Data Protection at the European Court of Human Rights: Fundamental Principles and Recent Developments

Judge Marko Bošnjak – European Court of Human Rights

European Judicial Training Network - April 22-23, via Zoom

Introduction:

This presentation will address:

1. Fundamental principles of data protection law in the Convention framework.
2. Three recent developments in the Court's jurisprudence on data protection.

This first section will address the fundamental principles of data protection at the Strasbourg Court, answering the following questions:

1. What is Data Protection? (Broadly)
2. How does the Convention understand 'data'?
3. What protections does it provide?

It will then turn to three recent developments in the Court's case law.

1. What is Data Protection? (Broadly)

Data protection law is the law relating to the protection of individual data, including that which may be of a sensitive or personal nature.

2. How does the Convention define 'data'?

- While the Convention itself does not define 'data', Council of Europe Convention no. 108 (1981, in force 1985), defines personal data broadly as:
  - 'any information relating to an identified or identifiable individual' (cited in *Amann v. Switzerland,* for example).
  - This identification also extends to means of indirect identification such as an IP address (as established by the Court in *Benedik v. Slovenia*).
  - The Court has established that the data of legal persons is also protected, including companies (see *Larsen Holding v. Norway*) and NGOs *(*see *Liberty and Others v. the United Kingdom).*
- Types of data protected by the Convention have included:
  - Voice recordings
  - DNA samples
  - Fingerprints
  - Banking documents
  - Professional details
  - Electronic data
  - Video surveillance data, including public CCTV data
  - Income and taxable assets
  - Data relating to birth and identity.
  - Details of political activity
  - The storage of names on a police database
  - GPS data
  - Documents disclosing ethnic or racial identity.
- Convention 108 also defines 'data processing' (at Article 2) as '"any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data'.

- However, where the gathering of data has been purely coincidental rather than "systematic or permanent" (*Mehmedovic v. Switzerland*), it has been found not to be protected by the Convention.
- Similarly, where blood samples were taken for identification purposes, then destroyed once consent forms had expired, the Court considered that the state had not interfered with the Convention (*Cakicisoy v. Cyprus*).

3. How is data protected by the Convention?

Personal data protected by Article 8 of the Convention, which includes the right to personal data as part of 'private life' and/or correspondence. The Court has dealt with data protection issues under Article 8 since the 1987 *Leander v. Sweden* judgment.

Article 8 (1) provides that everyone within the Court's jurisdiction shall enjoy the right to respect for his private and family life, his home and his correspondence.

This means that any interference with those interests will require state justification. In *S. and Marper v. UK,* the Court set a low threshold for "interference", holding that:

> *"The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8…"* (para 67).

The same judgment also provides the authoritative list of safeguards that are to be provided by the state in order to prevent abuse of personal data and ensure compliance with Article 8:

> *"The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article […] The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are* ***relevant and not excessive*** *in relation to the purposes for which they are stored; and* ***preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored*** *[…] The domestic law must also afford adequate guarantees that retained personal data were* ***efficiently protected from misuse and abuse****. The above considerations are especially valid as regards the protection of special categories of* ***more sensitive data*** *and* ***more particularly of DNA information****, which contains the person's genetic make-up of great importance to both the person concerned and his or her family..."* (para 103)

Article 8 imposes both a negative obligation on the state for public authorities to not interfere with these rights and a positive obligation to ensure respect for those rights in the public sphere, for example. It is to be noted that this positive obligation equally extends to relations between private individuals. As established in *Bărbulescu v. Romania*:

> *"While the essential object of Article 8 of the Convention is to protect individuals against arbitrary interference by public authorities, it may also impose on the State certain positive obligations to ensure effective respect for the rights protected by Article 8."* (para 108).

Surveillance carried out by an employer, as in that case, will require that the domestic authorities *"afford adequate protection"* of Article 8 and *"strike a fair balance"* between competing interests (para 141)

Article 8(2), then, sets out the framework within which contracting states may justify interferences with Article 8(1). It states that:

> *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.*

In practice, this requires that any state interference with data protection complies with three requirements:

1. Legality (that the interference is "in accordance with the law")
2. Legitimacy (that the interference pursues one of the legitimate aims listed in Article 8(2))
3. Proportionality (that the interference is "necessary in a democratic society")

These will be addressed briefly in turn, followed by analysis of recent developments in this field.

