zijn om de gegevens te bewaren die het mogelijk maken om eenieder te identificeren die heeft bijgedragen tot de creatie van

de inhoud of van om het even welke inhoud van de diensten waarvan zij aanbieder zijn, opdat de gerechtelijke autoriteit in voorkomend geval om mededeling ervan kan verzoeken teneinde de regels inzake burgerlijke of strafrechtelijke aansprakelijkheid te doen naleven.

73 In deze omstandigheden heeft de Conseil d'État de behandeling van de zaak geschorst en het Hof verzocht om een prejudiciële beslissing over de volgende vragen:

'1) Moet de verplichting tot algemene en ongedifferentieerde bewaring die rust op de aanbieders op grond van de permissieve bepalingen van artikel 15, lid 1, van [richtlijn 2002/58], met name gelet op de waarborgen en controles die vervolgens gelden voor zowel het opvragen als het gebruiken van die verbindingsgegevens, worden beschouwd als een inmenging die wordt gerechtvaardigd door het recht op veiligheid als gewaarborgd door artikel 6 van [het Handvest] en door de vereisten van nationale veiligheid, waarvoor de verantwoordelijkheid krachtens artikel 4 [VEU] uitsluitend op de lidstaten rust?

2) Moeten de bepalingen van [richtlijn 2000/31], gelezen tegen de achtergrond van de artikelen 6, 7, 8 en 11 alsook van artikel 52, lid 1, van [het Handvest], aldus worden uitgelegd dat zij toestaan dat een staat een nationale regeling invoert die de personen van wie de activiteit erin bestaat online toegang tot communicatiediensten aan het publiek aan te bieden, en de natuurlijke of rechtspersonen die, zelfs gratis, met het oog op de terbeschikkingstelling aan het publiek door het aanbieden van online communicatiediensten aan het publiek zorgen voor de opslag van door de afnemers van die diensten aangeleverde signalen, geschriften, beelden, geluiden of berichten van om het even welke aard, verplicht om gegevens te bewaren die het mogelijk maken om eenieder te identificeren die heeft bijgedragen tot de creatie van de inhoud of van om het even welke inhoud van de diensten waarvan zij aanbieder zijn, zodat de gerechtelijke autoriteit in voorkomend geval om mededeling ervan kan verzoeken om de regels inzake burgerlijke of strafrechtelijke aansprakelijkheid te doen naleven?'

Zaak C-520/18

74 Bij verzoekschriften die op 10 januari, 16 januari, 17 januari en 18 januari 2017 zijn ingediend en die in de procedure in het hoofdgeding zijn gevoegd, hebben de Ordre des barreaux francophones et germanophone, de Académie Fiscale ASBL en UA, de Liga voor Mensenrechten VZW en de Ligue des Droits de l'Homme ASBL, alsmede VZ, WY en XX bij het Grondwettelijk Hof (België) beroepen tot vernietiging van de wet van 29 mei 2016 ingesteld, omdat deze wet in hun ogen in strijd is met de artikelen 10 en 11 van de Belgische grondwet, gelezen in samenhang met de artikelen 5, 6 tot en met 11, 14, 15, 17 en 18 EVRM, met de artikelen 7, 8, 11 en 47 en artikel 52, lid 1, van het Handvest, met artikel 17 van het op 16 december 1966 door de Algemene Vergadering van de Verenigde Naties aangenomen en op 23 maart 1976 in werking getreden Internationaal Verdrag inzake burgerrechten en politieke rechten, met de algemene beginselen van rechtszekerheid, evenredigheid en zelfbeschikking op informatiegebied, en met artikel 5, lid 4, VEU.

75 Verzoekers in het hoofdgeding voeren ter ondersteuning van hun beroepen in wezen aan dat de wet van 29 mei 2016 met name onrechtmatig is omdat zij de grenzen van het strikt noodzakelijke overschrijdt en onvoldoende waarborgen biedt op het vlak van bescherming. Zij stellen in het bijzonder dat noch de in de wet opgenomen bepalingen betreffende de bewaring van gegevens, noch die welke de toegang van de autoriteiten tot de bewaarde gegevens regelen, voldoen aan de vereisten die voortvloeien uit het arrest van 8 april 2014, *Digital Rights Ireland e.a.* (C-293/12 en C-594/12, EU:C:2014:238; hierna: 'Arrest *Digital Rights*' (*NJ* 2016/446, m.nt. E.J. Dommering*; red.*)), en het arrest van 21 december 2016, *Tele2* (C-203/15 en C-698/15, EU:C:2016:970 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)). Volgens verzoekers houden die bepalingen in het hoofdgeding namelijk het risico in dat persoonlijkheidsprofielen worden opgesteld waarvan de bevoegde autoriteiten misbruik zouden kunnen maken, en voorzien zij niet in een passend niveau van beveiliging en bescherming van de bewaarde gegevens. Verzoekers in het hoofdgeding stellen tot slot dat de betrokken wet ook van toepassing is op personen voor wie het beroepsgeheim of een vertrouwelijkheidsplicht geldt, en betrekking heeft op communicatiegegevens die gevoelige persoonsgegevens zijn, terwijl zij niet voorziet in bijzondere waarborgen om deze gegevens te beschermen.

76 De verwijzende rechter merkt op dat de gegevens die op grond van de wet van 29 mei 2016 moeten worden bewaard door de aanbieders van telefoniediensten, ook via internet, van internettoegang en van e-mail via het internet, en door de exploitanten van openbare elektronischecommunicatienetwerken, identiek zijn aan die welke worden genoemd in richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronischecommunicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (*PB* 2006, L 105, blz. 54), zonder dat enig onderscheid wordt gemaakt naargelang van de betrokken personen of naargelang van het nagestreefde doel. Met betrekking tot dit laatste punt wijst de verwijzende rechter erop dat de wetgever met de wet van 29 mei 2016 niet alleen terrorisme en kinderpornografie heeft willen bestrijden, maar het ook mogelijk heeft willen maken de bewaarde gegevens te gebruiken in zeer veel verschillende situaties in het kader van strafrechtelijke onderzoeken. De verwijzende rechter stelt bovendien vast dat uit de memorie van toelichting van die wet blijkt dat de nationale wetgever invoering van een gerichte en gedifferenti-

eerde bewaarplicht in het licht van de nagestreefde doelstelling niet mogelijk heeft geacht en ervoor heeft gekozen om de algemene en ongedifferentieerde bewaarplicht met strikte waarborgen te omgeven, zowel op het vlak van de bewaring van de gegevens als op het vlak van de toegang ertoe, teneinde de inmenging in het recht op bescherming van de persoonlijke levenssfeer tot een minimum te beperken.

77 De verwijzende rechter voegt daaraan toe dat artikel 126, lid 2, 1° en 2°, van de wet van 13 juni 2005, zoals gewijzigd bij de wet van 29 mei 2016, de voorwaarden bepaalt waaronder de gerechtelijke autoriteiten respectievelijk de inlichtingen- en veiligheidsdiensten toegang kunnen krijgen tot de bewaarde gegevens, zodat het onderzoek of die wet in overeenstemming is met de vereisten die voortvloeien uit het Unierecht, moet worden opgeschort totdat het Hof uitspraak zal hebben gedaan in twee bij hem aanhangige prejudiciële procedures die gaan over een dergelijke toegang.

78 De verwijzende rechter merkt tot slot op dat de wet van 29 mei 2016 een effectief strafrechtelijk onderzoek naar en een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk beoogt te maken en het daarnaast mogelijk wil maken om de pleger van een dergelijk misdrijf te identificeren, ook wanneer wordt gebruikgemaakt van elektronischecommunicatiemiddelen. Tijdens de bij de verwijzende rechter aanhangige procedure zou in dit verband zijn gewezen op de positieve verplichtingen die voortvloeien uit de artikelen 3 en 8 EVRM. Die verplichtingen zouden volgens de verwijzende rechter ook kunnen voortvloeien uit de overeenkomstige bepalingen van het Handvest, wat gevolgen zou kunnen hebben voor de uitlegging van artikel 15, lid 1, van richtlijn 2002/58.

79 In deze omstandigheden heeft het Grondwettelijk Hof de behandeling van de zaak geschorst en het Hof verzocht om een prejudiciële beslissing over de volgende vragen:

‘1) Dient artikel 15, lid 1, van [richtlijn 2002/58], in samenhang gelezen met het recht op veiligheid, gewaarborgd bij artikel 6 van [het Handvest], en het recht op eerbiediging van de persoonsgegevens, zoals gewaarborgd bij de artikelen 7 en 8 en artikel 52, lid 1, van [het Handvest], in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronischecommunicatiediensten om de verkeers- en locatiegegevens in de zin van [richtlijn 2002/58] die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, nationale regeling die niet alleen ten doel heeft het onderzoeken, opsporen en vervolgen van feiten van zware criminaliteit, maar ook het waarborgen van de nationale veiligheid, de verdediging van het grondgebied en van de openbare veiligheid, het onderzoeken, opsporen en vervolgen van andere feiten dan die van zware criminaliteit of het voorkomen van een verboden gebruik van de elektronischecommunicatiesystemen, of de verwezenlijking van een andere doelstelling die is geïdentificeerd bij artikel 23, lid 1, van [verordening 2016/679] en die bovendien onderworpen is aan nader in die regeling opgenomen waarborgen op het vlak van de bewaring van de gegevens en van de toegang ertoe?

2) Dient artikel 15, lid 1, van [richtlijn 2002/58], gelezen in samenhang met de artikelen 4, 7, 8 en 11 en artikel 52, lid 1, van [het Handvest], in die zin te worden geïnterpreteerd dat het zich verzet tegen een nationale regeling zoals die welke in het geding is, die voorziet in een algemene verplichting voor de operatoren en aanbieders van elektronischecommunicatiediensten om de verkeers- en locatiegegevens in de zin van [richtlijn 2002/58] die door hen worden gegenereerd of verwerkt in het kader van het aanbieden van die diensten, te bewaren, indien die regeling mede tot doel heeft om de op de overheid rustende positieve verplichtingen ingevolge de artikelen 4 en [7] van het Handvest te bewerkstelligen om te voorzien in een wettelijk kader dat een effectief strafrechtelijk onderzoek en een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk maakt en het effectief mogelijk maakt om de pleger van het misdrijf te identificeren, ook wanneer gebruik wordt gemaakt van elektronischecommunicatiemiddelen?

3) Zou het Grondwettelijk Hof, indien het op grond van het antwoord verstrekt op de eerste of de tweede prejudiciële vraag tot de conclusie zou komen dat de bestreden wet één of meer van de uit de in die vragen vermelde bepalingen voortvloeiende verplichtingen schendt, de gevolgen van [de wet van 29 mei 2016] tijdelijk kunnen handhaven teneinde rechtsonzekerheid te voorkomen en het mogelijk te maken dat de voorheen verzamelde en bewaarde gegevens alsnog kunnen gebruikt worden voor de door de wet beoogde doeleinden?’

Procedure bij het Hof

80 Bij beslissing van de president van het Hof van 25 september 2018 zijn de zaken C-511/18 en C-512/18 gevoegd voor de schriftelijke en de mondelinge behandeling alsmede voor het arrest. Bij beslissing van de president van het Hof van 9 juli 2020 is zaak C-520/18 bij deze zaken gevoegd voor het arrest.

Prejudiciële vragen

Eerste vraag in de zaken C-511/18 en C-512/18 en eerste en tweede vraag in zaak C-520/18

81 Met de eerste vraag in de zaken C-511/18 en C-512/18 en de eerste en de tweede vraag in zaak C-520/18, die samen moeten worden onderzocht, wensen de verwijzende rechters in wezen te verne-

men of artikel 15, lid 1, van richtlijn 2002/58 aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die voor de in deze bepaling genoemde doeleinden aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens oplegt.

Inleidende opmerkingen

82 Uit de dossiers waarover het Hof beschikt blijkt dat de in de hoofdgedingen aan de orde zijnde regelingen zich uitstrekken tot alle elektronischecommunicatiemiddelen en tot alle gebruikers van die middelen, zonder dat daarbij enig onderscheid of enige uitzondering wordt gemaakt. Verder gaat het bij de gegevens die aanbieders van elektronischecommunicatiediensten op grond van die regelingen dienen te bewaren, met name om de gegevens die nodig zijn om de bron en de bestemming van een communicatie op te sporen, de datum, het tijdstip, de duur en de aard van die communicatie te bepalen, het gebruikte communicatiemateriaal te identificeren en de eindapparatuur en de communicatie te lokaliseren. Tot die gegevens behoren in het bijzonder de naam en het adres van de gebruiker, het telefoonnummer van de beller en het gebelde nummer, en het IP-adres voor de internetdiensten. De inhoud van de communicatie behoort daarentegen niet tot die gegevens.

83 De gegevens die op grond van de in de hoofdgedingen aan de orde zijnde nationale regelingen een jaar lang moeten worden bewaard, maken het dus in het bijzonder mogelijk om na te gaan met wie en met welk middel de gebruiker van een elektronisch communicatiemiddel heeft gecommuniceerd, om de datum, het tijdstip en de duur van de communicatie en de internetverbindingen te bepalen, alsook de plaats waarvandaan die communicatie en die verbindingen tot stand zijn gebracht, en om de eindapparatuur te lokaliseren, zonder dat er noodzakelijkerwijs informatie is overgebracht. Verder kan aan de hand van die gegevens worden achterhaald hoe vaak de gebruiker gedurende een bepaalde periode met bepaalde personen heeft gecommuniceerd. Tot slot lijkt in het geval van de in de zaken C-511/18 en C-512/18 aan de orde zijnde nationale regeling, die ook geldt voor gegevens betreffende het overbrengen van elektronische communicatie via netwerken, ook de aard van de online geraadpleegde informatie te kunnen worden bepaald.

84 Met betrekking tot de nagestreefde doelstellingen moet worden opgemerkt dat de in de zaken C-511/18 en C-512/18 aan de orde zijnde regelingen onder meer gericht zijn op het opsporen, vaststellen en vervolgen van strafbare feiten in het algemeen, het waarborgen van de nationale onafhankelijkheid, de integriteit van het grondgebied en de landsverdediging, de bescherming van de zwaarwegende belangen van het buitenlands beleid, de nakoming door Frankrijk van zijn Europese en internationale verplichtingen, de bescherming van de zwaarwegende economische, industriële en wetenschappelijke belangen van Frankrijk, en de voorkoming van terrorisme, van aanvallen op de republikeinse vorm van de instituties en van collectieve gewelddadigheden die de openbare vrede ernstig ondermijnen. De in zaak C-520/18 centraal staande regeling heeft onder meer het opsporen, onderzoeken en vervolgen van strafbare feiten alsmede het waarborgen van de nationale veiligheid, de verdediging van het grondgebied en de openbare veiligheid tot doel.

85 De verwijzende rechters vragen zich in het bijzonder af welke gevolgen het in artikel 6 van het Handvest verankerde recht op veiligheid kan hebben voor de uitlegging van artikel 15, lid 1, van richtlijn 2002/58. Ook vragen zij zich af of de inmenging die de door de betrokken nationale regelingen voorgeschreven gegevensbewaring vormt in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten als gerechtvaardigd kan worden beschouwd wegens het bestaan van regels die de toegang van de nationale autoriteiten tot de bewaarde gegevens beperken. De Conseil d'État is bovendien van mening dat die vraag ook moet worden beoordeeld in het licht van artikel 4, lid 2, VEU, aangezien zij rijst in een context die wordt gekenmerkt door ernstige en aanhoudende bedreigingen voor de nationale veiligheid. Het Grondwettelijk Hof benadrukt op zijn beurt dat de in zaak C-520/18 aan de orde zijnde nationale regeling ook uitvoering geeft aan de uit de artikelen 4 en 7 van het Handvest voortvloeiende positieve verplichting om te voorzien in een wettelijk kader dat een daadwerkelijke bestraffing van seksueel misbruik van minderjarigen mogelijk maakt.

86 Zowel de Conseil d'État als het Grondwettelijk Hof gaat ervan uit dat de in de hoofdgedingen aan de orde zijnde nationale regelingen betreffende de bewaring van verkeers- en locatiegegevens en de toegang van de nationale autoriteiten tot die gegevens voor in artikel 15, lid 1, van richtlijn 2002/58 genoemde doeleinden, zoals de bescherming van de nationale veiligheid, binnen de werkingssfeer van deze richtlijn vallen. Bepaalde partijen in de hoofdgedingen en enkele van de lidstaten die schriftelijke opmerkingen hebben ingediend bij het Hof, zijn op dit punt echter een andere mening toegedaan, met name als het gaat om de uitlegging van artikel 1, lid 3, van richtlijn 2002/58. Daarom moet om te beginnen worden onderzocht of de betrokken regelingen binnen de werkingssfeer van deze richtlijn vallen.

Werkingssfeer van richtlijn 2002/58

87 La Quadrature du Net, de Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International en het Center for Democracy and Technology voeren in wezen aan dat uit de rechtspraak van het Hof betreffende de werkingssfeer van richtlijn 2002/58 volgt dat deze richtlijn zowel van toepassing is op de bewaring van de gegevens als op de toegang, al dan niet in real time, tot

de bewaarde gegevens. Die partijen zijn namelijk van mening dat, aangezien de doelstelling van bescherming van de nationale veiligheid expliciet vermeld staat in artikel 15, lid 1, van richtlijn 2002/58, het nastreven van die doelstelling niet ertoe leidt dat deze richtlijn niet van toepassing is. Het door de verwijzende rechters genoemde artikel 4, lid 2, VEU doet in hun ogen niet aan dit oordeel af.

88 Met betrekking tot de inlichtingenmaatregelen die door de bevoegde Franse autoriteiten rechtstreeks worden toegepast zonder dat de activiteiten van aanbieders van elektronischecommunicatiediensten worden geregeld doordat hun specifieke verplichtingen worden opgelegd, merkt het Center for Democracy and Technology op dat die maatregelen noodzakelijkerwijs binnen de werkingssfeer van richtlijn 2002/58 en het Handvest vallen, aangezien daarmee wordt afgeweken van het door artikel 5 van deze richtlijn gewaarborgde vertrouwelijkheidsbeginsel. Die maatregelen moeten volgens die partijen dan ook voldoen aan de vereisten die voortvloeien uit artikel 15, lid 1, van richtlijn 2002/58.

89 De regering van het Verenigd Koninkrijk, de Franse, de Tsjechische en de Estse regering, Ierland en de Cypriotische, de Hongaarse, de Poolse en de Zweedse regering stellen daarentegen in wezen dat richtlijn 2002/58 niet van toepassing is op nationale regelingen als die van de hoofdgedingen, aangezien deze tot doel hebben de nationale veiligheid te waarborgen. Die regeringen zijn van mening dat de activiteiten van de inlichtingendiensten behoren tot de essentiële functies van de lidstaten, daar zij verband houden met de handhaving van de openbare orde en de bescherming van de binnenlandse veiligheid en de territoriale integriteit, en dus onder de exclusieve bevoegdheid van de lidstaten vallen, zoals met name uit artikel 4, lid 2, derde zin, VEU volgt.

90 Die regeringen alsmede Ierland verwijzen bovendien naar artikel 1, lid 3, van richtlijn 2002/58, dat volgens hen activiteiten die verband houden met openbare veiligheid, defensie en staatsveiligheid van de werkingssfeer van deze richtlijn uitsluit, zulks in navolging van artikel 3, lid 2, eerste streepje, van richtlijn 95/46. Zij baseren zich in dit verband op de uitlegging die aan laatstgenoemde bepaling is gegeven in het arrest van 30 mei 2006, *Parlement/Raad en Commissie* (C-317/04 en C-318/04, EU:C:2006:346 (*NJ* 2006/309, m.nt. M.R. Mok*; red.*)).

91 In dit verband zij erop gewezen dat richtlijn 2002/58 volgens artikel 1, lid 1, onder meer de nationale regelgeving harmoniseert die nodig is om een gelijk niveau van bescherming van fundamentele rechten en vrijheden — met name het recht op een persoonlijke levenssfeer en vertrouwelijkheid — bij de verwerking van persoonsgegevens in de sector elektronische communicatie te waarborgen.

92 Volgens artikel 1, lid 3, van die richtlijn zijn van de werkingssfeer ervan uitgesloten de 'activiteiten van de staat' op de aldaar bedoelde gebieden, waaronder de activiteiten van de staat op strafrechtelijk gebied en die welke verband houden met openbare veiligheid, defensie en staatsveiligheid, met inbegrip van het economische welzijn van de staat wanneer de activiteit verband houdt met de staatsveiligheid. De in die bepaling als voorbeeld genoemde activiteiten zijn in alle gevallen specifieke activiteiten van staten of overheidsdiensten en hebben niets van doen met de gebieden waarop particulieren activiteiten ontplooien (arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 32 (*NJ* 2020/232, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

93 Voorts bepaalt artikel 3 van richtlijn 2002/58 dat deze richtlijn van toepassing is op de verwerking van persoonsgegevens in verband met de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de Unie, met inbegrip van de openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen (hierna: 'elektronischecommunicatiediensten'). Bijgevolg moet worden aangenomen dat deze richtlijn de activiteiten van de aanbieders van dergelijke diensten regelt (arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 33 (*NJ* 2020/232, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

94 Op grond van artikel 15, lid 1, van richtlijn 2002/58 kunnen de lidstaten in dat kader met inachtneming van de in deze bepaling geformuleerde voorwaarden 'wettelijke maatregelen treffen ter beperking van de reikwijdte van de in de artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten' (arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 71 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)).

95 Artikel 15, lid 1, van richtlijn 2002/58 vooronderstelt noodzakelijkerwijs dat de daarin bedoelde nationale wettelijke maatregelen binnen de werkingssfeer van deze richtlijn vallen, aangezien deze richtlijn uitdrukkelijk bepaalt dat de lidstaten die maatregelen slechts mogen treffen met inachtneming van de in de richtlijn geformuleerde voorwaarden. Bovendien regelen die maatregelen de activiteit van aanbieders van elektronischecommunicatiediensten voor de in die bepaling vermelde doeleinden (arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 34 (*NJ* 2020/232, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

96 Met name op grond van deze overwegingen heeft het Hof geoordeeld dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met artikel 3 van deze richtlijn, aldus moet worden uitgelegd dat binnen de werkingssfeer van deze richtlijn niet alleen wettelijke maatregelen vallen die aanbieders van elektronischecommunicatiediensten de verplichting opleggen om verkeers- en locatiegegevens te bewaren, maar ook wettelijke maatregelen die hun de verplichting opleggen om de bevoegde nationale autoriteiten toegang tot die gegevens te ver-

lenen. Dergelijke wettelijke maatregelen impliceren immers noodzakelijkerwijs dat die aanbieders die gegevens verwerken, en kunnen, voor zover zij de activiteiten van die aanbieders regelen, niet worden gelijkgesteld met de in artikel 1, lid 3, van richtlijn 2002/58 bedoelde specifieke activiteiten van staten (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punten 35 en 37 (*NJ* 2020/232, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

97 Bovendien zou, gelet op de overwegingen in punt 95 van het onderhavige arrest en op de algemene opzet van richtlijn 2002/58, een uitlegging van deze richtlijn volgens welke de in artikel 15, lid 1, ervan bedoelde wettelijke maatregelen van de werkingssfeer van de richtlijn zijn uitgesloten omdat de doelstellingen die dergelijke maatregelen moeten nastreven, grotendeels overeenstemmen met de doelstellingen van de in artikel 1, lid 3, van diezelfde richtlijn bedoelde activiteiten, artikel 15, lid 1, elk nuttig effect ontnemen (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 72 en 73 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)).

98 Bijgevolg kan het begrip 'activiteiten' in artikel 1, lid 3, van richtlijn 2002/58, zoals de advocaat-generaal in wezen heeft opgemerkt in punt 75 van zijn conclusie in de gevoegde zaken *La Quadrature du Net e.a.* (C-511/18 en C-512/18, EU:C:2020:6), niet aldus worden uitgelegd dat daaronder ook de in artikel 15, lid 1, van die richtlijn bedoelde wettelijke maatregelen vallen.

