„necessity and proportionality“

Ralf Bendrath

EDPS Civil Society Summit

16 June 2016

Foundations

ECHR

Article 8 – Right to respect for private and family life

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.

ECHR

Article 13

Right to an effective remedy

Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

EU CFR

Article 7

Respect for private and family life

Everyone has the right to respect for his or her private and family life, home and **communications**.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such **data must be processed fairly** for specified purposes and on the basis of the consent of the person concerned or some other **legitimate basis laid down by law**. Everyone has the **right of access to data** which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

EU CFR

Article 47

Right to an effective remedy and to a fair trial

Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

EU CFR

Article 52

Scope of guaranteed rights

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and **respect the essence of those rights and freedoms**. Subject to the principle of **proportionality**, limitations may be made only if they are **necessary** and **genuinely meet objectives of general interest** recognised by the Union **or the need to protect the rights and freedoms of others**.

2. (...)

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the **meaning and scope of those rights shall be the same as those laid down by the said Convention**. This provision **shall not prevent Union law providing more extensive protection.**

Summary

- respect for correspondence / communications
- protection of personal data; access to the data
- interference / limitation only if
  - necessary and proportionate in a democratic society
  - genuinely meet objectives of general interest or the need to protect the rights and freedoms of others
  - legitimate basis laid down by law
  - respect the essence of those rights and freedoms
  - effective remedy

Case-Law (examples)

ECtHR Klass and Others v Germany (1978)

“the Court stresses that **this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance**. The Court, being aware of the danger such a law poses of **undermining or even destroying democracy on the ground of defending it**, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.

The Court must be satisfied that, whatever system of surveillance is adopted, there exist **adequate and effective guarantees against abuse**. This assessment has only a relative character: it depends on **all the circumstances of the case**, such as the **nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law**.

[…] **measures may only be ordered if the establishment of the facts by another method is without prospects of success or considerably more difficult**; even then, the **surveillance may cover only the specific suspect or his presumed "contact-persons**"

ECtHR *S and Marper v UK (2008)*

"the Court finds that the **blanket and indiscriminate** nature of the powers of **retention** of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences […] **fails to strike a fair balance** between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a **disproportionate** interference with the applicants' right to respect for private life and **cannot be regarded as necessary in a democratic society**. This conclusion **obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards**, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data.."

ECtHR Zakharov v. Russia (2015)

"The Court concludes that Russian legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and **the risk of abuse which is inherent in any system of secret surveillance**, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications. In particular, the circumstances in which public authorities are empowered to resort to secret surveillance measures are not defined with sufficient clarity. Provisions on discontinuation of secret surveillance measures do not provide sufficient guarantees against arbitrary interference. **The domestic law permits automatic storage of clearly irrelevant data** and is not sufficiently clear as to the circumstances in which the intercept material will be stored and destroyed after the end of a trial. **The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when "necessary in a democratic society".** The supervision of interceptions, as it is currently organised, does not comply with the requirements of independence, powers and competence which are sufficient to exercise an effective and continuous control, public scrutiny and effectiveness in practice. The **effectiveness of the remedies is undermined by the absence of notification at any point of interceptions**, or adequate access to documents relating to interceptions."

CJEU Digital Rights Ireland (2014)

"Directive 2006/24 covers, **in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made**."

"Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is **not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons** likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences. "

"that [retention] period is set at between a minimum of 6 months and a maximum of 24 months, but it is not stated that the **determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is strictly necessary**."

"Directive 2006/24 entails a **wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU**, **without such an interference being** precisely circumscribed by provisions to ensure that it is actually **limited to what is strictly necessary**."

CJEU Schrems (2015)

"In particular, legislation permitting the public authorities to have **access on a generalised basis to the content** of electronic communications must be regarded as **compromising the essence of the fundamental right to respect for private life**.

Likewise, **legislation not providing for any possibility for an individual to pursue legal remedies** in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, **does not respect the essence of the fundamental right to effective judicial protection."**

Political Reality

EUROPEAN COMMISSION

Brussels, 18.4.2011
COM(2011) 225 final

REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

Evaluation report on the Data Retention Directive (Directive 2006/24/EC)

no proof of necessity

„Overall, the evaluation has demonstrated that data retention is a **valuable** tool for criminal justice systems and for law enforcement in the EU."