1. Legality (that the interference is "in accordance with the law")

Article 8(2) requires that the interference not only complies with national law, but also that the national law displays the "quality of law" required by the Convention and developed through the Court's case law. In *Malone v. the United Kingdom,* the Court clarified that *"the phrase "in accordance with the law" does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law."* (para 67).

This requires, for example, that the law justifying the interference is sufficiently clear, accessible and foreseeable, such that it protects the individual from arbitrariness (*Leander v. Sweden,* para 51) and enables the individual to regulate his conduct accordingly (*Ammann v. Switzerland,* para 56).

In many cases that fail on the ground of legality, the national law has failed to clearly delimit the scope and extent of the discretion granted to national authorities when executing a particular power. See, for example, judicial discretion in *Kruslin v. France* or police discretion in *M.M. v. the United Kingdom.* (Short summaries of these cases – and further examples – are included in the handout).

2. Legitimacy (that the interference pursues one of the legitimate aims listed in Article 8(2))

In listing the grounds on which interferences with Article 8 may be justified, Article 8(2) limits the state to interfering with personal data only to the cases in which that interference protects:

> *"…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."*

3. Proportionality (that the interference is "necessary in a democratic society")

The more complex question, however, is whether the measure is "necessary in a democratic society" – in other words, whether the interference made by the state is proportionate to the legitimate aim that it invokes to justify that interference.

The term 'necessity' is therefore understood, as explained by the Court in *Leander v. Sweden,* to mean that *"the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued"* (para 58).

The *Silver v. United Kingdom* case famously set out four central principles on the meaning of this phrase (at para 97):

1. 'Necessary' is not as stringent as 'indispensable' nor as open as 'reasonable' or 'desirable'.
2. Contracting states enjoy a margin of appreciation on how Convention rights are protected. This will vary depending on contextual factors. Crucially, the *Handyside* case noted that this margin *"goes hand in hand with European supervision."* (at para 49 of that case).
3. Any interference must respond to a pressing social need and be proportionate to the legitimate aim pursued (as recalled in *Leander*)
4. Exceptions to rights (such as Art. 8(2)) are to be interpreted narrowly.

Recent Developments

Turning now to what these standards mean in practice, the following section discusses three recent (or upcoming) developments in the Court's case law on data protection.

1. Recent Development 1: Data Retention

An important aspect of data protection law is the question of data retention. In a series of recent judgments, the Court has developed its position on the circumstances and duration of data retention permitted by Article 8.

As the Court summarised in *Gaughran*, just two member states indefinitely retain data connected to criminal convictions (such as fingerprints and DNA profiles), 21 have set retention periods, and five states provide for limits and review instead.

This raises the question – should absolute limits be imposed on data retention, and – even if a consensus exists across the Court's *espace juridique* – should the Convention enforce those standards across its jurisdiction?

Catt v. the United Kingdom (Chamber, January 2019):

- This January 2019 judgment concerned a 90-year-old applicant with a long history of attending non-violent protests. The applicant had no criminal record or history of violence, yet the police continued to hold material related to his frequent attendance of peaceful protests – data which of course disclosed his political affiliation.
- He alleged a violation of Article 8 on the basis that the police held video recordings of him attending these protests on a domestic extremism database. The Court held that while the collection of the data had been necessary, the indefinite retention of that collected data was disproportionate.
- This case presents a number of questions:
    - Would the retention have been lawful if the applicant had a criminal record?
    - Should that criminal record have to reach a certain threshold of seriousness in order to prolong the lawful period of data retention?
    - Is it relevant that the data revealed the applicant's political affiliations?
    - Does data have to reveal something intimately *personal* in order to be protected by Article 8? Should that effect the legality and/or duration of the retention?
- The Court's jurisprudence has developed answers to some, but not all of these questions.