99 Artikel 4, lid 2, VEU, waaraan de in punt 89 van het onderhavige arrest genoemde regeringen hebben gerefereerd, kan niet afdoen aan deze conclusie. Volgens vaste rechtspraak van het Hof staat het immers weliswaar aan de lidstaten om hun wezenlijke veiligheidsbelangen te definiëren en om passende maatregelen te nemen teneinde hun binnenlandse en buitenlandse veiligheid te verzekeren, maar kan het enkele feit dat een nationale maatregel is genomen met het oog op de bescherming van de nationale veiligheid, niet ertoe leiden dat het Unierecht niet van toepassing is en dat de lidstaten worden ontheven van de verplichting om dit recht te eerbiedigen [zie in die zin arresten van 4 juni 2013, *ZZ*, C-300/11, EU:C:2013:363, punt 38 en aldaar aangehaalde rechtspraak; 20 maart 2018, *Commissie/Oostenrijk (Staatsdrukkerij)*, C-187/16, EU:C:2018:194, punten 75 en 76, en 2 april 2020, *Commissie/Polen, Hongarije en Tsjechië (Tijdelijk herplaatsingsmechanisme voor aanvragers van internationale bescherming)*, C-715/17, C-718/17 en C-719/17, EU:C:2020:257, punten 143 en 170].

100 Het is juist dat het Hof in het arrest van 30 mei 2006, *Parlement/Raad en Commissie* (C-317/04 en C-318/04, EU:C:2006:346, punten 56-59 (*NJ* 2006/309, m.nt. M.R. Mok*; red.*)), heeft geoordeeld dat de doorgifte van persoonsgegevens door luchtvaarmaatschappijen aan overheidsdiensten van een derde land met het oog op het voorkomen en bestrijden van terrorisme en andere ernstige misdrijven, ingevolge artikel 3, lid 2, eerste streepje, van richtlijn 95/46 niet binnen de werkingssfeer van deze richtlijn viel, aangezien die doorgifte geschiedde binnen een door de overheid ingesteld kader dat betrekking had op de openbare veiligheid.

101 Gelet op de overwegingen in de punten 93, 95 en 96 van het onderhavige arrest, kan die rechtspraak echter niet worden toegepast op de uitlegging van artikel 1, lid 3, van richtlijn 2002/58. Zoals de advocaat-generaal in wezen heeft opgemerkt in de punten 70 tot en met 72 van zijn conclusie in de gevoegde zaken *La Quadrature du Net e.a.* (C-511/18 en C-512/18, EU:C:2020:6), sloot artikel 3, lid 2, eerste streepje, van richtlijn 95/46, waarop die rechtspraak betrekking heeft, 'verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de staat' immers in het algemeen van de werkingssfeer van deze richtlijn uit, zonder onderscheid te maken naar de persoon die de gegevensverwerkingshandeling uitvoerde. In het kader van de uitlegging van artikel 1, lid 3, van richtlijn 2002/58 moet dat onderscheid echter wel worden gemaakt. Zoals uit de punten 94 tot en met 97 van het onderhavige arrest blijkt, valt immers elke verwerking van persoonsgegevens door aanbieders van elektronischecommunicatiediensten binnen de werkingssfeer van die richtlijn, inclusief de verwerking die het gevolg is van door de overheid aan die aanbieders opgelegde verplichtingen, terwijl laatstgenoemde verwerking eventueel onder de uitzondering kon vallen van artikel 3, lid 2, eerste streepje, van richtlijn 95/46, gelet op de ruimere formulering van deze bepaling, die zag op elke verwerking die betrekking had op de openbare veiligheid, de defensie of de veiligheid van de staat, ongeacht de persoon die de handeling uitvoerde.

102 Bovendien moet worden opgemerkt dat richtlijn 95/46, die aan de orde was in de zaak die heeft geleid tot het arrest van 30 mei 2006, *Parlement/Raad en Commissie* (C-317/04 en C-318/04, EU:C:2006:346 (*NJ* 2006/309, m.nt. M.R. Mok*; red.*)), overeenkomstig artikel 94, lid 1, van verordening 2016/679 met ingang van 25 mei 2018 is ingetrokken en vervangen door deze verordening. Verordening 2016/679 is volgens artikel 2, lid 2, onder d), weliswaar niet van toepassing op verwerkingen die 'door de bevoegde autoriteiten' worden verricht met het oog op onder meer de voorkoming en de opsporing van strafbare feiten, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, maar uit artikel 23, lid 1, onder d) en h), van deze verordening blijkt dat verwerkingen van persoonsgegevens die voor diezelfde doeleinden worden verricht door particulieren, binnen de werkingssfeer van deze verordening vallen. Hieruit volgt dat bovenstaande uitlegging van artikel 1, lid 3, artikel 3 en artikel 15, lid 1, van richtlijn 2002/58 in overeenstemming is met de afbakening van de werkingssfeer van verordening 2016/679, die door deze richtlijn wordt aangevuld en gespecificeerd.

103 Wanneer de lidstaten daarentegen rechtstreeks maatregelen toepassen die inbreuk maken op het beginsel van de vertrouwelijkheid van elektronische communicatie, zonder dat zij verwerkingsverplichtingen opleggen aan aanbieders van elektronischecommunicatiediensten, wordt de bescherming van de gegevens van de betrokken personen niet beheerst door richtlijn 2002/58, maar uitsluitend door nationaal recht, behoudens de toepassing van richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van kaderbesluit 2008/977/JBZ van de Raad (*PB* 2016, L 119, blz. 89), wat betekent dat de betrokken maatregelen met name in overeenstemming moeten zijn met het nationale constitutionele recht en met de vereisten van het EVRM.

104 Uit het voorgaande volgt dat een nationale regeling die, zoals de in de hoofdgedingen aan de orde zijnde regelingen, ten behoeve van de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot bewaring van verkeers- en locatiegegevens oplegt, binnen de werkingssfeer van richtlijn 2002/58 valt.

Uitlegging van artikel 15, lid 1, van richtlijn 2002/58

105 Vooraf zij eraan herinnerd dat volgens vaste rechtspraak bij de uitlegging van een Unierechtelijke bepaling niet alleen rekening moet worden gehouden met de bewoordingen ervan, maar ook met de context van die bepaling, de doelstellingen van de regeling waarvan zij deel uitmaakt en, met name, de ontstaansgeschiedenis van die regeling (zie in die zin arrest van 17 april 2018, *Egenberger*, C-414/16, EU:C:2018:257, punt 44).

106 Zoals met name uit de overwegingen 6 en 7 van richtlijn 2002/58 volgt, heeft deze richtlijn tot doel om de gebruikers van elektronischecommunicatiediensten te beschermen tegen de gevaren die de nieuwe technologieën en, met name, de steeds grotere mogelijkheden van geautomatiseerde opslag en verwerking van gegevens voor de persoonsgegevens en de persoonlijke levenssfeer van die gebruikers meebrengen. Zoals in overweging 2 van richtlijn 2002/58 wordt verklaard, beoogt deze richtlijn in het bijzonder de volledige eerbiediging van de in de artikelen 7 en 8 van het Handvest bedoelde rechten te waarborgen. Dienaangaande blijkt uit de toelichting bij het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [COM(2000) 385 definitief], waaruit richtlijn 2002/58 is voortgekomen, dat de Uniewetgever heeft willen 'zorgen voor een hoge mate van bescherming van de persoonsgegevens en van de persoonlijke levenssfeer voor alle elektronischecommunicatiediensten, ongeacht de gebruikte technologie'.

107 Daartoe legt artikel 5, lid 1, van richtlijn 2002/58 het beginsel van vertrouwelijkheid van zowel de elektronische communicatie als de daarmee verband houdende verkeersgegevens vast en impliceert het met name dat het anderen dan de gebruikers in beginsel moet worden verboden die communicatie en die gegevens op te slaan, indien de gebruikers daarin niet hebben toegestemd.

108 Wat in het bijzonder de verwerking en de opslag van verkeersgegevens door aanbieders van elektronischecommunicatiediensten betreft, blijkt uit artikel 6 en de overwegingen 22 en 26 van richtlijn 2002/58 dat een dergelijke verwerking slechts is toegestaan voor zover en zolang dat nodig is voor de marketing en de facturering van de diensten en voor de levering van diensten met toegevoegde waarde. Zodra die periode is verstreken, moeten de verwerkte en opgeslagen gegevens worden gewist of geanonimiseerd. Wat de andere locatiegegevens dan de verkeersgegevens betreft, bepaalt artikel 9, lid 1, van richtlijn 2002/58 dat die gegevens slechts onder bepaalde voorwaarden mogen worden verwerkt nadat zij zijn geanonimiseerd of wanneer de gebruikers of abonnees daarvoor hun toestemming hebben gegeven (arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 86 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

109 Met de vaststelling van richtlijn 2002/58 heeft de Uniewetgever dus de in de artikelen 7 en 8 van het Handvest neergelegde rechten geconcretiseerd, zodat de gebruikers van elektronischecommunicatiemiddelen in beginsel erop mogen vertrouwen dat hun communicatie en de daarmee verband houdende gegevens anoniem blijven en niet mogen worden vastgelegd, tenzij zij daarin hebben toegestemd.

110 Artikel 15, lid 1, van richtlijn staat 2002/58 staat de lidstaten echter toe, te voorzien in uitzonderingen op de in artikel 5, lid 1, van deze richtlijn geformuleerde principeverplichting om de vertrouwelijkheid van de persoonsgegevens te waarborgen, en op de met name in de artikelen 6 en 9 van deze richtlijn vermelde overeenkomstige verplichtingen, indien dat in een democratische samenleving een noodzakelijke, redelijke en proportionele maatregel vormt om de nationale veiligheid, de landsverdediging en de openbare veiligheid te waarborgen, of om strafbare feiten of onbevoegd gebruik van het elektronischecommunicatiesysteem te voorkomen, te onderzoeken, op te sporen en te vervolgen. Daartoe kunnen de lidstaten onder meer wettelijke maatregelen treffen om gegevens gedurende een beperkte periode te bewaren indien dat om een van die redenen gerechtvaardigd is.

111 De mogelijkheid om af te wijken van de in de artikelen 5, 6 en 9 van richtlijn 2002/58 vastgestelde rechten en verplichtingen kan echter niet recht-

vaardigen dat de uitzondering op de principeverplichting tot waarborging van de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens en, in het bijzonder, op het verbod om deze gegevens op te slaan de regel wordt (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 89 en 104 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)).

112 Met betrekking tot de doelstellingen die een beperking van de met name in de artikelen 5, 6 en 9 van richtlijn 2002/58 vastgestelde rechten en verplichtingen kunnen rechtvaardigen, heeft het Hof reeds geoordeeld dat de in artikel 15, lid 1, eerste zin, van deze richtlijn gegeven opsomming van doelstellingen exhaustief is, zodat een op grond van die bepaling vastgestelde wettelijke maatregel daadwerkelijk en strikt moet berusten op een van die doelstellingen (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 52 (*NJ* 2020/232, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

113 Bovendien volgt uit artikel 15, lid 1, derde zin, van richtlijn 2002/58 dat de lidstaten slechts wettelijke maatregelen ter beperking van de omvang van de in de artikelen 5, 6 en 9 van deze richtlijn bedoelde rechten en plichten mogen nemen voor zover deze maatregelen in overeenstemming zijn met de algemene beginselen van het Unierecht, waaronder het evenredigheidsbeginsel, en met de door het Handvest gewaarborgde grondrechten. In dit verband heeft het Hof reeds geoordeeld dat de door een lidstaat bij een nationale regeling aan aanbieders van elektronischecommunicatiediensten opgelegde verplichting om de verkeersgegevens te bewaren teneinde de bevoegde nationale autoriteiten in voorkomend geval toegang tot die gegevens te kunnen geven, niet alleen vragen doet rijzen betreffende de eerbiediging van de artikelen 7 en 8 van het Handvest, die betrekking hebben op, respectievelijk, de bescherming van het privéleven en de bescherming van persoonsgegevens, maar ook betreffende de eerbiediging van artikel 11 van het Handvest, dat betrekking heeft op de vrijheid van meningsuiting (zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 25 en 70 (*NJ* 2016/446, m.nt. E.J. Dommering*; red.*), en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 91 en 92 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

114 Bij de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 moet derhalve zowel het belang van het door artikel 7 van het Handvest gewaarborgde recht op bescherming van het privéleven als dat van het door artikel 8 van het Handvest gewaarborgde recht op bescherming van persoonsgegevens, zoals dat blijkt uit de rechtspraak van het Hof, in aanmerking worden genomen. Hetzelfde geldt voor het recht op vrijheid van meningsuiting, aangezien dit in artikel 11 van het Handvest gewaarborgde grondrecht een van de wezenlijke grondslagen is van een democratische en pluralistische samenleving, die behoort tot de waarden waarop de Unie volgens artikel 2 VEU is gebaseerd (zie in die zin arresten van 6 maart 2001, *Connolly/Commissie*, C-274/99 P, EU:C:2001:127, punt 39 (*NJ* 2001/473*; red.*), en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 93 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

115 In dit verband dient te worden gepreciseerd dat de bewaring van verkeers- en locatiegegevens als zodanig behalve een uitzondering op het in artikel 5, lid 1, van richtlijn 2002/58 gestelde verbod op de opslag van die gegevens door anderen dan de gebruikers, ook een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten op eerbiediging van het privéleven en bescherming van persoonsgegevens vormt, waarbij niet van belang is of de gegevens betreffende het privéleven al dan niet gevoelig zijn en of de betrokkenen door die inmenging enig nadeel hebben ondervonden [zie in die zin *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017, EU:C:2017:592, punten 124 en 126 en aldaar aangehaalde rechtspraak; zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 30 januari 2020, *Breyer tegen Duitsland*, CE:ECHR:2020:0130JUD005000112, § 81 (*NJ* 2020/431, m.nt. E.J. Dommering*; red.*)].

116 Het is ook irrelevant of de bewaarde gegevens vervolgens al dan niet worden gebruikt (zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 16 februari 2000, *Amann tegen Zwisterland*, CE:ECHR:2000:0216JUD002779895, § 69, en 13 februari 2020, *Trjakovski en Chipovski tegen Noord-Macedonië*, CE:ECHR:2020:0213JUD005320513, § 51), aangezien de toegang tot die gegevens, ongeacht het latere gebruik ervan, op zichzelf al een inmenging vormt in de in het voorgaande punt genoemde grondrechten [zie in die zin *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017, EU:C:2017:592, punten 124 en 126].

117 Deze conclusie is des te meer gerechtvaardigd daar verkeers- en locatiegegevens informatie kunnen prijsgeven over een groot aantal aspecten van het privéleven van de betrokken personen, waaronder ook gevoelige informatie, zoals seksuele geaardheid, politieke opvattingen, religieuze, filosofische, maatschappelijke of andersoortige overtuigingen en gezondheid, terwijl dergelijke gegevens bovendien in het Unierecht bijzondere bescherming genieten. Uit deze gegevens, in hun geheel beschouwd, kunnen zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren. In het bijzonder kan aan de hand van deze gegevens het profiel van de betrokken personen worden bepaald, informatie die vanuit het oogpunt van het recht op be-

scherming van het privéleven even gevoelig is als de inhoud zelf van de communicatie (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punt 27 (*NJ* 2016/446, m.nt. E.J. Dommering*; red.*), en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 99 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)).

118 De bewaring van verkeers- en locatiegegevens voor politiële doeleinden kan dus om te beginnen op zichzelf afbreuk doen aan het in artikel 7 van het Handvest verankerde recht op eerbiediging van communicatie en de gebruikers van elektronischecommunicatiemiddelen ontmoedigen om hun door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting uit te oefenen (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punt 28 (*NJ* 2016/446, m.nt. E.J. Dommering*; red.*), en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 101 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)). Dit laatste geldt in het bijzonder voor personen van wie de communicatie naar nationaal recht onder het beroepsgeheim valt, en voor klokkenluiders van wie de activiteiten worden beschermd door richtlijn (EU) 2019/1937 van het Europees Parlement en de Raad van 23 oktober 2019 inzake de bescherming van personen die inbreuken op het Unierecht melden (*PB* 2019, L 305, blz. 17). Dat ontmoedigende effect is bovendien des te ernstiger omdat de bewaarde gegevens talrijk en gevarieerd zijn.

119 Bovendien is het zo dat, gelet op de aanzienlijke hoeveelheid verkeers- en locatiegegevens die continu kunnen worden bewaard op grond van een algemene en ongedifferentieerde bewaringsmaatregel, en op het gevoelige karakter van de informatie die deze gegevens kunnen prijsgeven, het enkele feit dat die gegevens door aanbieders van elektronischecommunicatiediensten worden bewaard, risico's van misbruik en onrechtmatige toegang tot de gegevens inhoudt.

120 Het feit dat het de lidstaten op grond van artikel 15, lid 1, van richtlijn 2002/58 is toegestaan om te voorzien in de in punt 110 van het onderhavige arrest bedoelde uitzonderingen, heeft ermee te maken dat de in de artikelen 7, 8 en 11 van het Handvest verankerde rechten geen absolute gelding hebben, maar moeten worden beschouwd in relatie tot hun functie in de samenleving (zie in die zin arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C-311/18, EU:C:2020:559, punt 172 en aldaar aangehaalde rechtspraak (*NJ* 2021/24, m.nt. E.J. Dommering*; red.*)).

121 Zoals blijkt uit artikel 52, lid 1, van het Handvest, staat het Handvest immers beperkingen op de uitoefening van die rechten toe, mits deze beperkingen bij wet worden gesteld, de wezenlijke inhoud van die rechten eerbiedigen en, met inachtneming van het evenredigheidsbeginsel, noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.

122 Bij de uitlegging van artikel 15, lid 1, van richtlijn 2002/58 in het licht van het Handvest moet derhalve ook rekening worden gehouden met het belang van de door de artikelen 3, 4, 6 en 7 van het Handvest gewaarborgde rechten en met dat van de doelstellingen van bescherming van de nationale veiligheid en bestrijding van ernstige criminaliteit, die bijdragen tot de bescherming van de rechten en vrijheden van anderen.

123 Zo heeft ingevolge artikel 6 van het Handvest, waaraan de Conseil d'État en het Grondwettelijk Hof refereren, eenieder niet alleen recht op vrijheid, maar ook op veiligheid, en waarborgt deze bepaling rechten die overeenstemmen met die welke worden gewaarborgd door artikel 5 EVRM (zie in die zin arresten van 15 februari 2016, *N.*, C-601/15 PPU, EU:C:2016:84, punt 47; 28 juli 2016, *JZ*, C-294/16 PPU, EU:C:2016:610, punt 48, en 19 september 2019, *Rayonna prokuratura Lom*, C-467/18, EU:C:2019:765, punt 42 (*NJ* 2020/119*; red.*) en aldaar aangehaalde rechtspraak).

124 Voorts zij eraan herinnerd dat artikel 52, lid 3, van het Handvest beoogt te zorgen voor de nodige samenhang tussen de in het Handvest vervatte rechten en de daarmee corresponderende, door het EVRM gewaarborgde rechten, zonder de autonomie van het Unierecht en van het Hof van Justitie van de Europese Unie aan te tasten. Bijgevolg dient bij de uitlegging van het Handvest rekening te worden gehouden met de overeenkomstige rechten van het EVRM, die het minimale beschermingsniveau bepalen [zie in die zin arresten van 12 februari 2019, *TC*, C-492/18 PPU, EU:C:2019:108, punt 57, en 21 mei 2019, *Commissie/Hongarije (Vruchtgebruik op landbouwgrond)*, C-235/17, EU:C:2019:432, punt 72 (*NJ* 2019/373*; red.*) en aldaar aangehaalde rechtspraak].

125 Artikel 5 EVRM, waarin het 'recht op vrijheid' en het 'recht op veiligheid' zijn verankerd, beoogt volgens de rechtspraak van het EHRM eenieder te beschermen tegen willekeurige en ongerechtvaardigde vrijheidsontneming (zie in die zin EHRM, 18 maart 2008, *Ladent tegen Polen*, CE:ECHR:2008:0318JUD001103603, §§ 45 en 46; 29 maart 2010, *Medvedyev e.a. tegen Frankrijk*, CE:ECHR:2010:0329JUD000339403, §§ 76 en 77 (*NJ* 2010/643, m.nt. N. Keijzer*; red.*), en 13 december 2012, *El-Masri tegen 'The former Yugoslav Republic of Macedonia'*, CE:ECHR:2012:1213JUD003963009, § 239). Die bepaling ziet echter op vrijheidsontneming door overheidsinstanties, zodat artikel 6 van het Handvest niet aldus kan worden uitgelegd dat het de overheid een verplichting oplegt om specifieke maatregelen te nemen teneinde bepaalde strafbare handelingen tegen te gaan.

126 Wat daarentegen in het bijzonder de door het Grondwettelijk Hof genoemde effectieve bestrijding betreft van strafbare handelingen waarvan met name minderjarigen en andere kwetsbare personen het slachtoffer zijn, moet worden beklemtoond dat uit artikel 7 van het Handvest positieve verplichtingen voor de overheid kunnen voortvloeien om juridische maatregelen te nemen ter be-

scherming van het privéleven en het familie- en gezinsleven [zie in die zin arrest van 18 juni 2020, *Commissie/Hongarije (Transparantie van verenigingen)*, C-78/18, EU:C:2020:476, punt 123 en aldaar aangehaalde rechtspraak van het EHRM]. Dergelijke verplichtingen kunnen ook uit dat artikel voortvloeien ten aanzien van de bescherming van iemands woning en communicatie, en uit de artikelen 3 en 4 van het Handvest ten aanzien van de bescherming van iemands lichamelijke en geestelijke integriteit en het verbod op folteringen en onmenselijke en vernederende behandelingen.

127 Gelet op die verschillende positieve verplichtingen is het noodzakelijk de diverse op het spel staande belangen en rechten met elkaar te verzoenen.

128 Het EHRM heeft namelijk geoordeeld dat de positieve verplichtingen die voortvloeien uit de artikelen 3 en 8 EVRM, waarin rechten zijn gewaarborgd die corresponderen met de in de artikelen 4 en 7 van het Handvest gewaarborgde rechten, met name impliceren dat materiële en procedurele bepalingen moeten worden vastgesteld en praktische maatregelen moeten worden genomen die het mogelijk maken om criminaliteit gericht tegen personen effectief te bestrijden door middel van doeltreffend onderzoek en doeltreffende vervolging, hetgeen des te belangrijker is wanneer het lichamelijke en geestelijke welzijn van een kind wordt bedreigd. De bevoegde autoriteiten dienen daarbij echter de wettelijk voorgeschreven procedures en de overige waarborgen die de omvang van de strafrechtelijke onderzoeksbevoegdheden beperken, alsmede de overige vrijheden en rechten volledig in acht te nemen. Met name dient er volgens het EHRM een wettelijk kader te worden ingevoerd dat het mogelijk maakt de verschillende belangen en rechten die moeten worden beschermd, met elkaar te verzoenen (EHRM, 28 oktober 1998, *Osman tegen Verenigd Koninkrijk*,
CE:ECHR:1998:1028JUD002345294, §§ 115 en 116 (*NJ* 2000/134, m.nt. E.A. Alkema*; red.*); 4 maart 2004, *M.C. tegen Bulgarije*,
CE:ECHR:2003:1204JUD003927298, § 151; 24 juni 2004, *Von Hannover tegen Duitsland*,
CE:ECHR:2004:0624JUD005932000, §§ 57 en 58 (*NJ* 2005/22, m.nt. E.J. Dommering*; red.*), en 2 december 2008, *K.U. tegen Finland*,
CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 en 49).

129 Wat de eerbiediging van het evenredigheidsbeginsel betreft, staat in artikel 15, lid 1, eerste zin, van richtlijn 2002/58 te lezen dat de lidstaten een maatregel waarbij wordt afgeweken van het beginsel van vertrouwelijkheid van de communicatie en van de daarmee verband houdende verkeersgegevens kunnen treffen wanneer een dergelijke maatregel 'in een democratische samenleving noodzakelijk, redelijk en proportioneel is' in het licht van de in die bepaling genoemde doelstellingen. In overweging 11 van deze richtlijn wordt gepreciseerd dat een dergelijke maatregel 'strikt' evenredig moet zijn aan het nagestreefde doel.

130 In dit verband zij eraan herinnerd dat de bescherming van het grondrecht op eerbiediging van het privéleven volgens vaste rechtspraak van het Hof vereist dat de uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven. Bovendien kan een doelstelling van algemeen belang niet worden nagestreefd zonder rekening te houden met het feit dat deze doelstelling moet worden verzoend met de door de maatregel aangetaste grondrechten, zulks via een evenwichtige afweging tussen de doelstelling en de op het spel staande belangen en rechten [zie in die zin arresten van 16 december 2008, *Satakunnan Markkinapörssi en Satamedia*, C-73/07,
EU:C:2008:727, punt 56 (*NJ* 2009/193, m.nt. M.R. Mok*; red.*); 9 november 2010, *Volker und Markus Schecke en Eifert*, C-92/09 en C-93/09,
EU:C:2010:662, punten 76, 77 en 86 (*NJ* 2011/68*; red.*), en 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punt 52 (*NJ* 2016/446, m.nt. E.J. Dommering*; red.*); *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017, EU:C:2017:592, punt 140].

