Summary of judgment of Czech Republic Constitutional Court 22 March 2011 annulling national measures transposing Data Retention Directive

Key points

- A very comprehensive rejection of the transposing measures, for failing to provide sufficient clarity in purpose definition, retention period, authorities competent for accessing the data, data security provisions. The measures were held to be in breach of the CZ constitution and European human rights law.
- The Court said that it was possible for the legislator to comply with the DRD without breaching the constitution; but it expressed doubts (in *obiter dictum*) as to the necessity and effectiveness of blanket data retention
- Interestingly the Court upheld the plaintiffs view that it was *less* safe for economic operators to keep the store rather than the state
- COM is visiting CZ administration on 17 June to discuss how they intend to respond to this judgment.

The challenge

1. The case for annulment of Section 97(3) and (4) of Act No 127/2005 on electronic communications and amending certain related laws (the Electronic Communications Act), as amended and Decree No 485/2005 on the scope of traffic and location data, the period of retention, and the form and method of transmission thereof to bodies authorised to use them, was brought by 51 deputies of the Chamber of Deputies of the Parliament of the Czech Republic.

2. They objected that

   a) the collection and use of traffic and location data on telecommunications traffic to the extent defined by the contested provisions constituted a disproportionate interference with fundamental rights set out in the Charter of Fundamental Rights and Freedoms and ECHR

   b) this interference may also be regarded as undermining the essential requirements of the democratic rule of law, including the principle of proportionality within the meaning of Article 4(4) of the Charter.

   c) this interference was a direct breach (e.g. familiarisation with the data retained),

   d) measures by government authorities concealed a significant risk of restrictions on fundamental rights, which could occur at any moment with a latent risk of further direct interference by government authorities.

   e) the risk of the potential abuse of such retained data by a large number of private persons working in the field of telecommunications services is higher than if the data were retained by the State. There are insufficient conditions under which data are to be retained and the conditions for their use by

authorised bodies; nor do they make any guarantee to individuals that the data will not be misused.

f) the measures encourage the extensive use of the relevant databases, both in terms of the quantity of data drawn from them and as regards the number of entities that will be authorised to access them; it also allows for an expansion in the purposes for which the data will be used. The persons who could misuse the personal data are often the employees of companies or government authorities processing the data, as well as others (e.g. hackers).

g) the probable and expected benefit arising from the obligation to retain traffic and location data are grossly disproportionate to the associated interference with the fundamental rights

3. Curiously, the applicants argued that the invasion of the Article 8 ECHR right to privacy was permissible in fighting crime only if it serves to prevent crime.*not* in order to solve a crime that has already been committed contravenes Article 8 of the Convention.

4. They argued that the government had failed to provide information as to the number or specific cases, before the introduction of the contested legislation (which entails a huge increase in the quantity of and potential access to the data retained), in which the investigation, detection and prosecution of serious crimes collapsed due to the inability to obtain the required data because such data were not available. Nor is it known whether the establishment of the data retention obligation would genuinely result (or has genuinely resulted) in the improved investigation, detection and prosecution of serious crimes, the aversion of threats, a higher crime-solving rate or a reduction in crime, etc.

5. The applicants also asked the Court to consider submitting a question to the European Court of Justice for a preliminary ruling in accordance with Article 234 of the EC Treaty, concerning the (in)validity of the Data Retention Directive itself. The court rejected this request, on the basis that Community law is not part of the constitutional architecture and that the court did not have competence to interpret that law. *Furthermore, it said that* the Directive itself leaves the Czech Republic *sufficient room to transpose it into national in a manner consistent with the Constitution* as its individual provisions essentially only define the obligation to retain data. The legislator should have, in the areas of retention and handling of data, including measures to prevent data abuse, ensured adherence with Czech constitutional standards

Court's analysis of right to privacy

6. The court analysed case law on the right to privacy, and held that where criminal law facilitates the realisation of the public interest in prosecuting crimes by means of robust tools, the use of which results in severe restrictions on personal integrity and fundamental rights and freedoms of the individual, constitutional limits must be respected in their application. These restrictions may therefore only occur in exceptional circumstances necessitated in a democratic society, provided that the objective pursued by the public interest cannot be achieved otherwise and if this is

acceptable in terms of the legal existence and observance of effective and specific guarantees against arbitrariness. Legislation imposing these restrictions must be precise and clear in its formulation and predictable enough to provide potentially affected individuals with sufficient information about the circumstances and conditions under which a public authority is entitled to interference with their privacy, so that, where appropriate, they can adjust their behaviour so as not to come into conflict with such restrictive provisions. The powers granted to the competent authorities, and the method and rules for exercise thereof so that individuals are given protection against arbitrary interference, must be strictly defined.