Gaughran v. the United Kingdom (Chamber, February 2020)

- In February 2020, the Court handed down its verdict on an application brought by an individual with a spent drink-driving conviction, whose personal data (in this case, a DNA profile, fingerprints and a photograph) was subject to indefinite retention.
- Unlike *Catt,* the applicant had been convicted of a criminal offence.
- Nonetheless, the Court still found a violation of Article 8, holding that the indefinite retention of this data overstepped the margin of appreciation afforded to national authorities.
- The Court also considered that indefinite retention of a DNA profile constituted a weightier interference with Article 8 than lifetime retention, taking into account the possible importance of a DNA profile for family members.
- The Court specifically criticised the national authorities for not having assessed the necessity of the continued retention, the seriousness of the offence or the possibility of review (paras 87-88) in its proportionality analysis.
- More broadly, it found that the strength of consensus against indefinite retention in Council of Europe states narrowed the UK's margin of appreciation on that point.

Trajkovski and Chipovski v. North Macedonia (Chamber, February 2020)

- Decided on the same day as *Gaughran,* the Court made the same finding in relation to two applicants convicted of aggravated theft.
- Key point (from both cases): Indiscriminate retention without reference to seriousness of the offence or the need for indefinite retention will violate the Convention.
- Question: could a more severe crime justify indefinite retention?
    - Relevant here is *B.B. v. France,* where 30 years' data retention was deemed proportionate in the case of a sex offenders databased.
    - Also: *Peruzzo and Martens v. Germany* was filed by two applicants who had been convicted of drug and violent offences, respectively. Their data was to be held for up to ten years for identification purposes. The application was deemed proportionate to such an extent that the application was manifestly ill-founded.
- Further Questions: Where can this line be drawn? Can an absolute limit be established? Would this need to be established for different kinds of criminal offence?

2. Recent Development 2: Mass Surveillance Regimes

Big Brother Watch and Others v. the United Kingdom:

- This application, brought by a group of British NGOs, complained that the United Kingdom's bulk interception and intelligence sharing regimes violated Article 8. The Court held that bulk interception of data did not violate Article 8 per se but found that the UK's means of selecting relevant material from intercepted data lacked adequate safeguards. This was because the mass surveillance regime fulfilled neither the "quality of law" requirement nor was it proportionate to the legitimate aim in question. The Court found no violation, however, with respect to the UK's practice in sharing data with other governments, with the applicants having emphasised its intelligence links with the United States in that connection.
- This case was referred to the Grand Chamber of the Court on 4 February 2019 and a Grand Chamber hearing took place on 10 July 2019.
- Further Questions:
    - What measures could ensure compliance with Article 8 in the context of mass surveillance/bulk data interception?
    - Should these be mandatory minimum requirements or interchangeable?
    - Does mass surveillance require greater and/or different safeguards or standards of protection from targeted individual surveillance?
    - How does the sharing of intelligence with non-contracting states engage the convention? Does/should the Court's jurisdiction extend to the sharing of data retrieved by mass interception?

3. Recent Development 3: Tax Records

Casarini v. Italy:

- In a case currently communicated by the Court on 8 February 2021, *Casarini v. Italy,* a political activist had his tax records leaked to a journalist by an officer of the Italian Revenue Police, who had taken them from the database of the Taxpayers Information Service *(Servizio per le informazioni sul contribuente).* The officer had accessed the data 1,340 times in the years 2008-09 on the journalist's request. Both the officer and the journalist had been convicted of unauthorised access to the system and given suspended prison sentences.

- The applicant alleges a violation of Article 8 on the basis that the Italian tax records system lacks the required safeguards against abuse of access to personal data.
- Regarding these safeguards, the Court has requested that the Italian government clarify the following details both as they were at the material time and at present:
    - the data which is collected in the database;
    - the length of the data retention in the database;
    - the bodies or officials having access to the database;
    - the purposes for which the data stored in the database can be used;
    - who and how can authorise searches in the database;
    - the bodies or officials reviewing compliance with domestic law.
- The government have also been asked to disclose whether the following measures were put in place by the Italian Revenue Police:
    - sufficient security measures for access to the tax registry;
    - an automated monitoring system which could effectively identify irregular access;
    - an effective tracking system for access and searches in the database and systematic controls on the workstations of its agents.
- Further questions:
    - Are tax records 'data' for the purposes of Article 8? Should they be considered as such? Why/why not?
    - What obligations should be placed on states as concerns the protection of data in databases of this kind?
    - Which of the safeguards requested by the Government should be mandatory, if any?