131 Meer bepaald volgt uit de rechtspraak van het Hof dat bij de beoordeling of de lidstaten een beperking van de omvang van de met name in de artikelen 5, 6 en 9 van richtlijn 2002/58 bedoelde rechten en plichten kunnen rechtvaardigen, moet worden bepaald wat de ernst is van de inmenging die een dergelijke beperking meebrengt, en moet worden nagegaan of het belang van de met die beperking nagestreefde doelstelling van algemeen belang in verhouding staat tot die ernst (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 55 (*NJ* 2020/232, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

132 Om aan het evenredigheidsvereiste te voldoen, dient een regeling duidelijke en nauwkeurige regels te bevatten over de reikwijdte en de toepassing van de betrokken maatregel, zodat degenen van wie de persoonsgegevens aan de orde zijn, over voldoende waarborgen beschikken dat die gegevens doeltreffend worden beschermd tegen het risico van misbruik. Die regeling moet wettelijk verbindend zijn naar intern recht en in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het strikt noodzakelijke wordt beperkt. De noodzaak om over dergelijke waarborgen te beschikken is des te groter wanneer de persoonsgegevens op geautomatiseerde wijze worden verwerkt, met name wanneer er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd. Deze overwegingen gelden in het bijzonder wanneer het gaat om de bescherming van een bijzondere categorie persoonsgegevens, te we-

ten gevoelige gegevens [zie in die zin arresten van 8 april 2014, *Digital Rights Ireland e.a.*, C-293/12 en C-594/12, EU:C:2014:238, punten 54 en 55 (*NJ* 2016/446, m.nt. E.J. Dommering*; red.*), en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 117 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*); *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017, EU:C:2017:592, punt 141].

133 Een regeling die voorziet in de bewaring van persoonsgegevens, moet derhalve steeds beantwoorden aan objectieve criteria die een verband leggen tussen de te bewaren gegevens en het nagestreefde doel [zie in die zin *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017, EU:C:2017:592, punt 191 en aldaar aangehaalde rechtspraak, en arrest van 3 oktober 2019, *A e.a.*, C-70/18, EU:C:2019:823, punt 63].

- Wettelijke maatregelen die voorzien in de preventieve bewaring van verkeers- en locatiegegevens ten behoeve van de bescherming van de nationale veiligheid

134 Het Hof heeft zich in zijn arresten betreffende de uitlegging van richtlijn 2002/58 nog niet specifiek gebogen over de doelstelling van bescherming van de nationale veiligheid, waaraan is gerefereerd door de verwijzende rechters en de regeringen die opmerkingen hebben ingediend.

135 In dit verband moet om te beginnen worden opgemerkt dat de nationale veiligheid volgens artikel 4, lid 2, VEU tot de uitsluitende verantwoordelijkheid van elke lidstaat behoort. Deze verantwoordelijkheid strookt met het grote belang dat wordt gehecht aan de bescherming van de essentiële staatsfuncties en de fundamentele belangen van de samenleving, en omvat het voorkomen en bestrijden van activiteiten die de fundamentele constitutionele, politieke, economische of sociale structuren van een land ernstig kunnen destabiliseren en, met name, een rechtstreekse bedreiging kunnen vormen voor de samenleving, de bevolking of de staat als zodanig, zoals terroristische activiteiten.

136 Het belang van de doelstelling van bescherming van de nationale veiligheid, gelezen in het licht van artikel 4, lid 2, VEU, overstijgt dat van de andere doelstellingen die worden genoemd in artikel 15, lid 1, van richtlijn 2002/58, met name de doelstellingen van bestrijding van — zelfs ernstige — criminaliteit in het algemeen, en van bescherming van de openbare veiligheid. Bedreigingen als die waaraan in het voorgaande punt wordt gerefereerd, verschillen door hun aard en hun bijzondere ernst immers van het algemene risico dat zich — zelfs ernstige — spanningen of wanordelijkheden zullen voordoen die de openbare veiligheid ondermijnen. Mits aan de overige in artikel 52, lid 1, van het Handvest geformuleerde vereisten wordt voldaan, kan de doelstelling van bescherming van de nationale veiligheid derhalve maatregelen rechtvaardigen die ernstigere inmengingen in de grondrechten met zich brengen dan die welke door die andere doelstellingen zouden kunnen worden gerechtvaardigd.

137 In situaties als die welke in de punten 135 en 136 van het onderhavige arrest zijn beschreven, verzet artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zich derhalve in beginsel niet tegen een wettelijke maatregel op grond waarvan de bevoegde autoriteiten aan aanbieders van elektronischecommunicatiediensten een bevel kunnen opleggen om de verkeers- en locatiegegevens van alle gebruikers van elektronischecommunicatiemiddelen gedurende een beperkte periode te bewaren, wanneer er voldoende concrete aanwijzingen zijn dat de betrokken lidstaat wordt geconfronteerd met een ernstige bedreiging van de nationale veiligheid als bedoeld in de punten 135 en 136 van het onderhavige arrest, en die bedreiging werkelijk en actueel of voorzienbaar is. Ook al heeft een dergelijke maatregel zonder onderscheid betrekking op alle gebruikers van elektronischecommunicatiemiddelen, zonder dat er op het eerste gezicht enig verband in de zin van de in punt 133 van het onderhavige arrest bedoelde rechtspraak tussen die gebruikers en een bedreiging voor de nationale veiligheid van de betrokken lidstaat lijkt te bestaan, geoordeeld moet worden dat het bestaan van een dergelijke bedreiging op zichzelf dat verband aantoont.

138 Het bevel om preventief de gegevens te bewaren van alle gebruikers van elektronischecommunicatiemiddelen, mag echter slechts worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk. Het valt weliswaar niet uit te sluiten dat het aan aanbieders van elektronischecommunicatiemiddelen opgelegde bevel tot bewaring van die gegevens kan worden verlengd wegens het voortduren van een dergelijke bedreiging, maar dit neemt niet weg dat elk bevel slechts mag worden gegeven voor een voorzienbare periode. Een dergelijke gegevensbewaring moet bovendien zijn onderworpen aan beperkingen en zijn omgeven met strikte waarborgen die ervoor zorgen dat de persoonsgegevens van de betrokken personen doeltreffend worden beschermd tegen het risico van misbruik. Die bewaring mag derhalve geen stelselmatig karakter hebben.

139 Gelet op de ernst van de inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten die een dergelijke algemene en ongedifferentieerde bewaring van gegevens met zich brengt, dient te worden gewaarborgd dat de toepassing van die maatregel daadwerkelijk beperkt blijft tot situaties waarin de nationale veiligheid ernstig wordt bedreigd, zoals de in de punten 135 en 136 van het onderhavige arrest bedoelde situaties. Daartoe is het van wezenlijk belang dat een beslissing waarbij aan aanbieders van elektronischecommunicatiediensten een bevel tot een dergelijke gegevensbewaring wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is,

waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien.

- Wettelijke maatregelen die voorzien in de preventieve bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van criminaliteit en de bescherming van de openbare veiligheid

140 Als het gaat om de doelstelling strafbare feiten te voorkomen, te onderzoeken, op te sporen en te vervolgen, kunnen overeenkomstig het evenredigheidsbeginsel enkel de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen voor de openbare veiligheid een rechtvaardiging vormen voor ernstige inmengingen in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, zoals die welke voortvloeien uit de bewaring van verkeers- en locatiegegevens. De doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen, kan derhalve enkel niet-ernstige inmengingen in die grondrechten rechtvaardigen [zie in die zin arresten van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 102 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*), en 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punten 56 en 57 (*NJ* 2020/232, m.nt. E.J. Dommering*; red.*); *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017, EU:C:2017:592, punt 149].

141 Een nationale regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit, gaat verder dan strikt noodzakelijk is en kan niet worden beschouwd als een regeling die in een democratische samenleving gerechtvaardigd is, zoals artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, eist (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 107 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)).

142 Gezien het gevoelige karakter van de informatie die verkeers- en locatiegegevens kunnen prijsgeven, is de vertrouwelijkheid van deze gegevens immers essentieel voor het recht op eerbiediging van het privéleven. Mede gelet op het in punt 118 van het onderhavige arrest bedoelde ontmoedigende effect dat de bewaring van die gegevens kan hebben op de uitoefening van de in de artikelen 7 en 11 van het Handvest verankerde grondrechten, en op de ernst van de inmenging die een dergelijke bewaring met zich brengt, is het in een democratische samenleving dan ook van belang dat deze bewaring, zoals het bij richtlijn 2002/58 ingevoerde stelsel eist, de uitzondering en niet de regel vormt en dat de betrokken gegevens niet stelselmatig en continu kunnen worden bewaard. Deze conclusie geldt zelfs met betrekking tot de doelstellingen van bestrijding van zware criminaliteit en voorkoming van ernstige bedreigingen voor de openbare veiligheid en het belang dat aan deze doelstellingen moet worden toegekend.

143 Voorts heeft het Hof benadrukt dat een regeling die voorziet in de algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, de elektronische communicatie van vrijwel de gehele bevolking bestrijkt, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het met de regeling beoogde doel. Een dergelijke regeling betreft algemeen alle personen die gebruikmaken van elektronischecommunicatiediensten, zonder dat die personen zich — zelfs maar indirect — in een situatie bevinden die aanleiding kan zijn om strafvervolging in te stellen, wat in strijd is met het in punt 133 van het onderhavige arrest in herinnering gebrachte vereiste. Zij is dus zelfs van toepassing op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag — zelfs maar indirect of van ver — verband houdt met die doelstelling van bestrijding van zware misdrijven, en vereist met name niet dat er een verband is tussen de te bewaren gegevens en een bedreiging voor de openbare veiligheid (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punten 57 en 58 (*NJ* 2016/446, m.nt. E.J. Dommering*; red.*), en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 105 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)).

144 Zoals het Hof reeds heeft geoordeeld, beperkt een dergelijke regeling met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het bestrijden van zware criminaliteit (zie in die zin arresten van 8 april 2014, *Digital Rights*, C-293/12 en C-594/12, EU:C:2014:238, punt 59 (*NJ* 2016/446, m.nt. E.J. Dommering*; red.*), en 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 106 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)).

145 Zelfs de positieve verplichtingen die, naargelang van het geval, voor de lidstaten kunnen voortvloeien uit de artikelen 3, 4 en 7 van het Handvest en, zoals in de punten 126 en 128 van het onderhavige arrest is opgemerkt, betrekking hebben op de invoering van regels die een effectieve bestrijding van strafbare feiten mogelijk maken, kunnen geen inmengingen rechtvaardigen die zo ernstig zijn als de inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van vrijwel de gehele bevolking die een regeling die voorziet in de bewaring van verkeers- en locatiegegevens met zich brengt, zonder dat de gegevens van de betrokken personen, althans indirect, een verband met het nagestreefde doel aan het licht kunnen brengen.

146 Daarentegen kunnen, overeenkomstig hetgeen in de punten 142 tot en met 144 van het onder-

havige arrest is vastgesteld, en gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, de doelstellingen van bestrijding van zware criminaliteit, voorkoming van ernstige bedreigingen voor de openbare veiligheid en, a fortiori, bescherming van de nationale veiligheid — gezien het belang ervan in het licht van de in het voorgaande punt in herinnering gebrachte positieve verplichtingen waaraan met name het Grondwettelijk Hof heeft gerefereerd — de bijzonder ernstige inmenging rechtvaardigen die een gerichte bewaring van verkeers- en locatiegegevens met zich brengt.

147 Zoals het Hof reeds heeft geoordeeld, staat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, derhalve niet eraan in de weg dat een lidstaat een regeling vaststelt op grond waarvan verkeers- en locatiegegevens preventief gericht kunnen worden bewaard ten behoeve van de bestrijding van zware criminaliteit, de voorkoming van ernstige bedreigingen voor de openbare veiligheid en de bescherming van de nationale veiligheid, op voorwaarde dat die bewaring, wat de categorieën te bewaren gegevens, de betrokken communicatiemiddelen, de betrokken personen en de duur van de bewaring betreft, tot het strikt noodzakelijke wordt beperkt (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 108 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)).

148 De noodzakelijke afbakening van een dergelijke gegevensbewaringsmaatregel kan met name worden verricht aan de hand van de categorieën betrokken personen, aangezien artikel 15, lid 1, van richtlijn 2002/58 zich niet verzet tegen een regeling die is gebaseerd op objectieve factoren waarmee kan worden gemikt op de personen van wie de verkeers- en locatiegegevens, althans indirect, een verband met ernstige strafbare feiten aan het licht kunnen brengen, waarmee op de een of andere wijze kan worden bijgedragen tot de bestrijding van zware criminaliteit of waarmee een ernstig risico voor de openbare veiligheid of een risico voor de nationale veiligheid kan worden voorkomen (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 111 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)).

149 In dit verband moet worden gepreciseerd dat de personen op wie aldus wordt gemikt, met name diegenen kunnen zij die eerder in het kader van de toepasselijke nationale procedures en op basis van objectieve factoren zijn geïdentificeerd als personen die een bedreiging vormen voor de openbare veiligheid of de nationale veiligheid van de betrokken lidstaat.

150 Een maatregel die voorziet in de bewaring van verkeers- en locatiegegevens, kan ook worden afgebakend aan de hand van een geografisch criterium wanneer de bevoegde nationale autoriteiten op basis van objectieve factoren van mening zijn dat er in een of meer geografische gebieden sprake is van een situatie die wordt gekenmerkt door een hoog risico dat zware misdrijven worden voorbereid of gepleegd (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 111 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)). Het kan daarbij met name gaan om plekken waar veel zware criminaliteit plaatsvindt, om plaatsen waar er een verhoogd risico is op zware misdrijven, zoals plekken of faciliteiten die regelmatig door een zeer groot aantal personen worden bezocht, of om strategische plekken, zoals vliegvelden, stations of tolzones.

151 Om ervoor te zorgen dat de inmenging die de in de punten 147 tot en met 150 van het onderhavige arrest beschreven maatregelen inzake gerichte gegevensbewaring met zich brengen, in overeenstemming is met het evenredigheidsbeginsel, mogen die maatregelen niet langer gelden dan strikt noodzakelijk is in het licht van het ermee beoogde doel en van de omstandigheden waardoor zij worden gerechtvaardigd, met dien verstande dat zij eventueel kunnen worden verlengd mocht de noodzaak van een dergelijke bewaring blijven bestaan.

- Wettelijke maatregelen die voorzien in de preventieve bewaring van IP-adressen en gegevens inzake de burgerlijke identiteit ten behoeve van de bestrijding van criminaliteit en de bescherming van de openbare veiligheid

152 Opgemerkt dient te worden dat IP-adressen weliswaar behoren tot de verkeersgegevens, maar los van een bepaalde communicatie worden gegenereerd en primair dienen om via de aanbieders van elektronischecommunicatiediensten de natuurlijke persoon te identificeren die eigenaar is van een eindapparaat waarvandaan via het internet wordt gecommuniceerd. Voor zover bij e-mailverkeer en internettelefonie uitsluitend de IP-adressen van de bron van de communicatie en niet die van de ontvanger ervan worden bewaard, geven die adressen als zodanig geen enkele informatie prijs over de derden die in contact zijn geweest met de persoon die aan de basis ligt van de communicatie. Deze categorie gegevens is dan ook van mindere gevoelige aard dan de andere verkeersgegevens.

153 Aangezien IP-adressen echter onder meer kunnen worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit, kan aan de hand van die gegevens een gedetailleerd profiel van de betrokkene worden opgesteld. De voor een dergelijke tracking noodzakelijke bewaring en analyse van IP-adressen vormen dan ook ernstige inmengingen in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten van de internetgebruiker, die een ontmoedigend effect als bedoeld in punt 118 van het onderhavige arrest kunnen hebben.

154 Om de op het spel staande rechten en belangen met elkaar te verzoenen, zoals de in punt 130 van het onderhavige arrest aangehaalde rechtspraak verlangt, moet echter in aanmerking worden

genomen dat in het geval van een online gepleegd strafbaar feit het IP-adres het enige onderzoeksmiddel kan zijn met behulp waarvan de persoon kan worden geïdentificeerd aan wie dat adres was toegewezen op het moment waarop dat feit werd gepleegd. Bovendien lijkt de bewaring van IP-adressen door aanbieders van elektronischecommunicatiediensten na afloop van de periode waarvoor deze adressen werden toegewezen, in beginsel niet noodzakelijk te zijn met het oog op de facturering van die diensten, met als gevolg dat, zoals verschillende regeringen hebben aangevoerd in de door hen bij het Hof ingediende opmerkingen, het opsporen van online gepleegde strafbare feiten onmogelijk kan blijken zonder gebruik te maken van een wettelijke maatregel als bedoeld in artikel 15, lid 1, van richtlijn 2002/58. Zoals die regeringen hebben betoogd, kan dit met name het geval zijn bij zeer ernstige strafbare feiten op het gebied van kinderpornografie, zoals het online verwerven, verspreiden, uitzenden of ter beschikking stellen van kinderpornografie in de zin van artikel 2, onder c), van richtlijn 2011/93/EU van het Europees Parlement en de Raad van 13 december 2011 ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie, en ter vervanging van kaderbesluit 2004/68/JBZ van de Raad (*PB* 2011, L 335, blz. 1).

155 In deze omstandigheden moet worden vastgesteld dat, ook al zou een wettelijke maatregel die voorziet in de bewaring van de IP-adressen van alle natuurlijke personen die eigenaar zijn van eindapparatuur die internettoegang mogelijk maakt, personen betreffen bij wie op het eerste gezicht een verband met de nagestreefde doelstellingen in de zin van de in punt 133 van het onderhavige arrest aangehaalde rechtspraak ontbreekt, en ook al moeten internetgebruikers, zoals in punt 109 van het onderhavige arrest is vastgesteld, op grond van de artikelen 7 en 8 van het Handvest erop kunnen vertrouwen dat hun identiteit in beginsel niet wordt onthuld, een wettelijke maatregel die voorziet in de algemene en ongedifferentieerde bewaring van uitsluitend de aan de bron van een verbinding toegewezen IP-adressen, in beginsel niet in strijd is met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, voor zover die mogelijkheid afhankelijk wordt gesteld van de strikte naleving van de materiële en procedurele voorwaarden die het gebruik van die gegevens dienen te regelen.

156 Gelet op het feit dat die bewaring een ernstige inmenging inhoudt in de grondrechten die zijn verankerd in de artikelen 7 en 8 van het Handvest, kunnen enkel de bestrijding van zware criminaliteit en het voorkomen van ernstige bedreigingen van de openbare veiligheid, alsmede de bescherming van de nationale veiligheid, die inmenging rechtvaardigen. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk is gelet op het nagestreefde doel. Tot slot moet een dergelijke maatregel voorzien in strikte voorwaarden en waarborgen met betrekking tot het gebruik van die gegevens, met name in de vorm van het in kaart brengen van de online communicatie en de online activiteiten van de betrokken personen.

157 Wat ten slotte de gegevens betreffende de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen betreft, moet worden opgemerkt dat met die gegevens alleen noch de datum, het tijdstip, de duur en de ontvangers van de communicatie kunnen worden achterhaald, noch de plaats waar die communicatie heeft plaatsgevonden of het aantal malen dat in een specifieke periode met bepaalde personen is gecommuniceerd. Die gegevens verschaffen dus, afgezien van de contactgegevens van de betrokken gebruikers, zoals hun adres, geen informatie over wat die personen hebben gecommuniceerd en dus over hun privéleven. De inmenging die de bewaring van die gegevens met zich brengt, kan derhalve niet als 'ernstig' worden aangemerkt (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punten 59 en 60 (*NJ* 2020/232, m.nt. E.J. Dommering*; red.*)).

158 Hieruit volgt dat, overeenkomstig hetgeen is uiteengezet in punt 140 van het onderhavige arrest, wettelijke maatregelen die betrekking hebben op de verwerking van die gegevens als zodanig, in het bijzonder op de bewaring van en de toegang tot die gegevens met als enige doel de betrokken gebruiker te identificeren, zonder dat de gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie, kunnen worden gerechtvaardigd door de in artikel 15, lid 1, eerste zin, van richtlijn genoemde doelstelling strafbare feiten in het algemeen te voorkomen, te onderzoeken, op te sporen en te vervolgen (zie in die zin arrest van 2 oktober 2018, *Ministerio Fiscal*, C-207/16, EU:C:2018:788, punt 62 (*NJ* 2020/232, m.nt. E.J. Dommering*; red.*)).

159 Gelet op de noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, moet in deze omstandigheden om de in de punten 131 en 158 van het onderhavige arrest uiteengezette redenen worden geoordeeld dat, ook al bestaat er geen verband tussen alle gebruikers van elektronischecommunicatiemiddelen en de nagestreefde doelstellingen, artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 2, van het Handvest, zich niet verzet tegen een wettelijke maatregel op grond waarvan aanbieders van elektronischecommunicatiediensten verplicht zijn om de gegevens inzake de burgerlijke identiteit van alle gebruikers van elektronischecommunicatiemiddelen gedurende een niet nader bepaalde periode te bewaren ten behoeve van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten en het waarborgen van de openbare veiligheid, zonder dat het daarbij hoeft te gaan om ernstige strafbare feiten of om ernstige bedreigingen en verstoringen van de openbare veiligheid.

- Wettelijke maatregelen die voorzien in de spoedbewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit

160 Met betrekking tot de verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden verwerkt en opgeslagen op grond van de artikelen 5, 6 en 9 van richtlijn 2002/58 dan wel op grond van krachtens artikel 15, lid 1, van deze richtlijn vastgestelde wettelijke maatregelen als beschreven in de punten 134 tot en met 159 van het onderhavige arrest, dient te worden opgemerkt dat deze gegevens in beginsel moeten worden gewist of geanonimiseerd na het verstrijken van de wettelijke termijnen waarbinnen zij overeenkomstig de nationale bepalingen tot omzetting van die richtlijn moeten worden verwerkt en opgeslagen.

161 Gedurende die verwerking en opslag kunnen zich evenwel situaties voordoen die het noodzakelijk maken om de betrokken gegevens ook na het verstrijken van die termijnen te bewaren teneinde ernstige strafbare feiten of verstoringen van de nationale veiligheid op te helderen, en dit niet alleen wanneer die feiten of verstoringen reeds konden worden vastgesteld, maar ook wanneer er na een objectief onderzoek van alle relevante omstandigheden een redelijk vermoeden bestaat dat dergelijke feiten zijn gepleegd of dat de nationale veiligheid wordt bedreigd.

162 In dit verband zij erop gewezen dat het op 23 november 2001 onder auspiciën van de Raad van Europa gesloten Cybercrimeverdrag (Serie Europese Verdragen — nr. 185), dat door alle 27 lidstaten is ondertekend en door 25 lidstaten is geratificeerd, en dat tot doel heeft de bestrijding van door middel van een computersysteem begane strafbare feiten te vergemakkelijken, in artikel 14 bepaalt dat de verdragsluitende partijen ten behoeve van specifieke strafrechtelijke onderzoeken of procedures bepaalde maatregelen moeten nemen met betrekking tot reeds opgeslagen verkeersgegevens, zoals de spoedbewaring van die gegevens. Met name is in artikel 16, lid 1, van dit verdrag bepaald dat de verdragsluitende partijen de wetgevende en andere maatregelen moeten nemen die nodig zijn om hun bevoegde autoriteiten in staat te stellen de spoedbewaring te bevelen of op soortgelijke wijze de spoedbewaring te bewerkstelligen van verkeersgegevens die zijn opgeslagen door middel van een computersysteem, in het bijzonder wanneer er redenen zijn om te vermoeden dat die gegevens vatbaar zijn voor verlies of wijziging.

163 In een situatie als bedoeld in punt 161 van het onderhavige arrest staat het de lidstaten, gelet op de in punt 130 van het onderhavige arrest genoemde noodzaak om de op het spel staande rechten en belangen met elkaar te verzoenen, vrij om in een op grond van artikel 15, lid 1, van richtlijn 2002/58 vastgestelde wettelijke regeling te voorzien in de mogelijkheid om via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode.