7. For any interference with right to privacy, the legislator must demonstrate
    a. That the action is capable of achieving the intended objective of protecting another fundamental right or public good.
    b. Whether there is a need and whether the chosen measure is the most considerate in relation to the fundamental right.
    c. whether the loss incurred in respect of a fundamental right is proportionate to the intended objective.

8. The need to wield such guarantees is even greater as regards the protection of personal data subjected to automatic processing, particularly if these data are used for police objectives or in a situation where the available technology is becoming increasingly sophisticated. National law must, in particular, ensure that collected data are genuinely relevant and not excessive in relation to the purpose for which they were secure

9. The contested Decree of the Ministry of Informatics, despite this fact, has not been amended, resulting in a situation where the scope of the data retained, as regulated by the contested legislation, remains clearly above beyond? the framework of the scope anticipated by the Data Retention Directive.

10. The Court rejected the argument of the parliament that data retention could not be compared with wiretapping, because it is possible to infer, with up to 90% certainty, with whom, how often, and even at what hours an individual is in contact, who his closest acquaintances, friends or colleagues from work are, or what activities he is involved in and at what times of day

Grounds for annulling the CZ measures

11. The Court said that the measures

    a. vaguely and entirely indistinctly impose the obligation on legal or natural persons retaining traffic and location data in the above range "*to provide them, on request, to authorities authorised to request them pursuant to special legislation.*"
    b. Were not clear from the actual wording of the contested provisions of the act or of the explanatory memorandum which authorised authorities are specifically concerned.

c. Therefore, by enabling large-scale interference with fundamental rights, did not meet the requirements of certainty and clarity in terms of the rule of law.

12. There was no clear and precise definition of the purpose for which the traffic and location data are to be provided to authorised authorities, making it impossible to assess the contested legislation with regard to actual needs. The restriction in the DRD of the purpose to *the investigation, detection and prosecution of serious crime* is not reflected with (although it does not specify what sort of crime this is) was not reflected in the transposing measures or in the Criminal Code, so there was in effect no clear restriction on the purpose. (The Court also called on the legislature to amend the criminal code.)

13. There was a 'completely vague' definition of conditions for the use of data retained *"on the realisation of telecommunications traffic" in order to "clarify facts relevant to criminal proceedings"*.

14. The result was a situation where this instrument, is used (and abused) by law enforcement agencies even for the purposes of investigating petty (less serious) crime.

15. The measures quite inadequately (if at all) establishes clear and detailed rules laying down minimum requirements designed to keep retained data secure, in particular by preventing third-party access and setting out procedures to protect the integrity and confidentiality of data, as well as data destruction procedures. They also fail to provide the individuals concerned with sufficient guarantees that their data would not be at risk of abuse and arbitrariness.

16. The definition of the period of retention, i.e. *"not less than six months and not more than 12 months"*, the expiry of which gives rise to the obligation to destroy the data, is ambiguous and, considering the scale and sensitivity of the data retained, 'woefully inadequate'.

17. For none of these obligations do detailed rules and specific procedures for their implementation exist. There are no strictly defined requirements for the security of the data retained. The way the data are handled, either by the legal or natural persons retaining the traffic and location data, or, following a request, by authorised public authorities, is not sufficiently ascertainable, nor is a specific means of data destruction established. Likewise, there is no definition of responsibilities or penalties for failure to comply with such obligations, including the absence of the possibility for the individuals concerned to seek effective protection from abuse, arbitrariness, or con-compliance with set obligations. Oversight by the Office for Data Personal Protection *"of compliance with obligations in the processing of personal data"*

<u>Doubts about necessity and effectiveness of data retention in principle and in practice</u>

18. Accepts that evolutions in criminal behaviour need to be addressed. But Court has doubts about whether the blanket and preventive retention of traffic and location data on almost all electronic communications is a necessary and appropriate tool

given the intensity of its interference with the private sphere of a vast number of electronic communication users.