"Reliable quantitative and qualitative data are crucial in demonstrating the **necessity** and **value** of security measures such as data retention. (…) **It has not been possible to meet this objective** given that most Member States only fully transposed the Directive in the last two years and used different interpretations for the source of statistics."

"Statistics provided by 19 Member States (…) indicate that, overall in the EU, **over 2 million data requests were submitted each year**, with significant variance between Member States, **from less than 100 per year (Cyprus) to over 1 million (Poland)**. (…) Statistics do not indicate the precise purpose for which each request was submitted. (…) **There is no obvious explanation for these variances**."

"Member States generally reported data retention to be **at least valuable**, and in some cases indispensable, for preventing and combating crime."

no learning curve

- already half a year earlier: „data retention is here to stay“ (Malmström)
- CJEU disagreed in 2014
- Member States still want to keep it
  - Germany even adopted new law against CJEU and constitutional court rulings

EUROPEAN COMMISSION

Brussels, 2.2.2011
COM(2011) 32 final

2011/0023 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

{SEC(2011) 132 final}
{SEC(2011) 133 final}

no proof of necessity

- no majority in the EP for 4 years, LIBE rejected
- pushed by COM through pilot project funding
- EU-Canada PNR agreement at the CJEU
  - hearing in April was extremely critical
- Member States and grand coalition in EP hammered out a deal to show they are „against terrorism“

EUROPEAN
COMMISSION

Brussels, 6.4.2016
COM(2016) 194 final

2016/0106 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and

amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011

no proof of necessity

- better statistics about over-stayers
  - for 480 million Euros
- data retention massively expanded
  - changed from 181 days to 5 years
- law enforcement access
  - purpose limitation under Art. 8 CFR?

What to do?


Freiheit statt Angst
KEIN 4 REICH

HELP US SEND THESE POSTCARDS !

EDRi

NOPNR

NO MASS SURVEILLANCE OF YOUR TRAVEL DATA


vi eu ws

Borderline

The EU's New Border Surveillance Initiatives

Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders" Proposals

A study by the Heinrich Böll Foundation

Opinion of the European Data Protection Supervisor

on the Proposals for a Regulation establishing an Entry/Exit System (EES) and a Regulation establishing a Registered Traveller Programme (RTP)

More horizontal approach?

NECESSARY & PROPORTIONATE

The International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles" or "13 Principles") show how existing human rights law applies to modern digital surveillance. Drafted by a global coalition of civil society, privacy and technology experts in 2013, they have been endorsed by over 600 organizations and over 270,000 individuals worldwide.

THE 13 PRINCIPLES **REPORTS**

13 Principles

- **Legality**
- **Legitimate Aim**
- **Necessity**
- **Adequacy**
- **Proportionality**
- **Competent Judicial Authority**
- **Due Process**
- **User Notification**
- **Transparency**
- **Public Oversight**
- **Integrity of Communications and Systems**
- **Safeguards for International Cooperation**
- **Safeguards Against Illegitimate Access**

EUROPEAN DATA PROTECTION SUPERVISOR

Developing a 'toolkit' for assessing the necessity of measures that interfere with fundamental rights

Background paper

- for consultation -

first thoughts

- Full disclosure: I was against the 13 principles in 2013
  - Civil society proposing criteria for surveillance???
  - rather go into full attack mode after Snowden!
- EDPS has a different role
  - advising legislators at EU level

first thoughts

- EDPS „toolkit“ should be stricter in defining the limits of what is ok.
- By all means avoid it being used as mere exercise / checklist for adopting surveillance measures.
- On the other hand: Who will really use it?
- Does anybody read impact assessments?
  - Do they matter politically?

first thoughts

- The hard part is to translate the principles / toolkit to each new proposal anyway.
- Each new proposal is different, the narrative and social field around it are important.
- Case law is very dynamic these days, avoid impression to CJEU and others that we have stable criteria for acceptable / unacceptable surveillance.

</talk>
<discussion>