164 Aangezien het doel van een dergelijke spoedbewaring niet meer overeenkomt met de doelen waarvoor de gegevens oorspronkelijk zijn vergaard en bewaard, en aangezien ingevolge artikel 8, lid 2, van het Handvest iedere verwerking van gegevens bepaalde doelen moet dienen, moeten de lidstaten in hun wetgeving duidelijk maken voor welk doel spoedbewaring van gegevens mogelijk is. Gelet op het feit dat een dergelijke bewaring een ernstige inmenging inhoudt in de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten, kunnen enkel de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de nationale veiligheid die inmenging rechtvaardigen. Om ervoor te zorgen dat de inmenging die een dergelijke maatregel met zich brengt, tot het strikt noodzakelijke wordt beperkt, moet bovendien om te beginnen de bewaarplicht uitsluitend gelden voor verkeers- en locatiegegevens die kunnen helpen bij het ophelderen van het betrokken ernstige strafbare feit of de betrokken verstoring van de nationale veiligheid. Bovendien mag de bewaartermijn niet langer zijn dan strikt noodzakelijk, zij het dat die termijn kan worden verlengd wanneer de omstandigheden en het met de betrokken maatregel beoogde doel dit rechtvaardigen.

165 In dit verband moet worden gepreciseerd dat een dergelijke spoedbewaring niet moet worden beperkt tot de gegevens van personen op wie een concrete verdenking rust dat zij een strafbaar feit hebben gepleegd of de nationale veiligheid in gevaar hebben gebracht. Mits daarbij het kader in acht wordt genomen dat is ingesteld bij artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, en gelet op de overwegingen in punt 133 van het onderhavige arrest, kan een dergelijke maatregel naar keuze van de wetgever en binnen de grenzen van het strikt noodzakelijke worden uitgebreid tot verkeers- en locatiegegevens die betrekking hebben op andere personen dan die welke ervan worden verdacht een ernstig misdrijf of handelingen die een gevaar vormen voor de nationale veiligheid te hebben voorbereid of gepleegd, op voorwaarde dat op basis van objectieve en niet-discriminatoire factoren kan worden geoordeeld dat die gegevens kunnen helpen bij het ophelderen van een dergelijk misdrijf of een dergelijke verstoring van de nationale veiligheid. In dit verband kan bijvoorbeeld worden gedacht aan de gegevens van het slachtoffer van het misdrijf of van personen uit de sociale of professionele omgeving van de betrokkene, of aan de gegevens betreffende bepaalde geografische gebieden, zoals de plaatsen waar het misdrijf of de handeling die een gevaar heeft gevormd voor de nationale veiligheid, is voorbereid of gepleegd. Bovendien moet aan de bevoegde autoriteiten toe-

gang tot de aldus bewaarde gegevens worden verleend met inachtneming van de voorwaarden die voortvloeien uit de arresten waarin richtlijn 2002/58 is uitgelegd (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punten 118-121 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

166 Hieraan moet nog worden toegevoegd dat, zoals met name uit de punten 115 en 133 van het onderhavige arrest volgt, de toegang tot verkeers- en locatiegegevens die door aanbieders van elektronischecommunicatiediensten worden bewaard op grond van een krachtens artikel 15, lid 1, van richtlijn 2002/58 vastgestelde maatregel, in beginsel enkel kan worden gerechtvaardigd door de doelstelling van algemeen belang met het oog waarop de verplichting tot bewaring van die gegevens aan die aanbieders is opgelegd. Hieruit volgt met name dat in geen geval toegang tot dergelijke gegevens mag worden verleend met het oog op de vervolging en bestraffing van een gewoon strafbaar feit, wanneer de bewaring van die gegevens haar rechtvaardiging vindt in de doelstelling van bestrijding van zware criminaliteit of, a fortiori, de doelstelling van bescherming van de nationale veiligheid. Overeenkomstig het evenredigheidsbeginsel zoals dit is verduidelijkt in punt 131 van het onderhavige arrest, kan daarentegen de toegang tot gegevens die zijn bewaard met het oog op de bestrijding van zware criminaliteit, worden gerechtvaardigd door de doelstelling van bescherming van de nationale veiligheid, mist de in het voorgaande punt bedoelde materiële en procedurele voorwaarden voor een dergelijke toegang in acht worden genomen.

167 In zoverre staat het de lidstaten vrij om in hun wetgeving te bepalen dat met inachtneming van diezelfde materiële en procedurele voorwaarden toegang tot verkeers- en locatiegegevens kan worden verleend met het oog op de bestrijding van zware criminaliteit of de bescherming van de nationale veiligheid, wanneer die gegevens door een aanbieder zijn bewaard in overeenstemming met de artikelen 5, 6 en 9 of met artikel 15, lid 1, van richtlijn 2002/58.

168 Gelet op een en ander moet op de eerste vraag in de zaken C-511/18 en C-512/18 en op de eerste en de tweede vraag in zaak C-520/18 worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen wettelijke maatregelen die voor de in die bepaling genoemde doeleinden preventief voorzien in een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens. Artikel 15, lid 1, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, verzet zich daarentegen niet tegen wettelijke maatregelen

- die het mogelijk maken om ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronischecommunicatiediensten een bevel tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens op te leggen in situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, wanneer de beslissing waarbij dat bevel wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer dat bevel slechts kan worden opgelegd voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd indien die bedreiging voortduurt;
- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een gerichte bewaring van verkeers- en locatiegegevens, die op basis van objectieve en niet-discriminatoire factoren wordt afgebakend aan de hand van categorieën betrokken personen of aan de hand van een geografisch criterium, voor een periode die niet langer is dan strikt noodzakelijk, maar die kan worden verlengd;
- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van zware criminaliteit en de voorkoming van ernstige bedreigingen van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding, voor een periode die niet langer is dan strikt noodzakelijk;
- die ten behoeve van de bescherming van de nationale veiligheid, de bestrijding van criminaliteit en de bescherming van de openbare veiligheid voorzien in een algemene en ongedifferentieerde bewaring van de gegevens inzake de burgerlijke identiteit van de gebruikers van elektronischecommunicatiemiddelen, en
- die het mogelijk maken om ten behoeve van de bestrijding van zware criminaliteit en, a fortiori, de bescherming van de nationale veiligheid via een aan effectieve rechterlijke toetsing onderworpen beslissing van de bevoegde autoriteit aan aanbieders van elektronischecommunicatiediensten een bevel op te leggen tot spoedbewaring van de in hun handen zijnde verkeers- en locatiegegevens gedurende een bepaalde periode,

mits die maatregelen, door het gebruik van duidelijke en nauwkeurige regels, verzekeren dat de betrokken gegevens slechts worden bewaard indien aan de daarvoor geldende materiële en procedurele voorwaarden wordt voldaan, en dat de betrokken personen beschikken over effectieve waarborgen tegen het risico van misbruik.

Tweede en derde vraag in zaak C-511/18

169 Met de tweede en de derde vraag in zaak C-511/18 wenst de verwijzende rechter in wezen te

vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling die aan aanbieders van elektronischecommunicatiediensten de verplichting oplegt om op hun netwerken maatregelen toe te passen die het mogelijk maken om, ten eerste, verkeers- en locatiegegevens op geautomatiseerde wijze te analyseren en in real time op te vragen, en, ten tweede, technische gegevens over de locatie van de gebruikte eindapparatuur in real time op te vragen, maar die niet bepaalt dat de betrokken personen over die verwerkingen en opvragingen moeten worden geïnformeerd.

170 De verwijzende rechter wijst erop dat de in de artikelen L. 851-2 tot en met L. 851-4 CSI genoemde technieken voor het inwinnen van inlichtingen voor aanbieders van elektronischecommunicatiediensten geen specifieke verplichting tot bewaring van verkeers- en locatiegegevens impliceren. Wat in het bijzonder de in artikel L. 851-3 CSI bedoelde geautomatiseerde analyse betreft, merkt die rechter op dat deze verwerking bedoeld is om aan de hand van daartoe vastgestelde criteria verbindingen op te sporen die kunnen wijzen op een terroristische dreiging. Met betrekking tot de in artikel L. 851-2 CSI bedoelde opvraging in real time stelt de verwijzende rechter vast dat deze slechts betrekking heeft op een of meer personen die eerder zijn geïdentificeerd als personen die in verband kunnen worden gebracht met een terroristische dreiging. Volgens de verwijzende rechter kunnen die twee technieken uitsluitend worden toegepast ter voorkoming van terrorisme en betreffen zij de in de artikelen L. 851-1 en R. 851-5 CSI bedoelde gegevens.

171 Om te beginnen dient te worden gepreciseerd dat het feit dat volgens artikel L. 851-3 CSI de in deze bepaling geregelde geautomatiseerde analyse het op zichzelf niet mogelijk maakt om de gebruikers te identificeren van wie de gegevens aan die analyse worden onderworpen, niet aan de kwalificatie van die gegevens als 'persoonsgegevens' in de weg staat. Aangezien de procedure van punt IV van diezelfde bepaling het mogelijk maakt om de persoon of de personen op wie de gegevens betrekking hebben waarvan de geautomatiseerde analyse een mogelijke terroristische dreiging aan het licht heeft gebracht, in een later stadium te identificeren, blijven immers alle personen op wier gegevens die analyse worden toegepast, aan de hand van die gegevens identificeerbaar. Volgens de in artikel 4, punt 1, van verordening 2016/679 opgenomen definitie van het begrip 'persoonsgegevens' omvat dit begrip onder meer informatie over een identificeerbare persoon.

Geautomatiseerde analyse van verkeers- en locatiegegevens

172 Uit artikel L. 851-3 CSI blijkt dat de in deze bepaling geregelde geautomatiseerde analyse in wezen erop neerkomt dat aanbieders van elektronischecommunicatiediensten op verzoek van de bevoegde nationale autoriteiten en in overeenstemming met de door die autoriteiten vastgestelde parameters alle door hen bewaarde verkeers- en locatiegegevens filteren. Dit betekent dat van alle gegevens van de gebruikers van elektronischecommunicatiemiddelen wordt nagegaan of zij met die parameters corresponderen. Derhalve moet worden aangenomen dat een dergelijke geautomatiseerde analyse inhoudt dat aanbieders van elektronischecommunicatiediensten in opdracht van de bevoegde autoriteit overgaan tot een algemene en ongedifferentieerde verwerking van alle verkeers- en locatiegegevens van alle gebruikers van elektronischecommunicatiemiddelen, in die zin dat die gegevens via een geautomatiseerd procedé worden gebruikt in de zin van artikel 4, punt 2, van verordening 2016/679. Die verwerking staat los van de latere, op grond van artikel L. 851-3, lid IV, CSI toegestane opvraging van de gegevens betreffende de personen die na de geautomatiseerde analyse zijn geïdentificeerd.

173 Een nationale regeling die een dergelijke geautomatiseerde analyse van verkeers- en locatiegegevens toestaat, wijkt af van de in artikel 5 van richtlijn 2002/58 neergelegde principeverplichting om de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens te waarborgen. Een dergelijke regeling vormt ook een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten, ongeacht het latere gebruik van die gegevens. Tot slot kan zo'n regeling een ontmoedigend effect hebben op de uitoefening van de door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting.

174 Voorts is de inmenging die het gevolg is van een geautomatiseerde analyse van verkeers- en locatiegegevens als aan de orde in het hoofdgeding bijzonder ernstig, daar zij op algemene en ongedifferentieerde wijze de gegevens betreft van personen die gebruikmaken van elektronischecommunicatiemiddelen. Dit geldt te meer nu de gegevens die aan de geautomatiseerde analyse worden onderworpen, zoals uit de in het hoofdgeding aan de orde zijnde nationale regeling blijkt, de aard van de online geraadpleegde informatie kunnen onthullen. Bovendien vindt een dergelijke geautomatiseerde analyse algemeen plaats bij alle personen die gebruikmaken van elektronischecommunicatiemiddelen, dat wil zeggen ook bij personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag — zelfs maar indirect of van ver — een verband vertoont met terroristische activiteiten.

175 Wat de rechtvaardiging van een dergelijke inmenging betreft, moet worden gepreciseerd dat het in artikel 52, lid 1, van het Handvest geformuleerde vereiste dat elke beperking op de uitoefening van grondrechten bij wet wordt gesteld, inhoudt dat de rechtsgrond die de inmenging in die rechten toestaat, zelf de reikwijdte van de beperking op de uitoefening van het betrokken recht moet bepalen (zie in die zin arrest van 16 juli 2020, *Facebook Ireland en*

Schrems, C-311/18, EU:C:2020:559, punt 175 (*NJ* 2021/24, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

176 Om te voldoen aan het in de punten 130 en 131 van het onderhavige arrest in herinnering gebrachte evenredigheidsvereiste, dat verlangt dat uitzonderingen op de bescherming van persoonsgegevens en beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven, moet een nationale regeling die de toegang van de bevoegde autoriteiten tot de bewaarde verkeers- en locatiegegevens regelt, bovendien in overeenstemming zijn met de vereisten die voortvloeien uit de in punt 132 van het onderhavige arrest aangehaalde rechtspraak. Met name mag een dergelijke regeling zich er niet toe beperken te eisen dat de autoriteiten toegang tot de gegevens wordt verleend voor het doel dat met die regeling wordt nagestreefd, maar moet zij ook de materiële en procedurele voorwaarden voor dit gebruik bepalen [zie naar analogie *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017, EU:C:2017:592, punt 192 en aldaar aangehaalde rechtspraak].

177 In dit verband zij eraan herinnerd dat de bijzonder ernstige inmenging die het gevolg is van een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens, zoals besproken in de punten 134 tot en met 139 van het onderhavige arrest, en de bijzonder ernstige inmenging die de geautomatiseerde analyse van die gegevens met zich brengt, slechts aan het evenredigheidsvereiste kunnen voldoen in situaties waarin een lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en op voorwaarde dat de duur van die bewaring tot het strikt noodzakelijke wordt beperkt.

178 In situaties als bedoeld in het voorgaande punt kan een geautomatiseerde analyse van de verkeers- en locatiegegevens van alle gebruikers van elektronischecommunicatiemiddelen, gedurende een periode die niet langer is dan strikt noodzakelijk, gelet op de vereisten die voortvloeien uit artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, als gerechtvaardigd worden beschouwd.

179 Om te garanderen dat de toepassing van een dergelijke maatregel daadwerkelijk beperkt blijft tot hetgeen strikt noodzakelijk is ter bescherming van de nationale veiligheid en, meer bepaald, ter voorkoming van terrorisme, is het echter, overeenkomstig hetgeen is vastgesteld in punt 139 van het onderhavige arrest, van wezenlijk belang dat de beslissing waarbij de geautomatiseerde analyse wordt toegestaan, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of zich een situatie voordoet die die maatregel rechtvaardigt, en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien.

180 In dit verband dient te worden gepreciseerd dat de vooraf vastgestelde modellen en criteria waarop dit type gegevensverwerking is gebaseerd, ten eerste specifiek en betrouwbaar moeten zijn, zodat zij tot resultaten leiden waarmee die personen worden geïdentificeerd op wie een redelijk vermoeden van deelneming aan terrorisme kan rusten, en ten tweede niet mogen discrimineren [zie in die zin *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017, EU:C:2017:592, punt 172].

181 Voorts zij eraan herinnerd dat elke geautomatiseerde analyse aan de hand van modellen en criteria die ervan uitgaan dat de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, het lidmaatschap van een vakvereniging, de gezondheid of het seksueel gedrag van een persoon op zichzelf en los van het individuele gedrag van die persoon relevant zouden kunnen zijn in het licht van het voorkomen van terrorisme, in strijd zou zijn met de door de artikelen 7 en 8 juncto artikel 21 van het Handvest gewaarborgde rechten. De modellen en criteria die vooraf worden vastgesteld ten behoeve van een geautomatiseerde analyse die tot doel heeft terroristische activiteiten die een ernstige bedreiging vormen voor de nationale veiligheid, te voorkomen, kunnen dus niet alleen op die gevoelige gegevens zijn gebaseerd [zie in die zin *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017, EU:C:2017:592, punt 165].

182 Aangezien geautomatiseerde analyses van verkeers- en locatiegegevens noodzakelijkerwijs een zekere foutenmarge bevatten, moet bovendien elk positief resultaat van een geautomatiseerde verwerking nog eens individueel — met niet-geautomatiseerde middelen — worden onderzocht alvorens een individuele maatregel wordt genomen die nadelige gevolgen heeft voor de betrokken personen, zoals de latere opvraging in real time van de betrokken gegevens. Een dergelijke maatregel mag namelijk niet uitsluitend op het resultaat van een geautomatiseerde verwerking worden gebaseerd. Om te garanderen dat de vooraf vastgestelde modellen en criteria, het gebruik dat daarvan wordt gemaakt en de gehanteerde databases in de praktijk niet discrimineren en beperkt blijven tot hetgeen strikt noodzakelijk is in het licht van de doelstelling terroristische activiteiten die een ernstige bedreiging opleveren voor de nationale veiligheid, te voorkomen, moet ook regelmatig worden onderzocht of die vooraf vastgestelde modellen en criteria en de gebruikte databases betrouwbaar en up-to-date zijn [zie in die zin *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017, EU:C:2017:592, punten 173 en 174].

Opvraging in real time van verkeers- en locatiegegevens

183 Voor de in artikel L. 851-2 CSI geregelde opvraging in real time van verkeers- en locatiegegevens kan individueel machtiging worden verleend voor zover het gaat om ‘een persoon die eerder in verband is gebracht met een [terroristische] dreiging’. In diezelfde bepaling staat dat ‘[w]anneer er

zwaarwegende redenen zijn om aan te nemen dat een of meer personen uit de omgeving van de persoon op wie de machtiging betrekking heeft, informatie kunnen verstrekken voor het doel waarvoor de machtiging is verleend, […] de machtiging ook individueel voor elk van die personen [kan] worden verleend'.

184 De gegevens waarop een dergelijke maatregel betrekking heeft, stellen de bevoegde nationale autoriteiten in staat om voor de duur van de machtiging continu en in real time in de gaten te houden met wie, met welke middelen en hoelang de betrokken personen communiceren, alsook waar zij verblijven en waarheen zij zich verplaatsen. Ook lijkt uit die gegevens de aard van de online geraadpleegde informatie te kunnen worden afgeleid. Zoals uit punt 117 van het onderhavige arrest blijkt, kunnen uit die gegevens, in hun geheel genomen, zeer precieze conclusies worden getrokken over het privéleven van de betrokken personen, en kan aan de hand van die gegevens het profiel van deze personen worden bepaald, informatie die vanuit het oogpunt van het recht op eerbiediging van het privéleven even gevoelig is als de inhoud zelf van de communicatie.

185 Met betrekking tot de in artikel L. 851-4 CSI geregelde opvraging in real time van gegevens moet worden opgemerkt dat op grond van deze bepaling technische gegevens betreffende de locatie van de eindapparatuur kunnen worden opgevraagd en in real time kunnen worden doorgezonden aan een onder de eerste minister ressorterende dienst. Dergelijke gegevens stellen de bevoegde dienst in staat om voor de duur van de machtiging continu en in real time de locatie te bepalen van gebruikte eindapparatuur, zoals mobiele telefoons.

186 Een nationale regeling die een dergelijke opvraging in real time van gegevens toestaat, wijkt — net zoals nationale wetgeving die de geautomatiseerde analyse van gegevens toestaat — af van de in artikel 5 van richtlijn 2002/58 neergelegde principeverplichting om de vertrouwelijkheid van de elektronische communicatie en van de daarmee verband houdende gegevens te waarborgen. Zij vormt derhalve ook een inmenging in de in de artikelen 7 en 8 van het Handvest verankerde grondrechten en kan een ontmoedigend effect hebben op de uitoefening van de door artikel 11 van het Handvest gewaarborgde vrijheid van meningsuiting.

187 Benadrukt dient te worden dat de inmenging die de opvraging in real time van gegevens aan de hand waarvan een eindapparaat kan worden gelokaliseerd, met zich brengt, bijzonder ernstig is, aangezien die gegevens de bevoegde nationale autoriteiten in staat stellen om de verplaatsingen van gebruikers van mobiele telefoons nauwkeurig en permanent te volgen. Aangezien dergelijke gegevens dus als bijzonder gevoelig moeten worden beschouwd, dient de realtimetoegang van de bevoegde autoriteiten tot die gegevens te worden onderscheiden van de toegang daartoe die niet in real time plaatsvindt. De eerste soort toegang is ingrijpender omdat deze het mogelijk maakt om vrijwel alle gangen van de betrokken gebruikers na te gaan (zie naar analogie, met betrekking tot artikel 8 EVRM, EHRM, 8 februari 2018, *Ben Faiza tegen Frankrijk*, CE:ECHR:2018:0208JUD003144612, § 74). Die inmenging gaat nog verder wanneer de opvraging in real time zich ook uitstrekt tot de verkeersgegevens van de betrokken personen.

188 De doelstelling van voorkoming van terrorisme die met de in het hoofdgeding aan de orde zijnde nationale regeling wordt nagestreefd, kan weliswaar wegens het belang ervan de inmenging rechtvaardigen die de opvraging in real time van verkeers- en locatiegegevens met zich brengt, maar een dergelijke maatregel kan, gelet op het bijzonder ingrijpende karakter ervan, slechts worden toegepast met betrekking tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten. De gegevens van niet tot deze categorie behorende personen kunnen uitsluitend openstaan voor niet-realtime-toegang, die overeenkomstig de rechtspraak van het Hof slechts kan worden verleend in bijzondere situaties, zoals die waarin terroristische activiteiten aan de orde zijn, en wanneer op grond van objectieve factoren kan worden geoordeeld dat deze gegevens in het concrete geval daadwerkelijk tot de bestrijding van terrorisme zouden kunnen bijdragen (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 119 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak).

189 Bovendien moet een beslissing waarbij machtiging wordt verleend voor de opvraging in real time van verkeers- en locatiegegevens, gebaseerd zijn op objectieve, in de nationale wetgeving vastgestelde criteria. Die wetgeving moet overeenkomstig de in punt 176 van het onderhavige arrest aangehaalde rechtspraak in het bijzonder aangeven in welke omstandigheden en onder welke voorwaarden een dergelijke opvraging kan worden toegestaan, en bepalen dat, zoals in het voorgaande punt is gepreciseerd, deze maatregel slechts kan worden toegepast met betrekking tot personen die in verband kunnen worden gebracht met de doelstelling van voorkoming van terrorisme. Om te garanderen dat deze voorwaarden in de praktijk ten volle in acht worden genomen, is het van wezenlijk belang dat de toepassing van de maatregel waarbij machtiging wordt verleend voor de opvraging in real time van gegevens, is onderworpen aan voorafgaande rechterlijke toetsing door een rechterlijke instantie of een onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij die instantie of autoriteit zich met name ervan dient te vergewissen dat die opvraging slechts wordt toegestaan binnen de grenzen van het strikt noodzakelijke (zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 120 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*)). In naar beho-

ren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden.

Informatieverstrekking aan de personen van wie de gegevens zijn opgevraagd of geanalyseerd

190 Het is van belang dat de bevoegde nationale autoriteiten die in real time verkeers- en locatiegegevens opvragen, de betrokken personen in het kader van de toepasselijke nationale procedures daarover informeren zodra deze informatieverstrekking geen gevaar meer kan opleveren voor de taken die zij moeten uitvoeren. Deze informatieverstrekking is immers noodzakelijk om die personen in staat te stellen hun uit de artikelen 7 en 8 van het Handvest voortvloeiende rechten uit te oefenen, inzage te vragen in de persoonsgegevens die in real time zijn opgevraagd, en in voorkomend geval rectificatie of vernietiging van die gegevens te verlangen, alsook overeenkomstig artikel 47, eerste alinea, van het Handvest een doeltreffende voorziening in rechte in te stellen. Dat recht van beroep wordt overigens uitdrukkelijk gewaarborgd door artikel 15, lid 2, van richtlijn 2002/58, gelezen in samenhang met artikel 79, lid 1, van verordening 2016/679 [zie in die zin arrest van 21 december 2016, *Tele2*, C-203/15 en C-698/15, EU:C:2016:970, punt 121 (*NJ* 2017/186, m.nt. E.J. Dommering*; red.*) en aldaar aangehaalde rechtspraak, en *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017 2017, EU:C:2017:592, punten 219 en 220].