19. The Constitutional Court also had doubts effective tool, especially given the existence of anonymous SIM cards, according to observations by the Czech Police Force, account for up to 70% of communications used in the commission of crime. It refers to the analysis by the German BKA - published by AK Vorrat (!) - which, after comparing statistics on serious crimes committed in Germany in the period before and after the adoption of the legislation on data retention, arrived at the conclusion that the use of the blanket and preventive retention of traffic and location data had little effect on reducing the number of serious crimes committed or on improving the crime solving rate.

20. Doubts as to whether it is desirable for private entities (providers of Internet, telephony and mobile communications services, especially mobile operators and companies providing Internet access) to be granted the power to retain all data about the communications provided by them, as well as about customers to whom their services are provided (i.e. data beyond the scope of the data which they are required to retain by the contested legislation), and to dispose of such data freely for the purposes of recovering debts and developing their business activities and marketing operations.

10 June 2011

Data retention directive: Meeting with CZ Ministry of Industry and Trade, Prague 15 June 2011

lectronic Communications Department
lectronic Communications Department
DG Home Affairs

1. The meeting was set up at COM's initiative to discuss a) how CZ intended to respond to the decision of their constitutional court judgment annulling their measures transposing the Data Retention Directive (DRD) and b) CZ views on possible recast of the DRD

Transposition

2. JN said that the following week he expected the senior official in the ministry to write to DG explaining procedures and next steps for responding to the 22 March constitutional court judgment annulling the CZ transposing measures. JN said that the problem with both CZ and DRD was that the laws were rushed; in CZ there had been insufficient background - they relied too much on the DE transposing law. They disagreed with certain premises in the judgment – e.g. there were in fact data security measures in the now annulled telecommunications act.

3. CZ had set up a working group consisting of officials from ministries of interior, justice, industry and trade to prepare a new draft law. They were meeting with members of parliament who brought the case the case before the constitutional court. There would be a public consultation in the summer in which would explain the importance of data retention for solving problems such as car theft, gang crime, and locating missing children. They expected a proposal to be laid before parliament in autumn. Ministry of the Interior was in the lead, Ministry of Industry was responsible for implementation. This was not controversial in CZ as in DE – 'one day's headlines and then forgotten'.

4. On purpose limitation, CZ will narrow the old provision so that it applies only to specific crimes and those listed in international treaties, plus those carrying 3 years prison otherwise, no major changes were envisaged.

Review of the directive

5. CZ considered DRD a very valuable tool and wanted to support it – polite but general resistance to any significant changes.

6. On *purpose limitation,* JN was sceptical about whether it would be possible to have a single definition of serious crime. Data retention should cover also what CZ defined as civil offences and all crimes connected with the network e.g. email or telephone threats.

7. Reluctant to broaden scope as it would be costly for MS to pay for the data. Market of telecommunications companies is smaller than for information society services. There would be a huge cost for compensating this. On the other hand new mobile networks (not GSM) should be covered with different procedures.

8. *Statistics* created a burden for MS; it was better to hold a meeting and collect best practices on implementation. Under the old CZ law, the obligation for stats was operators; it's a 'huge problem' to get them from police or courts.

9. On *rentetion* period, 6 months is preferable; 1 year would be difficult to justify.

10. On *who should be able to access*, there be no strict rules. Whoever needs it in accordance with their roles should be allowed to do so.

11. On *cost recovery* – costs should be reimbursed by state bodies because it makes it easier to regulate, to get a better service from operators, and to protect against excessive use. CZ law includes a specific decree which covers investment and per-request cost which were agreed with the operators. – asked them to support the COM. This will remain in the new law (although Ministry of Interior have not been in favour).

16 June 2011