191 Wat de in het kader van een geautomatiseerde analyse van verkeers- en locatiegegevens te verstrekken informatie betreft, moet worden opgemerkt dat de bevoegde nationale autoriteit verplicht is om algemene inlichtingen inzake die analyse te publiceren, maar de betrokken personen niet individueel hoeft in te lichten. Wanneer die gegevens beantwoorden aan de parameters die zijn bepaald in de maatregel waarbij machtiging is verleend voor de geautomatiseerde analyse, en die autoriteit de betrokken persoon identificeert met als doel om de op hem of haar betrekking hebbende gegevens nader te analyseren, is het daarentegen wel noodzakelijk om die persoon individueel te informeren. Een dergelijke informatieverstrekking mag evenwel pas geschieden zodra dit geen gevaar meer kan opleveren voor de door die autoriteit uit te voeren taken [zie naar analogie *advies 1/15 (PNR-Overeenkomst EU-Canada)* van 26 juli 2017, EU:C:2017:592, punten 222-224].

192 Gelet op een en ander moet op de tweede en de derde vraag in zaak C-511/18 worden geantwoord dat artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich niet verzet tegen een nationale regeling die aanbieders van elektronischecommunicatiediensten verplicht om, ten eerste, met name verkeers- en locatiegegevens op geautomatiseerde wijze te analyseren en in real time op te vragen, en, ten tweede, technische gegevens over de locatie van de gebruikte eindapparatuur in real time op te vragen, wanneer

- die geautomatiseerde analyse beperkt is tot situaties waarin de betrokken lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en de toepassing van die analyse effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of er sprake is van een situatie die de genoemde maatregel rechtvaardigt en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien, en wanneer
- het in real time opvragen van verkeers- en locatiegegevens beperkt is tot personen ten aanzien van wie er een geldige reden bestaat om te vermoeden dat zij op de een of andere manier betrokken zijn bij terroristische activiteiten, en is onderworpen aan voorafgaande toetsing door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, om ervoor te zorgen dat een dergelijke maatregel slechts wordt toegestaan binnen de grenzen van het strikt noodzakelijke. In naar behoren gemotiveerde urgente gevallen dient die toetsing op korte termijn plaats te vinden.

Tweede vraag in zaak C-512/18

193 Met de tweede vraag in zaak C-512/18 wenst de verwijzende rechter in wezen te vernemen of de bepalingen van richtlijn 2000/31, gelezen in het licht van de artikelen 6 tot en met 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moeten worden uitgelegd dat zij zich verzetten tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd.

194 De verwijzende rechter, die van mening is dat dergelijke diensten binnen de werkingssfeer van richtlijn 2000/31 en niet binnen die van richtlijn 2002/58 vallen, stelt zich op het standpunt dat artikel 15, leden 1 en 2, van richtlijn 2000/31, gelezen in samenhang met de artikelen 12 en 14 van deze richtlijn, als zodanig geen principieel verbod op het bewaren van gegevens inzake de creatie van inhoud invoert waarvan slechts bij wijze van uitzondering zou kunnen worden afgeweken. Hij vraagt zich niettemin af of dit standpunt aanvaardbaar is, gelet op de noodzaak om de in de artikelen 6 tot en met 8 en 11 van het Handvest verankerde grondrechten te eerbiedigen.

195 De verwijzende rechter verduidelijkt voorts dat zijn vraag ziet op de bewaarplicht die is neergelegd in artikel 6 LCEN, gelezen in samenhang met decreet nr. 2011-219. Tot de gegevens die de betrokken aanbieders van diensten uit dien hoofde dienen te bewaren, behoren onder meer de gegevens betreffende de burgerlijke identiteit van de personen die van die diensten hebben gebruikge-

maakt, zoals hun naam, voornaam, hun bijbehorende postadressen, hun bijbehorende e-mail- of accountadressen, hun wachtwoorden en, wanneer het ondertekenen van het contract of het aanmaken van het account plaatsvindt tegen betaling, de gebruikte betaalsoort, de betalingsreferentie, het bedrag en de datum en het tijdstip van de transactie.

196 Tot de te bewaren gegevens behoren ook de identificatoren van de abonnees, van de verbindingen en van de gebruikte eindapparatuur, de aan de inhoud toegekende identificatoren, de datum en het tijdstip van het begin en het einde van de verbindingen en verrichtingen, en de soorten protocollen die zijn gebruikt voor de verbinding met de dienst en voor de overdracht van de inhoud. De bewaartermijn voor die gegevens bedraagt één jaar en er kan om toegang tot die gegevens worden verzocht in het kader van strafrechtelijke en civielrechtelijke procedures, om de regels inzake civielrechtelijke of strafrechtelijke aansprakelijkheid te doen naleven, en in het kader van maatregelen voor het inwinnen van inlichtingen waarop artikel L. 851-1 CSI van toepassing is.

197 In dit verband moet worden opgemerkt dat richtlijn 2000/31 volgens artikel 1, lid 2, bepaalde nationale bepalingen nader tot elkaar brengt die van toepassing zijn op de diensten van de informatiemaatschappij in de zin van artikel 2, onder a).

198 Tot die diensten behoren onder meer die welke op individueel verzoek van een afnemer van diensten en gewoonlijk tegen vergoeding worden verricht via elektronische apparatuur voor de verwerking en de opslag van gegevens op afstand, zoals diensten waarbij toegang wordt verschaft tot het internet of tot een communicatienetwerk, en opslagdiensten (zie in die zin arresten van 24 november 2011, *Scarlet Extended*, C-70/10, EU:C:2011:771, punt 40 (*NJ* 2012/479, m.nt. P.B. Hugenholtz*; red.*); 16 februari 2012, *SABAM*, C-360/10, EU:C:2012:85, punt 34 (*NJ* 2012/480, m.nt. P.B. Hugenholtz*; red.*); 15 september 2016, *Mc Fadden*, C-484/14, EU:C:2016:689, punt 55, en 7 augustus 2018, *SNB-REACT*, C-521/17, EU:C:2018:639, punt 42 en aldaar aangehaalde rechtspraak).

199 Artikel 1, lid 5, van richtlijn 2000/31 bepaalt evenwel dat deze richtlijn niet van toepassing is op kwesties in verband met diensten van de informatiemaatschappij die onder richtlijnen 95/46 en 97/66 vallen. Dienaangaande blijkt uit de overwegingen 14 en 15 van richtlijn 2000/31 dat de bescherming van het vertrouwelijke karakter van communicatie en van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de diensten van de informatiemaatschappij uitsluitend wordt beheerst door richtlijnen 95/46 en 97/66. Laatstgenoemde richtlijn stelt ter waarborging van de vertrouwelijkheid van communicatie in artikel 5 een verbod op iedere vorm van onderschepping of bewaking van berichten.

200 Vragen die verband houden met de bescherming van het vertrouwelijke karakter van communicatie en van persoonsgegevens moeten derhalve worden beoordeeld aan de hand van richtlijn 2002/58 en verordening 2016/679, die in de plaats zijn gekomen van, respectievelijk, richtlijn 97/66 en richtlijn 95/46, waarbij moet worden aangetekend dat de bescherming die richtlijn 2000/31 beoogt te verzekeren, hoe dan ook geen afbreuk mag doen aan de vereisten die voortvloeien uit richtlijn 2002/58 en verordening 2016/679 (zie in die zin arrest van 29 januari 2008, *Promusicae*, C-275/06, EU:C:2008:54, punt 57 (*NJ* 2009/551, m.nt. P.B. Hugenholtz*; red.*)).

201 De bewaarplicht die de in punt 195 van het onderhavige arrest bedoelde nationale regeling oplegt aan aanbieders die het publiek online toegang geven tot communicatiediensten en aanbieders van opslagdiensten, en die betrekking heeft op de met die diensten verband houdende persoonsgegevens, moet dus worden getoetst aan richtlijn 2002/58 of verordening 2016/679, zoals de advocaat-generaal in wezen heeft opgemerkt in punt 141 van zijn conclusie in de gevoegde zaken *La Quadrature du Net e.a.* (C-511/18 en C-512/18, EU:C:2020:6).

202 Afhankelijk van de vraag of de levering van de diensten waarop die nationale regeling betrekking heeft, al dan niet onder richtlijn 2002/58 valt, zal die levering derhalve ofwel worden beheerst door deze richtlijn, in het bijzonder door artikel 15, lid 1, ervan, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, ofwel door verordening 2016/679, in het bijzonder door artikel 23, lid 1, van deze verordening, gelezen in het licht van dezelfde bepalingen van het Handvest.

203 Zoals de Europese Commissie in haar schriftelijke opmerkingen heeft gesteld, valt in casu niet uit te sluiten dat sommige van de diensten waarop de in punt 195 van het onderhavige arrest bedoelde nationale regeling betrekking heeft, elektronischecommunicatiediensten in de zin van richtlijn 2002/58 zijn, hetgeen de verwijzende rechter dient na te gaan.

204 In dit verband moet worden opgemerkt dat richtlijn 2002/58 van toepassing is op elektronischecommunicatiediensten die voldoen aan de voorwaarden die vermeld staan in artikel 2, onder c), van richtlijn 2002/21, waarnaar artikel 2 van richtlijn 2002/58 verwijst en waarin een elektronischecommunicatiedienst wordt gedefinieerd als 'een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronischecommunicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt'. Wat de door richtlijn 2000/31 bestreken diensten van de informatiemaatschappij als bedoeld in de punten 197 en 198 van het onderhavige arrest betreft, deze diensten zijn elektronischecommunicatiediensten indien zij geheel of hoofdzakelijk bestaan in het overbrengen van signalen via elektronischecommunicatienetwerken (zie in die zin arrest van 5 juni 2019, *Skype Communications*, C-142/18, EU:C:2019:460, punten 47 en 48).

205 Internettoegangsdiensten, waarop de in punt 195 van het onderhavige arrest bedoelde nationale regeling van toepassing lijkt te zijn, zijn derhalve elektronischecommunicatiediensten in de zin van richtlijn 2002/21, zoals in overweging 10 van deze richtlijn wordt bevestigd (zie in die zin arrest van 5 juni 2019, *Skype Communications*, C-142/18, EU:C:2019:460, punt 37). Dit geldt ook voor webgebaseerde e-maildiensten, die mogelijk eveneens onder die nationale regeling vallen, aangezien die diensten technisch gezien kunnen worden beschouwd als diensten die geheel of hoofdzakelijk bestaan in het overbrengen van signalen via elektronischecommunicatienetwerken (zie in die zin arrest van 13 juni 2019, *Google*, C-193/18, EU:C:2019:498, punten 35 en 38).

206 Wat de vereisten betreft die voortvloeien uit artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zij verwezen naar alle vaststellingen en beoordelingen in het kader van de beantwoording van de eerste vraag in de zaken C-511/18 en C-512/18 en de eerste en de tweede vraag in zaak C-520/18.

207 Wat de uit verordening 2016/679 voortvloeiende vereisten betreft, zij eraan herinnerd dat deze verordening, zoals blijkt uit overweging 10 ervan, met name een consistent en hoog niveau van bescherming van natuurlijke personen binnen de Unie beoogt te waarborgen en daartoe een coherente en homogene toepassing van de regels inzake bescherming van de grondrechten van deze personen in verband met de verwerking van persoonsgegevens binnen de gehele Unie wil verzekeren (zie in die zin arrest van 16 juli 2020, *Facebook Ireland en Schrems*, C-311/18, EU:C:2020:559, punt 101 (*NJ* 2021/24, m.nt. E.J. Dommering*; red.*)).

208 Daartoe moeten bij elke verwerking van persoonsgegevens, behoudens de op grond van artikel 23 van verordening 2016/679 toegestane uitzonderingen, de in hoofdstuk II van deze verordening neergelegde beginselen inzake verwerking van persoonsgegevens en de in hoofdstuk III van deze verordening geregelde rechten van de betrokkene worden geëerbiedigd. In het bijzonder moet elke verwerking van persoonsgegevens ten eerste in overeenstemming zijn met de in artikel 5 van verordening 2016/679 geformuleerde beginselen, en ten tweede voldoen aan de in artikel 6 van deze verordening opgesomde rechtmatigheidsvoorwaarden (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 30 mei 2013, *Worten*, C-342/12, EU:C:2013:355, punt 33 en aldaar aangehaalde rechtspraak).

209 Wat meer bepaald artikel 23, lid 1, van verordening 2016/679 betreft, moet worden opgemerkt dat deze bepaling — net als artikel 15, lid 1, van richtlijn 2002/58 — de lidstaten de mogelijkheid biedt om met het oog op de erin genoemde doelstellingen via wetgevingsmaatregelen de reikwijdte van de erin bedoelde verplichtingen en rechten te beperken, 'op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van' het nagestreefde doel. Elke op die grondslag vastgestelde wettelijke maatregel moet met name voldoen aan de specifieke vereisten die zijn geformuleerd in artikel 23, lid 2, van verordening 2016/679.

210 Artikel 23, leden 1 en 2, van verordening 2016/679 kan derhalve niet aldus worden uitgelegd dat het de lidstaten de bevoegdheid kan verlenen om afbreuk te doen aan de eerbiediging van de persoonlijke levenssfeer, in strijd met artikel 7 van het Handvest, of aan de andere door het Handvest geboden waarborgen (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 20 mei 2003, arrest van 20 mei 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01 en C-139/01, EU:C:2003:294, punt 91 (*NJ* 2005/15*; red.*)). Net zoals geldt voor artikel 15, lid 1, van richtlijn 2002/58, is het met name zo dat de bevoegdheid die artikel 23, lid 1, van verordening 2016/679 de lidstaten verleent, slechts kan worden uitgeoefend in overeenstemming met het evenredigheidsvereiste, dat verlangt dat uitzonderingen op de bescherming van persoonsgegevens en beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven (zie naar analogie, met betrekking tot richtlijn 95/46, arrest van 7 november 2013, *IPI*, C-473/12, EU:C:2013:715, punt 39 en aldaar aangehaalde rechtspraak).

211 Bijgevolg gelden de vaststellingen die zijn gedaan in het kader van de beantwoording van de eerste vraag in de zaken C-511/18 en C-512/18 en van de eerste en de tweede vraag in zaak C-520/18, en de beoordelingen die in dat kader zijn verricht, mutatis mutandis voor artikel 23 van verordening 2016/679.

212 Gelet op een en ander moet op de tweede vraag in zaak C-512/18 worden geantwoord dat richtlijn 2000/31 aldus moet worden uitgelegd dat zij niet van toepassing is op de bescherming van het vertrouwelijke karakter van communicatie en van natuurlijke personen in verband met de verwerking van persoonsgegevens in het kader van de diensten van de informatiemaatschappij. Deze bescherming wordt, naargelang van het geval, beheerst door richtlijn 2002/58 of verordening 2016/679. Artikel 23, lid 1, van verordening 2016/679, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, moet aldus worden uitgelegd dat het zich verzet tegen een nationale regeling waarbij aanbieders die het publiek online toegang verlenen tot communicatiediensten en aanbieders van opslagdiensten een verplichting tot algemene en ongedifferentieerde bewaring van met name de met die diensten verband houdende persoonsgegevens wordt opgelegd.

Derde vraag in zaak C-520/18

213 Met de derde vraag in zaak C-520/18 wenst de verwijzende rechter in wezen te vernemen of

een nationale rechterlijke instantie een bepaling van haar nationale recht mag toepassen die haar machtigt om de werking in de tijd van een onwettigverklaring te beperken wanneer hij op grond van dit recht een nationale wettelijke regeling die ten behoeve van onder meer de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens oplegt, onwettig dient te verklaren omdat zij onverenigbaar is met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest.

214 Het beginsel van het primaat van het Unierecht houdt in dat dit recht voorrang heeft op het recht van de lidstaten. Dit beginsel verplicht dus alle instanties van de lidstaten om volle werking te verlenen aan de verschillende normen van de Unie, aangezien het recht van de lidstaten niet kan afdoen aan de werking die op het grondgebied van die staten aan deze verschillende normen is verleend [arrest van 15 juli 1964, *Costa*, 6/64, EU:C:1964:66, blz. 1219 en 1220, en 19 november 2019, *A. K. e.a. (Onafhankelijkheid van de tuchtkamer van de Sąd NajwyŻszy)*, C-585/18, C-624/18 en C-625/18, EU:C:2019:982, punten 157 en 158 en aldaar aangehaalde rechtspraak].

215 Het voorrangsbeginsel brengt mee dat, indien de nationale regelgeving niet in overeenstemming met de vereisten van het Unierecht kan worden uitgelegd, de nationale rechter die in het kader van zijn bevoegdheid is belast met de toepassing van de bepalingen van het Unierecht, verplicht is de volle werking van deze bepalingen te verzekeren en daarbij zo nodig, op eigen gezag, elke, zelfs latere, strijdige bepaling van de nationale wettelijke regeling buiten toepassing te laten, zonder dat hij de voorafgaande opheffing hiervan via de wetgeving of enige andere constitutionele procedure hoeft te vragen of af te wachten [arresten van 22 juni 2010, *Melki en Abdeli*, C-188/10 en C-189/10, EU:C:2010:363, punt 43 en aldaar aangehaalde rechtspraak; 24 juni 2019, *Popławski*, C-573/17, EU:C:2019:530, punt 58 (*NJ* 2020/104*; red.*), en 19 november 2019, *A. K. e.a. (Onafhankelijkheid van de tuchtkamer van de Sąd NajwyŻszy)*, C-585/18, C-624/18 en C-625/18, EU:C:2019:982, punt 160].

216 Enkel het Hof kan, bij wijze van uitzondering en om dwingende redenen van rechtszekerheid, een voorlopige opschorting toestaan van het effect dat een regel van het Unierecht op het daarmee strijdige nationale recht heeft, namelijk de terzijdestelling daarvan. Een dergelijke beperking in de tijd van de werking van de door het Hof aan het Unierecht gegeven uitlegging kan slechts worden vastgesteld in het arrest waarin de gevraagde uitlegging wordt gegeven [zie in die zin arresten van 23 oktober 2012, *Nelson e.a.*, C-581/10 en C-629/10, EU:C:2012:657, punten 89 en 91 (*NJ* 2013/4, m.nt. M.R. Mok*; red.*); 23 april 2020, *Herst*, C-401/18, EU:C:2020:295, punten 56 en 57, en 25 juni 2020, *A e.a. (Windturbines in Aalter en Nevele)*, C-24/19, EU:C:2020:503, punt 84 en aldaar aangehaalde rechtspraak].

217 Aan de voorrang en de uniforme toepassing van het Unierecht zou afbreuk worden gedaan indien de nationale rechterlijke instanties bevoegd waren om, al was het maar tijdelijk, aan nationale bepalingen voorrang te geven boven het Unierecht waarmee deze bepalingen in strijd zijn (zie in die zin arrest van 29 juli 2019, *Inter-Environnement Wallonie en Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, punt 177 en aldaar aangehaalde rechtspraak).

218 Het Hof heeft evenwel in een zaak waarin het draaide om de rechtmatigheid van maatregelen die waren vastgesteld in strijd met de Unierechtelijke verplichting om een voorafgaande beoordeling te verrichten van de gevolgen van een project voor het milieu of voor een beschermd gebied, geoordeeld dat een nationale rechterlijke instantie, indien het nationale recht dat toestaat, bij wijze van uitzondering de gevolgen van dergelijke maatregelen kan handhaven indien deze handhaving wordt gerechtvaardigd door dwingende redenen die verband houden met de noodzaak om het reële en ernstige risico af te wenden dat de elektriciteitsbevoorrading van de betrokken lidstaat wordt onderbroken, en aan dit risico niet het hoofd zou kunnen worden geboden met andere middelen en alternatieven, met name in het kader van de interne markt, met dien verstande dat die handhaving niet langer kan duren dan strikt noodzakelijk is om een einde te maken aan die onrechtmatigheid (zie in die zin arrest van 29 juli 2019, *Inter-Environnement Wallonie en Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, punten 175, 176, 179 en 181).

219 Anders dan de niet-nakoming van een procedurele verplichting als de voorafgaande beoordeling van de gevolgen van een project op het specifieke terrein van de milieubescherming, kan een schending van artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, niet worden geregulariseerd via een procedure die vergelijkbaar is met die waaraan in het voorgaande punt wordt gerefereerd. Handhaving van de gevolgen van een nationale wettelijke regeling als in het hoofdgeding aan de orde is, zou immers betekenen dat die regeling aan aanbieders van elektronischecommunicatiediensten verplichtingen blijft opleggen die in strijd zijn met het Unierecht en leiden tot een ernstige inmenging in de grondrechten van de personen van wie de gegevens zijn bewaard.

220 Hieruit volgt dat de verwijzende rechter geen bepaling van zijn nationale recht mag toepassen die hem machtigt om de werking in de tijd te beperken van een door hem op grond van dit recht uit te spreken onwettigverklaring van de in het hoofdgeding aan de orde zijnde nationale wettelijke regeling.

221 VZ, WY en XX stellen in hun bij het Hof ingediende schriftelijke opmerkingen dat de derde

vraag impliciet maar noodzakelijkerwijs de vraag opwerpt of het Unierecht zich ertegen verzet dat in het kader van een strafrechtelijke procedure wordt gebruikgemaakt van informatie en bewijzen die zijn verkregen door middel van een met dit recht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens.

222 Om de verwijzende rechter een nuttig antwoord te verstrekken, zij er in dit verband aan herinnerd dat het bij de huidige stand van het Unierecht uitsluitend een zaak van het nationale recht is om de regels vast te stellen met betrekking tot de aanvaarding en de beoordeling van door middel van een dergelijke met het Unierecht strijdige gegevensbewaring verkregen informatie en bewijzen in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van ernstige strafbare feiten.

223 Het is immers vaste rechtspraak dat het bij gebreke van Unieregelgeving ter zake krachtens het beginsel van procedurele autonomie een aangelegenheid van de interne rechtsorde van elke lidstaat is om de procedureregels vast te stellen voor rechtsvorderingen die ertoe strekken de rechten die de justitiabelen aan het Unierecht ontlenen, te beschermen, op voorwaarde evenwel dat die regels niet ongunstiger zijn dan die welke voor soortgelijke situaties naar nationaal recht gelden (gelijkwaardigheidsbeginsel) en de uitoefening van de door het Unierecht verleende rechten in de praktijk niet onmogelijk of uiterst moeilijk maken (doeltreffendheidsbeginsel) (zie in die zin arresten van 6 oktober 2015, *Târşia*, C-69/14, EU:C:2015:662, punten 26 en 27 (*NJ* 2016/232, m.nt. B.J. Drijber*; red.*); 24 oktober 2018, *XC e.a.*, C-234/17, EU:C:2018:853, punten 21 en 22 en aldaar aangehaalde rechtspraak, en 19 december 2019, *Deutsche Umwelthilfe*, C-752/18, EU:C:2019:1114, punt 33).

224 Wat het gelijkwaardigheidsbeginsel betreft, staat het aan de nationale rechter bij wie een strafrechtelijke procedure is aangebracht die gebaseerd is op informatie of bewijzen die in strijd met de uit richtlijn 2002/58 voortvloeiende vereisten zijn verkregen, om na te gaan of het op die procedure van toepassing zijnde nationale recht minder gunstige regels bevat voor de aanvaarding en het gebruik van dergelijke informatie en bewijzen dan voor de aanvaarding en het gebruik van informatie en bewijzen die zijn verkregen in strijd met het interne recht.

225 Met betrekking tot het doeltreffendheidsbeginsel moet worden opgemerkt dat nationale regels inzake de aanvaarding en het gebruik van informatie en bewijzen tot doel hebben om in overeenstemming met de in het nationale recht gemaakte keuzen te voorkomen dat onrechtmatig verkregen informatie en bewijzen ongerechtvaardigd nadeel toebrengen aan een persoon die ervan wordt verdacht strafbare feiten te hebben gepleegd. Dat doel kan naar nationaal recht niet alleen worden bereikt door middel van een verbod op het gebruik van dergelijke informatie en bewijzen, maar ook door middel van nationale regels en praktijken met betrekking tot de beoordeling en de weging van de informatie en de bewijzen, of door de inaanmerkingneming van het onrechtmatige karakter ervan bij de straftoemeting.

226 Uit de rechtspraak van het Hof volgt dat bij de beoordeling of informatie en bewijzen die in strijd met de voorschriften van het Unierecht zijn verkregen, moeten worden uitgesloten, met name moet worden nagegaan of de aanvaarding van dergelijke informatie en bewijzen schending van het beginsel van hoor en wederhoor en dus ook van het recht op een eerlijk proces tot gevolg kan hebben (zie in die zin arrest van 10 april 2003, *Steffensen*, C-276/01, EU:C:2003:228, punten 76 en 77). Een rechterlijke instantie die van oordeel is dat een partij niet in de gelegenheid is om doeltreffend commentaar te leveren op een bewijsmiddel dat betrekking heeft op een gebied waarvan de rechters geen kennis hebben en dat een doorslaggevende invloed kan hebben op de beoordeling van de feiten, moet vaststellen dat het recht op een eerlijk proces hierdoor wordt geschonden, en dat bewijsmiddel uitsluiten om die schending te voorkomen (zie in die zin arrest van 10 april 2003, *Steffensen*, C-276/01, EU:C:2003:228, punten 78 en 79).

227 Bijgevolg brengt het doeltreffendheidsbeginsel voor de nationale strafrechter de verplichting mee om informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten.

228 Gelet op een en ander moet op de derde vraag in zaak C-520/18 worden geantwoord dat een nationale rechterlijke instantie geen bepaling van haar nationale recht mag toepassen die haar machtigt om de werking in de tijd te beperken van de door haar op grond van dit recht uit te spreken onwettigverklaring van een nationale wettelijke regeling waarbij ten behoeve van met name de bescherming van de nationale veiligheid en de bestrijding van criminaliteit aan aanbieders van elektronischecommunicatiediensten een verplichting tot algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens wordt opgelegd die onverenigbaar is met artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest. Op grond van artikel 15, lid 1, uitgelegd in het licht van het doeltreffendheidsbeginsel, dient de nationale strafrechter informatie en bewijzen die door middel van een met het Unierecht onverenigbare algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens zijn verkregen, in het kader van een strafrechtelijke procedure tegen

personen die worden verdacht van strafbare handelingen buiten beschouwing te laten indien die personen niet in de gelegenheid zijn om doeltreffend commentaar te leveren op die informatie en die bewijzen, die betrekking hebben op een gebied waarvan de rechter geen kennis heeft en een doorslaggevende invloed kunnen hebben op de beoordeling van de feiten.

(…)

Het Hof (Grote kamer) verklaart voor recht: [zie *cursieve* kop].

Noot

I. Inleiding en de feiten in de verschillende zaken

1. In deze (Britse resp. Frans-Belgische) zaken staat de verwerking van persoonsgegevens door nationale inlichtingendiensten centraal. Zij hebben zowel bij het EHRM als het HvJ EU een pendant in op dezelfde dag gewezen uitspraken in gevoegde zaken, t.w. een Zweedse zaak bij het EHRM: *Centrum för Rättvisa/Zweden* (Application no. 35252/08) en een Britse zaak bij het HvJ EU: *Privacy International* (C-623/17). De twee uitspraken van het HvJ EU zijn al ter sprake gekomen in mijn noot bij het arrest *Schrems II* van het HvJ EU (16 juli 2020, zaak C-311/18 *NJ* 2021/24, noot onder punt 5). Verder zijn er bij het HvJ EU nog aanhangig de gevoegde zaken C-215/20 en C-222/20, resp. C-793/19 en C-140/20. Alle uitspraken zullen hierna besproken worden, maar om redenen van beperking van ruimte worden alleen deze twee gepubliceerd omdat de twee hoven zich daarin het meest volledig hebben uitgelaten. Het gaat in alle gevallen om uitspraken van de Grand Chambers van beide colleges.

2. De juridische positie van de inlichtingendiensten is ingewikkeld omdat zij eigenlijk in geen enkel model van bestuursrechtelijke of strafrechtelijke rechtsbescherming passen en zij ook in het privacyrecht een eigen positie innemen. Verder is er een verstrengeling van politiek en juridisch toezicht en zijn er vele politieke instanties (ministeries, parlement) bij betrokken. De organisatie van de diensten zelf verschilt per land. In vele landen zijn er meer diensten, al naar gelang doelstelling, interceptietechniek en binnen- of buitenlands object van onderzoek, soms (zoals in het Zweedse geval) gespecialiseerd toezicht. In Nederland is die organisatiestructuur geleidelijk aan teruggebracht tot twee diensten: de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), waarvan de juridische status en bevoegdheden zijn geregeld in de Wet op de inlichtingen- en veiligheidsdiensten, in 2017 ingrijpend vernieuwd (Wiv 2017, *Stb.* 317). Die vernieuwing was een uitvoering van de aanbevelingen van de Commissie Dessens uit 2013. Deze nieuwe wet is, nadat zij was vastgesteld, politiek in discussie gekomen omdat zij te veel bevoegdheden aan de diensten zou geven. De diensten zouden een 'sleepnet' over de samenleving kunnen werpen waar iedereen in gevangen zou kunnen worden. Dit heeft geleid tot een referendum over de 'sleepwet' dat 'nee' tegen de wet zei. Dit was aanleiding om de wet aan te passen en er is binnen twee jaar een evaluatie van de wet toegezegd die inmiddels is uitgevoerd (Evaluatie 2020, Wiv 2017, https://www.rijksoverheid.nl/documenten/rapporten/2021/01/20/rapport-evaluatie-2020-wet-op-de-inlichtingen-en-veiligheidsdiensten-2017).[1]

De ontwikkeling van de informatie- en communicatietechnologie vergroot die complicaties. De juridische wereld is bezig zich te verplaatsen van de echte wereld naar de virtuele wereld van cyberspace, maar die ontwikkeling gaat bij de inlichtingendiensten nog sneller. De grens tussen binnen- en buitenland is immers vervaagd en daardoor zijn de activiteiten van de inlichtingendiensten moeilijk te lokaliseren.

Gelet op deze complicaties is het van belang de feiten nauwkeurig te omschrijven en de informatiestromen en verwerkingsprocessen waar het om gaat precies te analyseren. De normatieve beslissingen zijn daar sterk mee verweven. Ik zal eerst die bij het EHRM en dan die bij het HvJ EU weergeven. Ter vereenvoudiging zal ik daarbij van sommige aspecten abstraheren.

Een andere complicatie is dat we te maken hebben met het recht van de Raad van Europa en de EU-rechtsorde, zodat het gaat om uitspraken van het EHRM en het HvJ EU. Daarom zal ik in II eerst behandelen hoe dat precies zit en tot wat voor soort complicaties dat leidt. In de paragrafen III t/m VI zal ik dan bepaalde belangrijke thema's uit de beslissingen van het EHRM lichten, die erop neer komen dat van een kleine omwenteling in de jurisprudentie kan worden gesproken, ook al zijn er terugkerende thema's. In VII doe ik hetzelfde voor de uitspraken van het HvJ EU en zal ik laten zien dat de aanpak van dat Hof verschilt en dat dit complicerend werkt. In VIII sta ik tenslotte stil bij wat de consequenties zijn voor Nederland en de naar aanleiding van de adviezen van de Evaluatiecommissie op stapel staande wijziging van de Wiv 2017.

De feitelijke constellaties van de zaken bij het EHRM zien er als volgt uit. De *Big Brother Watch (BBW)* zaak heeft zijn oorsprong in de *Snowden*-affaire, die aan het licht bracht dat de Amerikaanse inlichtingendiensten via onder meer een als PRISM aangeduid project op grote schaal de communicaties van niet-Amerikaanse burgers onderschepten. Britse mensenrechtenorganisaties, advocaten en journalisten beklaagden zich, omdat zij, in de bewoordingen van het EHRM 'all believed that due to the nature of their activities, their electronic communications were likely to have either been intercepted by the United Kingdom intelligence services, obtained by the United Kingdom intelligence services after being intercepted by foreign governments;

1 Ondergetekende was lid van deze commissie.

and/or obtained by the United Kingdom authorities from communications service providers'. Zij waren dus bevreesd dat deze gegevens onder meer ook via het 'Amerikaanse lek' in handen waren gekomen van Britse autoriteiten. Maar het ging ook om mogelijk rechtstreekse onderschepping daarvan door de Britse diensten. De Britse inlichtingendienst "was running an operation, codenamed 'TEMPORA', which allowed it to tap into and store huge volumes of data drawn from bearers. The United Kingdom authorities neither confirmed nor denied the existence of an operation codenamed TEMPORA." (voor de details verwijs ik naar de overwegingen 17 e.v., van het EHRM). Zowel in het Amerikaanse (PRISM, zie overweging 22 e.v.) als in het Britse geval (het al genoemde TEMPORA) ging het om zogenaamde 'bulkinterceptie'. Ik citeer de definitie van 'bulkdata' uit het rapport van de Evaluatiecommissie WIV 2017 (Den Haag: Ministerie BZK 2021), p. 39: "Bulkdata is een omvangrijke verzameling van gegevens waarvan het merendeel betrekking heeft op personen en organisaties die niet in onderzoek zijn van de inlichtingendiensten en dit ook nooit zullen worden." Bulk wordt gebruikt om via analyses van communicatiepatronen onbekende dreigingen (in het jargon: de 'unknown unknowns') op te sporen. Bij bulkinterceptie gebeurt dus precies het omgekeerde als in het strafrecht: in het strafrecht verzamel je informatie in de hoop een dader of daders die strafbare feiten *hebben gepleegd* te vinden, bij het inlichtingenwerk verzamel je informatie die relevant kan zijn voor het vinden van mogelijke daders om te voorkomen dat deze staatsgevaarlijke daden *gaan plegen*. Toch komt bulkinterceptie bij de uitvoering van stafrechtelijke opsporingstaken steeds meer voor, zoals uit de in november 2021 door de belangenorganisatie Privacy First gevoerde procedure tegen de Staat blijkt: hierin werd het op grote schaal fotograferen en opslaan van autokentekens aan de orde gesteld.[2]

3. In de (hier niet opgenomen) Zweedse zaak is de klacht primair gericht op een bepaalde manier van verwerving van gegevens en de verstrekking van die gegevens door de Zweedse dienst aan buitenlandse diensten. Een Zweedse mensenrechtenorganisatie voelde zich daardoor bedreigd, in de woorden van het EHRM (overweging 10) omdat: "The applicant communicates on a daily basis with individuals, organisations and companies in Sweden and abroad by email, telephone and fax. It asserts that a large part of that communication is particularly sensitive from a privacy perspective. Due to the nature of its function as a non-governmental organisation scrutinising the activities of State actors, it believes that there is a risk that its communications have been or will be intercepted and examined by way of signals intelligence." De zaak spitst zich in dit geval dus toe op mogelijke signaalinterceptie (in het jargon van de inlichtingendiensten: SIGINT) door de Zweedse inlichtingendienst, zowel via de ether als de kabel. Daarnaast gaat het — in tegenstelling tot de Britse zaak — om *verstrekking* van bulkgegevens aan buitenlandse diensten.

4. Het nationale klachtmechanisme dat aan de basis staat van beide zaken ziet er als volgt uit. In de *BBW*-zaak diende een deel van de klagers (allen geheimhouders, sommigen met verschoningsrecht, zoals advocaten en journalisten) een klacht in bij de Investigatory Power Tribunal (hierna: IPT) omdat hun elektronische communicaties via een van de verwervingskanalen *mogelijk* in de bulk verzeild zijn geraakt.

Het EHRM onderzoekt eerst de IPT. Dit (in overweging 26) wordt omschreven als: 'A specialised Tribunal (…) to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by [the Regulation of Investigatory Power Authority (hierna: RIPA)]' dat exclusief bevoegd is om bij klachten van personen dat hun persoonlijke (elektronische) communicaties door staatsautoriteiten onderschept waren, te onderzoeken of die onderschepping onrechtmatig was. Het gaat uitvoerig in op dit IPT/RIPA systeem van rechtsbescherming, en in het bijzonder ook op de 'bulk powers review' die in de UK in 2016 is uitgevoerd (overweging 163 e.v.). Vervolgens komen andere aspecten van het toezicht aan de orde. Dit is bestuurlijk toezicht in de vorm van de jaarlijkse toezichtrapporten van de Communications Commissioner (overweging 168 e.v.) en de Intelligence Services Commissioner (overweging 181 e.v.). Daarnaast bestaat er semi-rechterlijk toezicht vooraf op het verstrekken van een last tot het uitoefenen van bulkinterceptie, die door een Judicial Commissioner moet worden gegeven (het zogenaamde 'double-lock' systeem besproken in overweging 185, waarbij met name de toetsing aan artikel 8 lid 2 EVRM moet plaatsvinden).

5. In de (hier niet opgenomen) Zweedse zaak is het nationale traject als volgt. Blijkens overweging 17 is de bevoegde autoriteit de 'National Defence Radio Establishment (*Försvarets radioanstalt*; 'FRA'). Voor de uitoefening van zijn bevoegdheden zijn er zeer specifieke voorschriften opgesteld (overwegingen 19-28, zie in het bijzonder ook overwegingen 37-44, en, voor privacy: overwegingen 55-56). Het proces van 'signal intelligence' verloopt in zes fasen (overweging 29) die gaan van verzamelen tot bewerken en bewaren. Blijkens de overwegingen 30-34 moet er bovendien een rechterlijke toestemming vooraf worden gevraagd aan het Foreign Intelligence Court (*Försvarsunderrättelsedomstolen*, 'FRD'), dat een niet voor beroep vatbare beslissing geeft over de rechtmatigheid van de last. Interessant is overweging 34 waarin het EHRM uiteenzet hoe de FRD wordt samengesteld en hoe de FRD werkt. In het bijzonder verdient de aandacht dat tijdens de besloten zittingen 'the FRA as well as a privacy protection representative (*integritetsskyddsombud*) are

2 Op het moment van het schrijven van deze noot is er nog geen vonnis; voor details over de vordering, zie: https://www.privacyfirst.nl/images/stories/PDFs/20211110_DEF_Pleitaantekeningen.pdf — geraadpleegd 24 november 2021).

present.' De laatste is een soort ombudsman/advocaat algemeen belang die de privacybelangen en rechten van het publiek vertegenwoordigt.

Daarnaast (overweging 50 e.v.) is er bestuurlijk toezicht op buitenlandse activiteiten door een autoriteit aangeduid als 'Foreign Intelligence Inspectorate (FII)', waavan voorzitter en vice-voorzitter (ex)-rechters zijn. Deze ziet toe op onder meer 'compliance with the Signals Intelligence Act by examining in particular the selectors used, the destruction of intelligence and the communication of reports; if an inspection reveals that a particular intelligence collection is incompatible with a permit, the Inspectorate may decide that the operation shall cease or that the intelligence shall be destroyed'.

De privacy-toezichthouder is ook betrokken (overwegingen 55-57, 70). Deze heeft eigen onderzoeksbevoegdheden en zelfs de mogelijkheid aan de bestuursrechter in Stockholm vernietiging te vragen van ten onrechte bewerkte persoonsgegevens (van welke bevoegdheid nog nooit gebruik was gemaakt).

Individuen kunnen klagen bij de FII (overweging 61) dat hun persoonsgegevens ten onrechte zijn onderschept of onjuist verwerkt. De FRA heeft tegenover eenieder een informatie- en rectificatieplicht met betrekking tot persoonsgegevens die door de dienst zijn verwerkt. Er is mogelijkheid van beroep op de bestuursrechter, van welke mogelijkheid nog geen gebruik was gemaakt. Verder hebben de ombudsman en 'de Kanselier' van het Ministerie van Justitie een taak (overwegingen 67-69).

6. In de EU-zaken ging het om de volgende feitelijke constellaties. In de hier gepubliceerde *Quadrature*-zaak is het uitgangspunt een prejudiciële vraag betreffende de uitleg van artikel 15 lid 1 van de richtlijn voor privacy en elektronische communicatie (2002/58/EG), zoals gewijzigd bij Richtlijn 2009/136/EG en van de artikelen 12 tot en met 15 van de e-commerce richtlijn 2000/31/EG, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 4, 6 tot en met 8 en 11 en artikel 52, lid 1, van het Handvest van de grondrechten van de Europese Unie. Het betreft gevoegde zaken, twee uit Frankrijk, één uit België. De klagers in de Franse zaken waren (organisaties) van internet serviceproviders. In de Belgische zaak ging het om klachten van de Orde van Advocaten, soortgelijk aan die in de *BBW*-zaak.

De Franse wetgeving die ter discussie stond was de *Code de la sécurité intérieure* (wetboek binnenlandse veiligheid (CSI)). Zo stelt artikel L. 811-3 CSI:

> "Uitsluitend met het oog op de uitoefening van hun respectieve taken kunnen de gespecialiseerde inlichtingendiensten gebruikmaken van de in titel V van dit boek genoemde technieken voor het inwinnen van inlichtingen betreffende de verdediging en bevordering van de volgende fundamentele staatsbelangen:
>
> 1° de nationale onafhankelijkheid, de integriteit van het grondgebied en de landsverdediging;
>
> 2° de zwaarwegende belangen van het buitenlands beleid, de nakoming door Frankrijk van zijn Europese en internationale verplichtingen, en de voorkoming van elke vorm van buitenlandse inmenging;"

De inlichtingendiensten kunnen op grond van deze bepalingen de aanbieders van elektronische communicatiediensten verplichten bulkinformatiebestanden af te zonderen.

Zij kunnen verder deze aanbieders tot medewerking verplichten bij de verwerking van die gegevens behulpzaam te zijn en de resultaten van dit alles aan de diensten af te dragen. Zo staat dat in artikel L. 851-3 CSI:

> "Onder de in titel II, hoofdstuk I, van dit boek bepaalde voorwaarden kan, uitsluitend ter voorkoming van terrorisme, aan de in artikel L. 851-1 genoemde exploitanten en personen de verplichting worden opgelegd om op hun netwerken geautomatiseerde verwerkingen uit te voeren die bedoeld zijn om, in overeenstemming met in de machtiging bepaalde parameters, verbindingen op te sporen waaruit een terroristische dreiging zou kunnen blijken. Bij die geautomatiseerde verwerkingen wordt uitsluitend gebruikgemaakt van de in artikel L. 851-1 genoemde informatie of documenten. Er mogen geen andere gegevens worden opgevraagd dan die welke beantwoorden aan de ontwerpparameters, en de personen op wie de informatie of documenten betrekking hebben, mogen niet kunnen worden geïdentificeerd."

Het gaat in deze zaken, naast de hiervoor besproken bulkinterceptie, om de zogenaamde geautomatiseerde data-analyse (afgekort als GDA) van de 'bulk' die in het geciteerde Evaluatierapport WIV 2017 op p. 73-74 wordt gedefinieerd in twee vormen. De 'eenvoudige' vorm: het resultaat van de zoekvraag op bepaalde kenmerken is in essentie een deelverzameling van de verzameling die voldoet aan de kenmerken van de zoekvraag, en de 'complexe' vorm die iets toevoegt aan de oorspronkelijke verzameling met behulp van geautomatiseerde bewerkingen, bijvoorbeeld door waarschijnlijkheidsmarges in te voeren (*waarschijnlijke* doel, persoons- of groepsidentificatie). Om wat voor soort GDA het in de Franse zaak ging is uit het arrest niet duidelijk.

Het Belgische recht (overweging 54 e.v.) bevat soortgelijke bepalingen die de aanbieders van elektronische communicatiediensten tot bewaren en bewerken van gegevens in opdracht van de inlichtingendiensten verplichten.

De prejudiciële vragen werden gesteld door respectievelijk de Franse *Conseil d'Etat* en het Belgische Constitutionele Hof omdat de klagers hun zaken als constitutionele klachten bij de daarvoor in de nationale jurisdicties aangewezen constitutionele rechters aanhangig hadden gemaakt. Het ging dus, evenals in de EHRM-zaken, om algemene klachten: er bestond *een kans* dat de klager (geheimhouder) met zijn persoonsgegevens in de bulk zit en voorwerp van een GDA wordt.

In de (hier niet opgenomen) Britse *Privacy International*-zaak (C-623/17) gaat het om soortge-

lijke onderwerpen. Begin 2015 werd onder meer in een rapport van de Intelligence and Security Committee of Parliament (parlementaire inlichtingen- en veiligheidscommissie, Verenigd Koninkrijk) bekendgemaakt dat door de verschillende veiligheids- en inlichtingendiensten van het Verenigd Koninkrijk, te weten de GCHQ, de MI5 en de MI6, bulkcommunicatiegegevens werden verwerkt en gebruikt. Op 5 juni 2015 heeft Privacy International, een non-gouvernementele organisatie, bij de IPT een zaak aangespannen tegen de Minister van Buitenlandse Zaken en Gemenebestzaken, de Minister van Binnenlandse Zaken en die veiligheids- en inlichtingendiensten, waarbij zij de rechtmatigheid van die praktijken heeft betwist. Het gaat om Section 94 ('Aanwijzingen in het belang van de nationale veiligheid etc.') van de Telecommunications Act 1984 die bepaalt:

> "(1) Na overleg met een persoon op wie deze section van toepassing is, kan de Secretary of State [minister] aan die persoon de algemene aanwijzingen geven die hij noodzakelijk acht in het belang van de nationale veiligheid of de betrekkingen met de regering van een land of gebied buiten het Verenigd Koninkrijk.
>
> (2) Indien de Secretary of State zulks noodzakelijk acht in het belang van de nationale veiligheid of de betrekkingen met de regering van een land of gebied buiten het Verenigd Koninkrijk, kan hij, na overleg met een persoon op wie deze section van toepassing is, die persoon een aanwijzing geven om (naargelang van de omstandigheden van het geval) de in die aanwijzing gespecificeerde handeling te verrichten dan wel daarvan af te zien.
>
> (2A) De Secretary of State kan alleen dan een aanwijzing krachtens lid 1 of lid 2 geven, indien hij van oordeel is dat het door die aanwijzing voorgeschreven gedrag in verhouding staat tot het ermee beoogde doel.
>
> (3) Een persoon op wie deze section van toepassing is, dient alle aanwijzingen op te volgen die hem door de Secretary of State krachtens deze section worden gegeven, niettegenstaande eventuele andere verplichtingen die op hem rusten ingevolge deel 1 of hoofdstuk 1 van deel 2 van de Communications Act 2003 [Communicatiewet 2003], en, in het geval van een aanwijzing gegeven aan een exploitant van een openbaar elektronische communicatienetwerk, ongeacht of deze exploitant die aanwijzing ontvangt in een andere hoedanigheid dan die van exploitant van een dergelijk netwerk."

In zijn vonnis van 17 oktober 2016 stelt de IPT vast dat de geheime diensten hebben erkend dat zij in het kader van hun activiteiten bulkdatasets met persoonsgegevens verzamelen en gebruiken, zoals biografische gegevens of reisgegevens, financiële of zakelijke informatie, communicatiegegevens die gevoelige informatie kunnen bevatten die onder het beroepsgeheim valt, of journalistiek materiaal. Die gegevens, die langs verschillende, mogelijk geheime wegen worden verkregen, worden volgens de verwijzende rechter door middel van kruiscontrole of automatische verwerking geanalyseerd (GDA) en kunnen aan andere personen of autoriteiten worden bekendgemaakt en met buitenlandse partners worden gedeeld. In dit kader maken de veiligheids- en inlichtingendiensten ook gebruik van bulkcommunicatiegegevens die zij hebben verkregen van exploitanten van openbare elektronische communicatienetwerken op grond van de krachtens artikel 94 van de wet van 1984 gegeven ministeriële aanwijzingen. Ook in deze zaak is niet duidelijk of het om 'eenvoudige' of 'complexe' GDA ging.

II. De relatie tussen het EU recht en het recht van het EVRM in zaken van nationale veiligheid

7. Alvorens in te gaan op de merites van de verschillende zaken sta ik eerst stil bij de relatie tussen beide rechtsordes. In het algemeen geldt dat de inhoud van de 'extern' werkende internationale rechtsorde (de internationale/regionale van de Raad van Europa) en die van de Europese 'intern' werkende rechtsorde (de Europese van de Europese Unie) op elkaar worden afgestemd. Deze laatste wordt wel gekarakteriseerd als een gecombineerde unie van staten en burgers, ook wel aangeduid als de 'gedeelde soevereiniteit' van een 'Europese Democratie'.[3] Artikel 52 lid 3 van het EU Handvest bevat een afstemmingsbepaling dat rechten in het Handvest die overeenstemmen met die in het EVRM op dezelfde manier zullen worden uitgelegd en toegepast als in het EVRM. Het EHRM hanteert bij zijn rechtsvinding een comparatieve methode waarbij zowel naar de internationale en de EU-rechtsorde als de nationale rechtsorde van bij het EVRM aangesloten staten wordt gekeken. De laatste jaren zien wij dat, met name bij bescherming van persoonsgegevens (waarvan het Handvest in artikel 8 een uitgewerkte regeling bevat die in het EVRM ontbreekt), het EHRM bij het 'relevante recht' een uitvoerige opsomming geeft van de rechtspraak van het HvJ EU op dit vlak. Zo ook in deze zaken.

8. Een snijpunt vormt het gebied van de openbare veiligheid, defensie en staatsveiligheid dat niet onder de VWEU (artikel 4 lid 2) valt en in de richtlijn over elektronische communicatie en privacy (2002/58/EG) expliciet is uitgezonderd. In de hier besproken beslissingen van het HvJ EU ging het om de uitleg van die richtlijn en in het bijzonder artikel 15 dat bepaalt dat de lidstaten wetgevende maatregelen mogen treffen waarbij de rechten en verplichtingen die bij de richtlijn worden ingesteld kunnen worden beperkt in het belang van openbare veiligheid, defensie en staatsveiligheid. Het artikel bepaalt dat deze maatregelen noodzakelijk moeten zijn en aan proportionaliteitscriteria moeten voldoen. Bij het HvJ EU was daarom in discussie of het Hof bevoegd was om een oordeel over de voorgelegde vragen te geven (die immers door inlichtin-

3 Zie Jaap Hoeksma, *The Theory of democratic Integration*, Oisterwijk: Wolf Legal Publishers 2018.

gendiensten genomen maatregelen betroffen). De grens die het HvJ EU hier trekt is of het betreft *verwerkingen door de elektronische communicatiedienstverleners*, dus degenen tot wie de richtlijn zich richt. In de *Quadrature*-zaak zegt het Hof dat het duidelijkst in overweging 103:

"Wanneer de lidstaten daarentegen rechtstreeks maatregelen toepassen die inbreuk maken op het beginsel van de vertrouwelijkheid van elektronische communicatie, *zonder dat zij verwerkingsverplichtingen opleggen aan aanbieders van elektronische communicatiediensten*, wordt de bescherming van de gegevens van de betrokken personen niet beheerst door richtlijn 2002/58, maar uitsluitend door nationaal recht (…), wat betekent dat de betrokken maatregelen met name in overeenstemming moeten zijn met het nationale constitutionele recht en met de vereisten van het EVRM." De Advocaat-Generaal stelt in zijn conclusie in de *Quadrature*-zaak in punt 77 (noot 41) dat 'activiteiten van persoonlijke of commerciële aard buiten de activiteiten vallen die aan de staat zijn voorbehouden' en hij verwijst naar de conclusie in de *Ministerio Fiscal*-zaak (C-207/16): "Onderscheid moet worden gemaakt tussen enerzijds persoonsgegevens die *rechtstreeks* in het kader van de klassieke activiteiten van de staat op strafrechtelijk gebied worden verwerkt en anderzijds gegevens die in het kader van de — commerciële — activiteiten van een aanbieder van elektronische-communicatiediensten worden verwerkt, en *vervolgens* door de bevoegde overheidsdiensten worden gebruikt."

In deze zaken mondden de door de inlichtingendiensten opgelegde maatregelen wel uit in verwerkingsverplichtingen van de aanbieders van elektronische communicatiediensten en achtte het HvJ EU zich daarom bevoegd om zelf de noodzakelijkheid- en proportionaliteitstoets van artikel 15 van de richtlijn uit te voeren. De arresten komen daarmee in lijn met de dataretentiejurisprudentie van het Hof die, kort gezegd, een algemene retentieverplichting in het belang van de opsporing van strafbare feiten verbiedt: 1. HvJ EU 21 december 2016 (gevoegde zaken *Tele2 Sverige AB/Post-och telestyrelsen* en de Engelse Minister van Binnenlandse Zaken, zaken C-203/15 en C-698/15), *NJ* 2017/186 (met noot E.J. Dommering), 2. HvJ EU 8 april 2014, (*Digital Rights/Ireland*, zaken C-293/12 en C-594/12), en HvJ EU 6 oktober 2015 (de zaak *Schrems I*, C-362/14), beide met noot E.J. Dommering gepubliceerd in *NJ* 2016/446 en 447. Dat is niet onbelangrijk om vast te stellen, omdat over de *Quadrature*-beslissing in Frankrijk nogal wat ophef is ontstaan waarbij door de regering zelfs de *Conseil d'Etat* werd ingeschakeld om een oordeel te vragen of de beslissing van het HvJ EU wel in overeenstemming was met de Franse Grondwet. De *Conseil* antwoordde op 21 april 2021 in een lange beslissing dat dit zo was; daarbij verwees hij nadrukkelijk naar de dataretentie jurisprudentie van het HvJ EU. Maar er zaten zo veel mitsen en maren in die beslissing dat de partij Quadrature daar niet over te spreken is (zie de beslissing van de Raad van State: https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-07-06/453505 en het commentaar van Quadrature: https://www.laquadrature.net/2021/04/21/le-conseil-detat-valide-durablement-la-surveillance-de-masse/, beide geraadpleegd 15 juli 2021).

9. Dezelfde vraag deed zich voor in de *Schrems II*-zaak (HvJ EU 16 juli 2020, zaak C-311/18, *NJ* 2021/24 met noot E.J. Dommering). De Oostenrijkse advocaat Schrems had zich als gebruiker van Facebook bij de Ierse Data Autoriteit beklaagd over het feit dat het kantoor van Facebook in Ierland, dat een dochteronderneming is van Facebook Inc in de VS, de over hem bij zijn communicaties via Facebook vergaarde persoonsgegevens verzamelt en deze deelt met de moedermaatschappij in de VS. Hij stelde dat, gegeven het zwakke beschermingsregime voor privacy aldaar, de Amerikaanse veiligheidsdienst NSA toegang tot zijn persoonsgegevens had kunnen krijgen, omdat de provider daaraan zonder meer (zonder dat daartegen enig rechtsmiddel bestond) moest meewerken. Kon het Hof een oordeel geven over de kwaliteit van de Amerikaanse veiligheidswetgeving wegens de uitzondering van artikel 4 lid 2 VEU? Het Hof behandelt die vraag in de overwegingen 80-89 van dat arrest. Daar stelt het allereerst vast dat deze uitzondering alleen ziet op het verkeer tussen Uniestaten, terwijl de doorgifte niet plaatsvindt tussen inlichtingendiensten (maar tussen een Oostenrijkse particulier en de Ierse Facebookonderneming en tussen onderdelen van het Facebook-concern in Ierland en de VS). Bovendien moet deze uitzondering strikt worden geïnterpreteerd.

10. We zien dus dat er een scheidslijn loopt bij de handelingen van de inlichtingendiensten en de wet- en regelgeving die op hen van toepassing is wanneer de verwerking van persoonsgegevens bij de diensten plaats vindt. De veiligheids*exceptie* in het EU recht dat dit buiten de sfeer van de EU-rechtsorde valt, is dan van toepassing. Dit gehele complex van feiten en regels moet in dat geval worden getoetst aan het nationale recht, de nationale grondwet en/of het EVRM. Zodra voor de uitvoering van die veiligheidstaken door deze autoriteiten handelingen van private (rechts)personen worden verlangd of op eigen initiatief (zoals Facebook in *Schrems II*) worden teweeggebracht, zijn de voor deze EU-rechtssubjecten geldende EU-regels van toepassing en voert het HvJ EU de toetsing aan proportionaliteitsbeginselen die in het EU-recht zijn neergelegd en/of toetsing aan het EU Handvest uit.

11. Maar daarmee blijven er toch fundamentele vragen over. De principiële kwestie blijft immers *wanneer* die nationale veiligheidsexceptie van artikel 4 lid 2 VWEU van toepassing is en, als zij onder de EU valt, *wat* deze precies inhoudt? *Wanneer:* is een medewerkingshandeling of verstrekkingshandeling van een commerciële partij waarbij bewaarde (en ontsloten) persoonsgegevens worden overgedragen aan een inlichtingendienst al een activiteit die buiten de

staatsactiviteiten valt, zodat het EU-recht van toepassing is? En als dat zo is, moet dan de inhoud daarvan niet, overeenkomstig de afstemmingsbepaling 52 lid 3 van het Handvest, in beide rechtsordes (ook qua proportionaliteit van de daaruit voortvloeiende beperkingen) overeenkomstig worden uitgelegd (wat in de *Quadrature*-zaak duidelijk niet het geval is)? Ook is het een vraag of de uitwisselingsregimes en de daarvoor geldende waarborgen tussen landen voor de EU en het EVRM hetzelfde moeten zijn. Het EHRM oordeelt in de Zweedse zaak (zie hierna onder punt 16) dat uitwisseling is toegestaan bij 'een acceptabel minimumniveau aan waarborgen'. Is dat ook de norm van het HvJ EU?[4]

III. De criteria van het EHRM voor de bescherming van de privacy in het kader van het handelen van de inlichtingendiensten (de materiële normen)

12. Het EHRM heeft voor de verwerving van persoonsgegevens door strafrechtelijke en/of veiligheidsautoriteiten zes criteria ontwikkeld die het (naar de eerste zaak *Weber* waarin dat gebeurde) de zes 'Webercriteria' noemt (EHRM 29 juni 2006, appl. 54934/00; de meest recente over inlichtingendiensten is *Zakharov/Rusland*, EHRM 4 december 2015, appl. 47143/06, *NJ* 2017/185, m.nt. E.J. Dommering; voor een overzicht zie Egbert Dommering, *De Europese Informatierechtsorde,* Amsterdam: DeLex 2019, VII.4). Het strafrecht was daarbij het uitgangspunt. De criteria zijn: 1. De aard van de verdenkingen, 2. Categorieën van personen die mogen worden 'gevolgd', 3. De tijdsduur dat ze mogen worden gevolgd, 4. Regels voor opslag, toegang, en onderzoek van verzamelde gegevens, 5. De transparantie van de regels en 6. Regels omtrent de duur van de opslag. Het Hof constateert in zijn preliminaire beschouwingen in de *BBW*-zaak (overwegingen 322- 323) dat deze criteria niet onverkort toegepast kunnen worden op bulkinterceptie. Het geeft daarin een korte schets van de veranderde technische, maatschappelijke en politieke situatie in de internet wereld en trekt daaruit de conclusie:

> "Consequently, the Court is required to carry out its assessment of Contracting States' bulk interception regimes, a valuable technological capacity to identify new threats in the digital domain, for Convention compliance by reference to the existence of safeguards against arbitrariness and abuse, on the basis of limited information about the manner in which those regimes operate."

Het accent van de toetsing verschuift daarmee van de eerste drie van de 'Webercriteria' naar de laatste drie, terwijl het EHRM die verder preciseert en uitbreidt. Ze vormen met de laatste twee (die over toezicht gaan) een geheel dat het aanduidt als 'end-to-end safeguards'. Het EHRM preciseert dit in overweging 361 (onder verwijzing naar onder meer het *Zakharov*-arrest):

> "1. the grounds on which bulk interception may be authorised;
> 2. the circumstances in which an individual's communications may be intercepted;
> 3. the procedure to be followed for granting authorisation;
> 4. the procedures to be followed for selecting, examining and using intercept material;
> 5. the precautions to be taken when communicating the material to other parties;
> 6. the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
> 7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
> 8. the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance."

Over het loslaten van de concrete strafrechtelijke toets bij de eerste drie punten is het EHRM niet unaniem, zoals blijkt uit de dissenting opinions bij *BBW*. Ook het HvJ EU is daarin strikter.

13. Van de acht criteria zien de eerste drie op aangepaste ex ante criteria, de tweede drie op de procedures voor bewerking en opslag, de laatste twee op het toezicht. Het is een verschuivend proces waarin de kans op inmenging in de privacy toeneemt, zoals het EHRM in de overwegingen 325 en 330 preciseert:

> "The Court views bulk interception as a gradual process in which the degree of interference with individuals' Article 8 rights increases as the process progresses. Bulk interception regimes may not all follow exactly the same model, and the different stages of the process will not necessarily be discrete or followed in strict chronological order." (…) "Finally, at the end of the process, where information about a particular person will be analysed or the content of the communi-

4 Mogelijk dat deze vragen (deels) in de in de onder 1 genoemde zaken C-215/20 en C-222/20, beantwoord worden. Deze zaken betreffen prejudiciële vragen die het Verwaltungsgericht in Wiesbaden heeft gesteld over de verenigbaarheid van de richtlijn betreffende de uitwisseling van passagiersgegevens (2016/681, de zogenaamde PNR-richtlijn) met de artikelen 7 en 8 van het Handvest. Het gaat dan om algemene opslag van deze gegevens en de verstrekking daarvan in verband met de opsporing van 'zware criminaliteit'. Behalve deze zaak liggen er soortgelijke prejudiciële vragen over deze richtlijn van het Constitutionele Hof in België (C-817/19) en de districtsrechtbank in Keulen (zaak C-148/20). Ik verwijs ook naar het WODC-rapport dat de Nederlandse PNR wet evalueert (november 2021, https://repository.wodc.nl/bitstream/handle/20.500.12832/3118/3181-evaluatie-pnr-wet-volledige%20tekst.pdf?sequence=7&isAllowed=y). De tweede groep zaken (resp. C-793/19 en C-140/20) betreft vragen van het Bundesverwaltungsgericht en de Ierse Supreme Court over de verenigbaarheid van de dataretentierichtlijn (2006/24/EG) met de artikelen 7 en 8 van het Handvest. Zij passen dus in de in 8 en 9 besproken dataretentierichtlijn-beslissingen, maar nu wordt specifiek gevraagd naar de betekenis van de 'nationale veiligheid' en de speelruimte die artikel 4 lid 2 VWEU aan de lidstaten laat.

cations is being examined by an analyst, the need for safeguards will be at its highest. This approach of the Court is in line with the finding of the Venice Commission, which in its report on the Democratic Oversight of Signals Intelligence Agencies considered that in bulk interception the main interference with privacy occurred when stored personal data were processed and/or accessed by the agencies."

14. Er is discussie bij het EHRM geweest hoeveel selectiecriteria reeds in de fase van het ex ante toezicht bekend moeten zijn. Omdat de overwegingen 353 en 354 van het Hof in de *BBW*-zaak mede zijn ingegeven door de Nederlandse interventie, geef ik die overwegingen hier integraal in vertaling (evenals andere wat langere citaten, hierna) weer:

"Het gebruik van selectors — en met name sterke selectors — is een van de belangrijkste stappen in het bulkinterceptieproces, aangezien dit het punt is waarop de communicatie van een bepaald individu het doelwit kan zijn van de inlichtingendiensten. Hoewel sommige systemen de voorafgaande toestemming van categorieën selectors mogelijk maken (zie bijvoorbeeld het Zweedse systeem dat in detail is beschreven in het arrest Centrum för rättvisa v. Zweden), merkt het Hof op dat de regeringen van zowel het Verenigd Koninkrijk als Nederland hebben aangevoerd dat elke verplichting om selectors of zoekcriteria in de aanvraag voor de vergunning toe te lichten of te onderbouwen, de doeltreffendheid van bulkonderschepping ernstig zou beperken. Dit werd aanvaard door de IPT, die vond dat de opname van de selectors in de autorisatie onrealistisch is. Rekening houdend met de kenmerken van bulkonderschepping (zie de punten 344-345 hierboven), het grote aantal gebruikte selectors en de inherente behoefte aan flexibiliteit bij de keuze van selectors, die in de praktijk kan worden uitgedrukt als technische combinaties van cijfers of letters, *aanvaardt het Hof dat het opnemen van alle selectors in de autorisatie in de praktijk wellicht niet haalbaar is. Aangezien echter de keuze van selectors en zoektermen bepaalt welke communicatie in aanmerking komt voor onderzoek door een analist, moet de autorisatie op zijn minst aangeven welke typen of categorieën selectors moeten worden gebruikt."*

15. Alle fasen zien op de kwaliteit van de wet waarin de (noodzaak van de) beperkingen is geregeld. Zoals het EHRM in overweging 348 aangeeft kunnen strafrechtelijke criteria niet in de eerste fase worden toegepast. Er moeten echter *gedetailleerde* regels in de nationale wetgeving bestaan wanneer en hoe de verwerkingsbevoegdheden mogen worden ingezet en hoe daarop toezicht wordt uitgeoefend. Het EHRM onderneemt dan (overweging 365 e.v.) een uitgebreide toetsing van de kwaliteit van de Britse regeling. Deze voldoet op veel punten aan de waarborgcriteria in het rijtje van acht criteria, maar bevat ook zodanige gebreken dat het EHRM concludeert tot schending van artikel 8 EVRM. Het EHRM somt dat in zijn conclusie in overweging 425 op. Het is een optelsom: het ene gebrek kan een ander misschien nog aanvaardbaar zwak punt ook tot een gebrek maken:

"Het Hof herinnert eraan dat er een aanzienlijk potentieel is voor misbruik van massa-interceptie op een wijze die afbreuk doet aan de rechten van individuen op eerbiediging van het privéleven (zie punt 347 hierboven). In een rechtsstaat (die als instituut uitdrukkelijk wordt genoemd in de preambule van het verdrag en inherent is aan het voorwerp en doel van artikel 8 (zie Roman Zakharov, reeds aangehaald, § 228), is het Hof van oordeel dat, als geheel beschouwd, de regeling van sectie 8, lid 4, ondanks de waarborgen, waaronder enkele robuuste zoals hierboven aangegeven (zie bijvoorbeeld de overwegingen 412 en 415), niet voldoende 'end-to-end' adequate en effectieve waarborgen biedt tegen willekeur en het risico van misbruik. Het Hof heeft met name de volgende fundamentele tekortkomingen in de regeling vastgesteld: het ontbreken van een onafhankelijke machtiging, het niet opnemen van de categorieën selectors in de aanvraag van een bevelschrift en het ontbreken van een systeem van voorafgaande interne machtiging (zie overwegingen 377-382). Deze tekortkomingen hadden niet alleen betrekking op het onderscheppen van de inhoud van communicatie, maar ook op het onderscheppen van gerelateerde communicatiegegevens (zie punt 416 hierboven). Hoewel de IC-commissaris onafhankelijk en effectief toezicht hield op het regime en de IPT een krachtig rechtsmiddel bood aan iedereen die vermoedde dat zijn of haar communicatie was onderschept door de inlichtingendiensten, volstonden deze belangrijke waarborgen niet om de tekortkomingen op te heffen die in de punten 377-382 zijn belicht."

16. In de (hier niet opgenomen) Zweedse zaak valt de integrale toetsing ook negatief uit. In de overwegingen 369-373 constateert het EHRM drie gebreken in de regulering, waarvan er twee fataal zijn:

"Het Hof constateerde drie tekortkomingen in de Zweedse regeling voor het onderscheppen van bulk: het ontbreken van een duidelijke regel voor het vernietigen van onderschept materiaal dat geen persoonsgegevens bevat (zie punt 342 hierboven); het ontbreken van een vereiste in de *Signals Intelligence Act* of andere relevante wetgeving dat bij het nemen van een besluit om inlichtingenmateriaal aan buitenlandse partners door te geven, rekening wordt gehouden met de privacybelangen van individuen (zie paragrafen 326-330 hierboven); en het ontbreken van een effectieve controle achteraf (zie de punten 359-364 hierboven).

Wat de eerste van deze tekortkomingen betreft, wordt de mogelijkheid om nadelige gevolgen te hebben voor de rechten van artikel 8 beperkt door het feit dat de Zweedse wet voorziet in dui-

delijke regels voor de vernietiging van onderschept materiaal in een aantal omstandigheden en ook vooral wanneer het persoonsgegevens bevat.[5]

Het Hof is echter van oordeel dat de tweede tekortkoming potentieel kan leiden tot zeer aanzienlijke nadelige gevolgen voor getroffen personen of organisaties. Zoals opgemerkt, kan de bovengenoemde tekortkoming het mogelijk maken dat informatie die de privacyrechten of het recht op respect voor correspondentie ernstig in gevaar brengt, naar het buitenland wordt verzonden, zelfs als de intelligencewaarde ervan zeer laag is. Een dergelijke doorgifte kan derhalve duidelijk onevenredige risico's opleveren voor de rechten van artikel 8 van het Verdrag. Verder wordt het FRA geen juridisch bindende verplichting opgelegd om te analyseren en vast te stellen of de buitenlandse ontvanger van inlichtingen een acceptabel minimumniveau aan waarborgen biedt.

Ten slotte verzwakt de dubbele rol van de inspectie en het ontbreken van de mogelijkheid voor het publiek om in een of andere vorm gemotiveerde besluiten te verkrijgen naar aanleiding van vragen of klachten over het massaal aftappen van communicatie, het controlemechanisme achteraf zodanig dat er risico's ontstaan voor de naleving van de grondrechten van de getroffen personen. Bovendien kan het ontbreken van een effectieve toetsing in de laatste fase van de onderschepping niet worden verzoend met de opvatting van het Hof dat de mate van inmenging in de rechten van individuen op grond van artikel 8 toeneemt naarmate het proces vordert (zie de punten 239 en 245 hierboven) en niet voldoet aan het vereiste van 'end-to-end'-waarborgen (zie punt 264 hierboven).

Het Hof is van oordeel dat de belangrijkste kenmerken van het Zweedse regime voor het onderscheppen van bulk voldoen aan de vereisten van het Verdrag inzake de kwaliteit van de wet en is van oordeel dat de werking van dit regime ten tijde van het onderzoek van het Hof daarom in de meeste opzichten valt binnen de grenzen van wat 'noodzakelijk is in een democratische samenleving'. Het is echter van oordeel dat de in de voorgaande paragrafen genoemde tekortkomingen niet voldoende worden gecompenseerd door de bestaande waarborgen en dat de Zweedse regeling voor het onderscheppen van bulk derhalve de beoordelingsmarge overschrijdt die in dat opzicht aan de autoriteiten van de verwerende staat is gelaten. Het Hof herhaalt dat er een aanzienlijk potentieel is voor misbruik van massale interceptie op een manier die afbreuk doet aan de rechten van individuen op eerbiediging van het privéleven (zie punt 261 hierboven). Gelet op het beginsel van de rechtsstaat, (…) is het EHRM van oordeel dat de Zweedse bulk interceptieregime, als geheel beschouwd, onvoldoende 'end-to-end'-waarborgen bevatte om adequate en effectieve garanties te bieden tegen willekeur en het risico van misbruik."

17. De toetsing ziet dus vooral op de kwaliteit en toegankelijkheid van de wettelijke regels, de organisatie van de inlichtingendienst zelf en de daarbij 'ingebouwde' waarborgen die bij de verwerking in acht worden genomen, de mogelijkheden van rechtsbescherming voor de burgers en de *effectiviteit* van het externe toezicht op alle fasen van het verwerkingsproces. Op de notie van 'effectiviteit' kom ik in VI terug.

IV. Uitwisseling van bulkdata tussen inlichtingendiensten van verschillende landen

18. De vijfde factor in het rijtje betreft de uitwisseling van bulkgegevens. Van belang is stil te staan bij het internationale karakter daarvan. Daarbij gaat om de uitwisseling van gegevens tussen inlichtingendiensten uit verschillende landen. Een belangrijke factor bij bulkinterceptie is dat het doorgaans gaat om interceptie van gegevens uit het buitenland (overwegingen 344-347 in de *BBW*-zaak): 'the early detection and investigation of cyberattacks, counter-espionage and counter-terrorism'. Hoewel dit ook op individuen kan zijn gericht heeft dit een ander karakter zoals het EHRM in overweging 346 preciseert:

"Hoewel het onderscheppen van bulk niet noodzakelijkerwijs wordt gebruikt om bepaalde individuen te 'targeten', kan en wordt het kennelijk wel voor dit doel gebruikt. Wanneer dit echter het geval is, worden de apparaten van de beoogde personen niet gecontroleerd. Integendeel, individuen worden 'getarget' door de toepassing van sterke selectors (zoals hun e-mailadressen) op de communicatie die massaal wordt onderschept door de inlichtingendiensten. Alleen die 'pakketten' van de communicatie van de beoogde personen die via de door de inlichtingendiensten geselecteerde dragers binnenkwamen, zullen op deze manier zijn onderschept, en alleen die onderschepte communicatie die overeenkwam met een sterke selector of een complexe zoekopdracht, kon door een analist worden onderzocht."

19. In deze zaken speelt het allemaal een rol. Het EHRM vermeldt daarom in de overwegingen 247 e.v. (het relevante recht) van de *BBW*-zaak de uitspraak van het Bundesverfassungsgericht van 19 mei 2020 (1 BvR 2835/17). Het zegt over deze, voor de rechtsvergelijking in Europa, belangrijke uitspraak (in overweging 251):

"Wat betreft het delen van intelligence die is verkregen via buitenlands toezicht, constateert het BVerfG opnieuw dat de waarborgen ontbreken. Met name werd niet voldoende duidelijk gespecificeerd wanneer zwaarwegende belangen ge-

5 Kennelijk vindt het Hof de beperking tot persoonsgegevens een te smalle bescherming.

gevensoverdrachten zouden kunnen rechtvaardigen. Het BVerfG was weliswaar van oordeel dat het niet nodig is dat een ontvangende staat vergelijkbare regels voor de verwerking van persoonsgegevens heeft, maar was niettemin van oordeel dat gegevens alleen naar het buitenland konden worden doorgegeven als er een passend niveau van gegevensbescherming bestond en er geen reden was te vrezen dat de informatie zou worden gebruikt om fundamentele beginselen van de rechtsstaat te schenden. Meer in het algemeen oordeelde het BVerfG in het kader van het delen van inlichtingen dat samenwerking met buitenlandse staten niet mag worden gebruikt om binnenlandse waarborgen te ondermijnen (…)."

Bij bulkdata speelt bij factor 5 dus in het bijzonder welke waarborgen en procedures er bestaan voor de uitwisseling van welke persoonsgegevens met andere buitenlandse inlichtingendiensten (Evaluatierapport Wiv 2017, p. 63). Hier schiet het Zweedse systeem te kort omdat het ongefilterd gegevens doorgeeft (overwegingen 318-330). Met name in overweging 326 contrasteert het Hof de Zweedse regeling met de Britse. Ik citeer:

"Het hof constateert dat bijvoorbeeld het relevante regime in het VK in tegenstelling tot de Zweedse regeling een verplichting bevat om redelijke stappen te nemen om vast te stellen dat het buitenlandse regime voorziet in de noodzakelijke waarborgen dusdanig dat er procedures zijn dat de ontsluiting, bewerking, uitwisseling en opslag van het onderschepte materiaal tot het minimum dat noodzakelijk is wordt beperkt (zie paragraaf 7.5 van de United Kingdom Interception of Communications Code of Practice, geciteerd in overweging 96 van de BBW zaak.)."

V. 'Inhoud van communicatie' en 'verkeersgegevens', 'registratie' en 'gedrag'

20. Het EHRM heeft lang vastgehouden aan het onderscheid tussen de inhoud van de communicatie en registratie van tijd, plaats en communicanten (tussen 'wat' iemand communiceert en '(tussen) wie, waar en wanneer' iemand communiceert). De inhoud zou meer bescherming verdienen. In de wereld van de bulktechnologie waarin alles draait om het opsporen van waarschijnlijkheidspatronen is dat onderscheid nauwelijks nog relevant. Het EHRM lijkt dit te aanvaarden, in die zin dat de 'wie, waar, wanneer' gegevens evenveel over iemand kunnen zeggen als de inhoud van de communicatie en daarom een gelijkwaardige bescherming op zijn plaats is. Ook de Evaluatiecommissie Wiv 2017 acht het onderscheid niet langer relevant (p. 60, par. 4.4.5.1). In de uitspraken speelt, voor zover ik kan zien, (nog) geen rol dat gegevens die iemand registreren of identificeren minder gevoelig zijn dan gegevens die iets over iemands gedrag zeggen. Dat is het onderscheid tussen de verbinding van een persoon met een emailadres of een nummerplaat (identificatie) en de verbinding van iemand op een passagierslijst (reisgedrag naar tijd en plaats te traceren).[6] Bij het vorderen van communicatiegegevens van iPhones hebben zowel het EHRM als het HvJ EU dat onderscheid aanvaard: EHRM 30 januari 2020, (zaak *Breyer*, appl. 50001/12), *NJ* 2020/431 en HvJ EU 2 oktober 2018 (zaak *Ministerio Fiscal/Spanje*), *NJ* 2020/232, beide m.nt. E.J. Dommering). Je zou dus bij de bulkbehandeling onderscheid kunnen maken in de waarborgen die in acht moeten worden genomen voor identificatie en voor gedrag (zoals de Evaluatiecommissie Wiv 2017 ook doet, rapport, p. 43 par. 4.2.4), maar het EHRM komt aan dat onderscheid in deze zaken niet toe. Het is ook de vraag of het onderscheid wel zo scherp is te maken als het Evaluatierapport doet.[7]

VI. Het ex ante en ex post toezicht

21. De factoren 7 en 8 zien hierop en zij moeten in onderling verband worden gezien. In het Britse systeem is er geen rechterlijk, maar wel bestuurlijk ex ante toezicht, er is ex post zowel rechterlijk (de IPT) als bestuurlijk toezicht. Het Zweedse ex ante toezicht is sterk, immers volgens het ideaalbeeld van het EHRM door een semi-rechterlijk college, dat ook als een rechterlijk college functioneert in een niet-openbare zitting waar een 'algemeen belang advocaat' aanwezig is die in abstracto het belang van de 'slachtoffers' behartigt. Toch vindt het EHRM dat niet voldoende omdat het ex post toezicht te zwak is (overweging 302 in de Zweedse zaak):

"Voor de doeleinden van de analyse van het Hof is het relevante punt in dit stadium echter dat het Zweedse machtigingssysteem een gerechtelijke ex ante beoordeling van vergunningsaanvragen biedt die alomvattend is, in die zin dat het doel van de missie en de dragers en categorieën van de te gebruiken selectors zijn onderworpen aan controle, en het voldoende gedetailleerd is met betrekking tot geheime bulksignaalinlichtingen als onderdeel van buitenlandse inlichtingen. Een dergelijke controle biedt een belangrijke bescherming tegen, met name, het starten van onrechtmatige of duidelijk onevenredige onderscheppingsoperaties in bulk. Belangrijk is dat het ook het kader schept waarbinnen een concrete operatie zich moet ontvouwen en de grenzen waarvan de naleving dan het voorwerp wordt van het geldende toezicht en de controle achteraf."

Maar (overweging 372 in de Zweedse zaak):

"Tot slot verzwakt als gevolg van de dubbele rol van de Inspectie en het ontbreken van een mogelijkheid voor leden van het publiek om in een of andere vorm gemotiveerde besluiten te verkrijgen naar aanleiding van vragen of klachten over het massaal aftappen van communicatie,

6 Zie daarover uitvoerig het in noot 2 geciteerde WODC rapport.

7 Deze kwestie zal waarschijnlijk wel aan de orde komen in de in noot 2 genoemde bij het HvJ EU aanhangige zaken.

het controlemechanisme achteraf in een mate die risico's met zich meebrengt voor de naleving van de grondrechten van de betrokken personen. Bovendien kan het ontbreken van een effectieve toetsing in de laatste fase van de onderschepping niet worden verzoend met de opvatting van het EHRM dat de mate van inmenging in de rechten van individuen op grond van artikel 8 toeneemt naarmate het proces vordert (zie de punten 239 en 245 hierboven) en niet voldoet aan de vereiste van 'end-to-end'-waarborgen (zie punt 264 hierboven)."

Al met al vindt het EHRM in de 'ketenbeoordeling' het Britse toezichtsysteem wel voldoende, maar het Zweedse niet. Daarbij tilt het kennelijk zwaar aan de dubbelrol van de inspectie die onvoldoende onafhankelijk over klachten kon oordelen.

22. We moeten in aanmerking nemen dat het gaat om een mengvorm van bestuurlijk/rechterlijk toezicht, waarvan de bijzonderheid is dat er maar één subject van toezicht is (namelijk de inlichtingendienst) hetgeen betekent dat de toezichthouder en het subject van toezicht dicht op elkaar opereren (in Nederland zelfs in real time, zodat de toezichthouder kan 'meekijken' met wat de diensten doen).

Het EHRM spreekt in beide zaken over 'effectief' toezicht. In Nederland wordt door sommigen[8] wel het standpunt vertolkt dat 'effectief' toezicht 'bindend' moet zijn, maar dat is mijns inziens een misverstand. Maakt men het toezicht over de hele linie bindend, zoals een rechterlijke beslissing, dan worden de verrichtingen van de diensten en de toezichthouder aan bestuurlijke en politieke controle onttrokken, omdat alleen nog een rechter over het bindende oordeel kan oordelen. Dan wordt het een strafrechtelijk of bestuursrechtelijk model, maar daarvan mist het dan weer de waarborgen. De toezichthouder geeft dan immers bindende oordelen over de 'rechtmatigheid' van het handelen van de diensten zonder dat voor de besluitvorming rechterlijke (de regels van strafvordering) of bestuurlijke (de regels van de Awb) kwaliteitseisen gelden. Dat kan ook moeilijk, omdat dat praktisch veelal ondoenlijk is. Zou men dit willen ondervangen met een volle beroepsgang bij de bestuursrechter dan dreigt het gevaar dat het toezicht een geformaliseerd conflictmodel wordt, hetgeen evenmin wenselijk is.

Een ander bezwaar (zeker in een system van end-to-end control) is dat de verantwoordelijkheid van de inlichtingendienst en die van de toezichthouder verstrengeld raken, en eigenlijk iedere handeling binnen de dienst aan toestemming van de toezichthouder wordt onderworpen, hetgeen onwerkbaar is.

Bindend toezicht zal dus dikwijls niet effectief zijn. De effectiviteit van het toezicht kan ook worden bereikt door intern overleg, publiciteit van toezichtrapporten, bestuurlijke en politieke verantwoording. De bindendheid van het toezicht is wel nodig bij het (bestuurlijke) toezicht vooraf bij de inzet van bevoegdheden en bij de klachtbehandeling van mogelijk door het handelen van de diensten getroffen burgers, omdat daarin nu eenmaal 'een knoop moet worden doorgehakt'.

Ik lees de beslissingen van het EHRM zo dat dit met 'effectiviteit' wordt bedoeld (dat is ook de opvatting van de al geciteerde Evaluatiecommissie, zie hoofdstuk 9 van het Evaluatierapport).

VII. De beslissingen van het HvJ EU in de Quadrature en Privacy International zaken

23. Het HvJ EU formuleert de materiële vraag waar het om draait in deze arresten als volgt: of artikel 15, lid 1, van Richtlijn 2002/58, gelezen in het licht van artikel 4, lid 2, VEU en de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, aldus moet worden uitgelegd dat het zich verzet tegen een nationale regeling op grond waarvan een overheidsorgaan ten behoeve van de bescherming van de nationale veiligheid aan aanbieders van elektronische communicatiediensten een verplichting tot algemene en ongedifferentieerde doorzending van verkeers- en locatiegegevens aan de veiligheids- en inlichtingendiensten kan opleggen. Het Hof is daar zeer duidelijk over: het in artikel 5, lid 1, van Richtlijn 2002/58 neergelegde verbod op het onderscheppen van de communicatie en de daarmee verband houdende verkeersgegevens omvat dus elke vorm van beschikbaarstelling door aanbieders van verkeers- en locatiegegevens aan overheidsinstanties, zoals veiligheids- en inlichtingendiensten, alsmede de bewaring van de beschikbaar gestelde gegevens door die instanties, ongeacht het latere gebruik van die gegevens. De *Privacy International*-zaak kon daarmee worden afgedaan omdat de Engelse rechter niet meer had gevraagd. In de *Quadrature*-zaak gaat het HvJ EU echter in op wat de proportionaliteitstoetsing in dit verband inhoudt.

24. In punt 137 van het *Quadrature*-arrest formuleert het HvJ EU het criterium in welke gevallen de nationale veiligheid een rechtvaardiging kan zijn voor het opleggen van vergaande retentieverplichtingen aan aanbieders van elektronische communicatiediensten:

"In situaties als die welke in de punten 135 en 136 van het onderhavige arrest zijn beschreven, verzet artikel 15, lid 1, van richtlijn 2002/58, gelezen in het licht van de artikelen 7, 8 en 11 en artikel 52, lid 1, van het Handvest, zich derhalve in beginsel niet tegen een wettelijke maatregel op grond waarvan de bevoegde autoriteiten aan aanbieders van elektronische communicatiediensten een bevel kunnen opleggen om de verkeers- en locatiegegevens van alle gebruikers van elektronische communicatiemiddelen ge-

8 Met name door de CTIVD. Zij beroept zich daarvoor op het zogenaamde 108 + verdrag (de aanpassing van het Dataprotectieverdrag 1981 van de Raad van Europa). Daar is echter geen steun voor dat standpunt te vinden. Zie daarvoor uitvoerig R.H.T. Janssen en M.D. Reijneveld, 'Conventie 108+ en (toezicht op) de gegevensverwerking in het nationale veiligheidsdomein', in: *Computerrecht* 2021, afl. 5, 411-421 (208).

durende een beperkte periode te bewaren, wanneer er voldoende concrete aanwijzingen zijn dat de betrokken lidstaat wordt geconfronteerd met een ernstige bedreiging van de nationale veiligheid als bedoeld in de punten 135 en 136 van het onderhavige arrest, en die bedreiging werkelijk en actueel of voorzienbaar is. Ook al heeft een dergelijke maatregel zonder onderscheid betrekking op alle gebruikers van elektronische communicatiemiddelen, zonder dat er op het eerste gezicht enig verband in de zin van de in punt 133 van het onderhavige arrest bedoelde rechtspraak tussen die gebruikers en een bedreiging voor de nationale veiligheid van de betrokken lidstaat lijkt te bestaan, geoordeeld moet worden dat het bestaan van een dergelijke bedreiging op zichzelf dat verband aantoont."

25. In overweging 139 vervolgt het HvJ EU: "Daartoe is het van wezenlijk belang dat een beslissing waarbij aan aanbieders van elektronische communicatiediensten een bevel tot een dergelijke gegevensbewaring wordt opgelegd, effectief kan worden getoetst door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit waarvan de beslissing bindend is, waarbij het doel van die toetsing is om na te gaan of een van die situaties zich voordoet en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien." Wat hiermee wordt bedoeld is niet zonder meer duidelijk. De doelomschrijving 'om na te gaan of een van de situaties zich voordoet' lijkt op een ex ante toetsing maar het vervolg van de zin kun je anders lezen. In ieder geval gaat het om een maatregel waarin door de overheidsdienst een 'gegevensbewaring is opgelegd' aan de particuliere serviceprovider.

26. Zoals ik in II aangaf, blijven er vragen. Het HvJ EU maakt geen duidelijk onderscheid tussen wat de inlichtingendienst doet (interceptie) en wat de elektronische communicatiedienst doet (retentie). Daarnaast hanteert het een ander materieel criterium dan het EHRM. Er moet immers een concrete bedreiging van de nationale veiligheid zijn. Bovendien formuleert het zelf enige proportionaliteitseisen waaraan het verzamelen en opslaan van gegevens moet voldoen (tijdsduur, categorie, geografische beperking etc.). Zoals hiervoor uiteen is gezet is bulkinterceptie nu juist bedoeld om bedreigingen van die veiligheid op het spoor te komen die nog niet bekend zijn. Heeft het HvJ EU de ratio van bulkinterceptie niet begrepen of moeten we de beslissing zo lezen dat lidstaten die bulkinterceptie willen toepassen dit geheel binnen de operationele sfeer van de inlichtingendiensten en de daarvoor geldende constitutionele en EVRM waarborgen moeten brengen? Mij lijkt deze laatste conclusie de meest zinvolle, maar we raken hier aan het probleem van de afbakening en de uniforme uitleg van de inhoud van fundamentele rechten, zoals artikel 52 lid 3 van het Handvest voorschrijft (zie hiervoor onder II).

27. Het HvJ EU laat zich ook uit over geautomatiseerde data-analyse (GDA) op bulkbestanden. Allereerst is van belang dat het Hof de onbekende persoonsgegevens die zich in bulkbestanden bevinden aanmerkt als persoonsgegeven, omdat ze 'identificeerbaar' zijn en daarmee dus voldoen aan de definitie van (thans) artikel 4 aanhef en onder 1 van de AVG. Aangezien GDA daarvoor het geëigende hulpmiddel is, moet de medewerking door de telecomoperators aan de uitoefening van de GDA-bevoegdheid aan waarborgen voldoen. Dat betekent dat (overweging 177):

> 'de bijzonder ernstige inmenging die de geautomatiseerde analyse van die gegevens met zich brengt, slechts aan het evenredigheidsvereiste kunnen voldoen in situaties waarin een lidstaat wordt geconfronteerd met een werkelijke en actuele of voorzienbare bedreiging van de nationale veiligheid, en op voorwaarde dat de duur van die bewaring tot het strikt noodzakelijke wordt beperkt.'

Ook hiervoor verlangt het HvJ EU een rechterlijke/bestuurlijke toetsing (overweging 179): 'om na te gaan of zich een situatie voordoet die die maatregel rechtvaardigt, en of is voldaan aan de voorwaarden en waarborgen waarin moet worden voorzien.' Dat is dus iets anders dan de end-to-end control van het EHRM, een complexe analyse waarvan pas in de eindfase de mogelijkheid van inmenging in privéleven kan worden vastgesteld.

28. Het voegt nog enige algemene criteria toe waaraan GDA moet voldoen, die wel de aandacht verdienen, omdat ze ook van belang zijn voor de comparatieve interpretatie van het EVRM (zie II), en die ik daarom volledig citeer:

> "180 In dit verband dient te worden gepreciseerd dat de vooraf vastgestelde modellen en criteria waarop dit type gegevensverwerking is gebaseerd, ten eerste specifiek en betrouwbaar moeten zijn, zodat zij tot resultaten leiden waarmee die personen worden geïdentificeerd op wie een redelijk vermoeden van deelneming aan terrorisme kan rusten, en ten tweede niet mogen discrimineren [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 172].
>
> 181 Voorts zij eraan herinnerd dat elke geautomatiseerde analyse aan de hand van modellen en criteria die ervan uitgaan dat de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, het lidmaatschap van een vakvereniging, de gezondheid of het seksueel gedrag van een persoon op zichzelf en los van het individuele gedrag van die persoon relevant zouden kunnen zijn in het licht van het voorkomen van terrorisme, in strijd zou zijn met de door de artikelen 7 en 8 juncto artikel 21 van het Handvest gewaarborgde rechten. De modellen en criteria die vooraf worden vastgesteld ten behoeve van een geautomatiseerde analyse die tot doel heeft terroristische activiteiten die een ernstige bedreiging vormen voor de nationale veiligheid, te voorkomen, kunnen dus niet alleen op die ge-

voelige gegevens zijn gebaseerd [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punt 165].

182 Aangezien geautomatiseerde analyses van verkeers- en locatiegegevens noodzakelijkerwijs een zekere foutenmarge bevatten, moet bovendien elk positief resultaat van een geautomatiseerde verwerking nog eens individueel — met niet-geautomatiseerde middelen — worden onderzocht alvorens een individuele maatregel wordt genomen die nadelige gevolgen heeft voor de betrokken personen, zoals de latere opvraging in real time van de betrokken gegevens. Een dergelijke maatregel mag namelijk niet uitsluitend op het resultaat van een geautomatiseerde verwerking worden gebaseerd. Om te garanderen dat de vooraf vastgestelde modellen en criteria, het gebruik dat daarvan wordt gemaakt en de gehanteerde databases in de praktijk niet discrimineren en beperkt blijven tot hetgeen strikt noodzakelijk is in het licht van de doelstelling terroristische activiteiten die een ernstige bedreiging opleveren voor de nationale veiligheid, te voorkomen, moet ook regelmatig worden onderzocht of die vooraf vastgestelde modellen en criteria en de gebruikte databases betrouwbaar en up-to-date zijn [zie in die zin advies 1/15 (PNR-Overeenkomst EU-Canada) van 26 juli 2017, EU:C:2017:592, punten 173 en 174]."

VIII. Wat betekenen deze arresten voor Nederland?

29. De Wet op de Inlichtingen- en Inlichtingendiensten is recent vervangen door een nieuwe wet (Wiv 2017, *Stb.* 2017, 317). Naar aanleiding van het referendum over de 'sleepwet' gericht tegen de bepalingen van de wet die met name zagen op de bulkinterceptie via de kabel heeft de in artikel 167 van de wet voorziene evaluatie vervroegd plaatsgehad (*Handelingen I* 2016/17, 35, nr. 8, p. 4). Dit heeft geleid tot het rapport van de Evaluatiecommissie 2017 dat hiervoor al enige malen werd geciteerd. De beoordeling van de Nederlandse situatie moet mijns inziens plaatsvinden in het licht van de voorstellen van de commissie in de hoofdstukken 4, 5 en 8 van haar rapport, met name om de kwaliteit van de wet op het vlak van bulkdata, GDA en internationale uitwisseling aan te passen c.q. te verbeteren. Deze voorstellen sporen met het end-to-end controlesysteem dat het EHRM voorstelt en de waarborgen die in deze arresten, *Schrems II* en de geciteerde uitspraak van BVerfGer voor internationale uitwisseling zijn ontwikkeld. Aangezien dit hele systeem al in de huidige Wiv is ontworpen als een systeem van bevoegdheden dat wordt uitgeoefend in de sfeer van de operaties van de inlichtingendiensten is het toetsingskader dat van het EHRM en niet dat van de EU. De waarborgen tegen discriminatie en automatische besluitvorming die het HvJ EU (zie VII) adresseert zijn al in de huidige wet verankerd (rapport Evaluatiecommissie 3.3.1). Maar op grond van de onduidelijke grenslijn tussen EU en EVRM recht (zie hiervoor onder II) zal ook een EU-toetsing moeten plaatsvinden.

30. Het systeem van toezicht van de Wiv 2017 bracht grote veranderingen. Zo is er een onafhankelijk toezicht vooraf gekomen op de inzet van bijzondere bevoegdheden in de vorm van de Toetsingscommissie Inzet Bijzondere bevoegdheden (de TIB). Het is bestuurlijk toezicht, maar de leden van het orgaan hebben een semi-rechterlijke status. (Voor de eigenaardigheden van deze figuur verwijs ik naar hoofdstuk 9 van het rapport van de Evaluatiecommissie Wiv 2017.) Dat vertoont dus gelijkenis met het Zweedse systeem al is de aanpak minder contentieus, omdat een rechterlijke zitting ontbreekt. Het algemene bestuurlijke toezicht inclusief het ex post toezicht op de uitvoering van de wet is ondergebracht bij de Commissie van Toezicht op de Inlichtingen- en Inlichtingendiensten (CTIVD). Deze Commissie beschikt over vergaande onderzoeksbevoegdheden; zij rapporteert op ieder door haar gewenst moment over deelvragen aan de bewindslieden en via deze aan het parlement en doet daarbij aanbevelingen. Daarnaast maakt zij, evenals de TIB, jaarverslagen. Dit systeem lijkt op het Britse systeem, zoals in het *BBW*-arrest beoordeeld. Daarnaast is er een individuele klachtafdeling bij de CTIVD. Binnen de CTIVD is zij onafhankelijk en haar beslissingen zijn bindend. Feitelijk heeft zij in deze constructie niet de functie gekregen van de Britse IPT en in het licht van de Zweedse uitspraak is moeilijk te zeggen hoe het EHRM deze dubbelrol (toezicht en klachtbehandeling binnen de CTIVD, zij het in een afzonderlijke zelfstandige afdeling) zou beoordelen. Uit de evaluatie blijkt dat de klachtenafdeling in de praktijk slechts een ombudsfunctie vervult bij klachten over op individuen gerichte veiligheidsonderzoeken. Procedures zoals bij de IPT hebben zich niet voorgedaan. Burgers en collectief belang organisatie kunnen echter steeds terecht bij de gewone (burgerlijke) rechter. Zo zijn in Nederland al diverse malen belangrijke uitspraken door de burgerlijke rechter gedaan over privacybescherming (een recent voorbeeld is de *SyRI* uitspraak van de Rechtbank Den Haag 5 februari 2020, *NJ* 2020/386, m.nt. E.J. Dommering). De Evaluatiecommissie constateerde dat in het systeem een beroep op de onafhankelijke rechter ontbreekt over rechtsvragen bij toepassing van de wet door de toezichthouders en de inlichtingendiensten en dat de toepassing van de wet daarop vastloopt. Zij heeft daarom een beperkt beroep van beslissingen van de CTIVD (zowel ten aanzien van het toezicht als ten aanzien van de klachten) op de ABRvST voorgesteld (zie verder hoofdstuk 9 van het Evaluatierapport).

31. Het kabinet heeft de aanbevelingen van de Commissie overgenomen. Omdat de uitspraken van de Grand Chamber van het EHRM op het moment van publicatie van het advies nog niet bekend waren, zal een en ander met die uitspraken moeten worden gefinetuned. Verder zijn er nog de bij het HvJ EU aanhangige zaken die mogelijk meer helder-

heid kunnen brengen over de betekenis van de veiligheidsexceptie van artikel 4 lid 2 VWEU.

E.J. Dommering