2014 ISSE

What Now?

Data Retention Scenarios after the ECJ Ruling

Bruxelles, 14 October 2014

Alessandro Guarino
CEO, StudioAG

Background

ISSE 2014

Data Retention

the storing and processing of detailed information about phone calls and internet communications

Was regulated in the European Union by the 2006/24 directive (and its national transpositions)

Background

The European Court of Justice declared early in 2014 the directive invalid because its provisions gravely infringe on fundamental rights, namely privacy and data protection.

This opens of course new scenarios in the onging debate on the regulation of online activities.

Background

The European Directive on data retention (2006/24/EC of 15 March 2006) was born at the peak of the post-9/11 historical period.

- Rationale: the extreme usefulness of the information generated in the course of operations of mobile and ICT networks for criminal investigations in general and particularly for those regarding Organised Crime and Terrorism, where reconstructing networks of contacts is important.

Background

Existing EU legislative context:

- Data Protection directive
- Directive on data processing by network services providers

Objects:

- Protect individuals from misuse of their data
- Fundamental right recognized both by the EU Charter and the UN Declaration of Human rights

Background

ISSE 2014

Pragmatic approach

- Risk based: controllers of personal data must assess risks, manage them and are allowed to accept a residual risk

Motivations of EU directives in general

- Remove obstacles to single internal market
- Observed in the text of DR Directive (Art. 6 & 21)

Background

2014 ISSE

Legislative context - transpositions

- Different for each Member State
- Example – Italy – Risk-based approach totally lost in translation, strictly beaurocratic approach – extended to legal persons!
- MSs also mandated to establish a supervised independ authority

The directive

Scope of the Data Retention directive

What is it all about?

- COMMUNICATIONS (phone calls, texts, internet – email, chat, web and all the rest)
- METADATA (context not content)

The directive

Metadata:

- User Id or Phone number
- ***Name & (physical) address of subscriber***
- Date/time (beginning, end of comm.)
- IP addresses (for Internet comms)
- Terminal equipment or Internet service used
  - IMSI/IMEI, date/time for prepaid, dial-up number or xDSL endpoint
- Cell ID / geolocalized

The directive

Only (meta)data originating in the operator's network and

...in the course of normal operations

The ECJ ruling

ISSE 2014

Origins of the case

- Groups in IE & AT challenged the national data retention laws (transpositions)
- IE: Digital Rights Group
- AT: Local government & citizens

The ECJ ruling

2014 ISSE

The question

- Were the provisions in the Directive contrary to the EU treaties, i.e.:
- Necessary, proportionate?
- (to achive the stated objectives – internal market)

Specifically – is the directive in contrast with the Charter?

The ECJ ruling

The EU Fundamental Charter

- Part of the EU treaties since Lisbon

Art. 7 – Right to privacy

Art .8 – Protection of personal data

- Not the same thing!

Art. 11 – Freedom of expression

The ECJ ruling

The reasoning of the Court:

First: assessing the relevance of those articles of the Charter as to the validity of the directive

- More than enough to reach a decision, as we'll see...

The ECJ ruling

ISSE 2014

Stated by the ECJ:

- Bulk collection of metadata is enough to infringe on individuals' personal lives and privacy, even (possibly) on freedom of expression
- Even if “anonymized”, an this is not the case in Europe (full data of subscriber is retained)

The ECJ ruling

Interference?

- Is there an interference with fund rights?

The answer of the ECJ is yes

- The obligation of retention, the stated period (up to two years) were by themselves an infringment
- No notification to the subjects

Conclusion: “the interference on fundamental rights allowed is enough to generate a feeling that lives are costantly under surveillance”

The ECJ ruling

This is not enough however to declare invalid the legislation

ECJ goes on to examine the justification provided for this interference

- The Charter states the conditions under which a protected fundamental right CAN be limited

The ECJ ruling

ISSE 2014

Conditions for the limiting of rights:

- Limitation must be provided by law
- Necessary
- Proportionate

Clearly provided by law (the directive...) so let's examine the others...

The ECJ ruling

Necessity (to achieve stated objectives):

- Objectives:
- Contribute to the fight against serious crime (and ultimately to public security, itself a fundamental right)
- In general, of assuring international peace

Clearly objectives of general interest, so the means are appropriate, given the ubiquity of electronic communicationas

- Data retention *per se* does not affect fundamental rights even if it is “a serious interference”

The ECJ ruling

2014 ISSE

Proportionality

The law fails this test and the ECJ proceeds to explain why:

- The scope of retention "involves […] the entire EU population without any discrimination"
- No relation is requested btw retained data and a specific threat to security (date, time interval, geographic zone, specific suspects...) →

The ECJ ruling

Proportionality

- No limitations to data access by national authorities were specified and no objective criteria by which access is limited to specific authorized persons.
- Also, access not dependant by a ruling by a Court or independent authority.
- Minimum period (6 months) deemed excessive, maximum period of two years without objective criteria for determining the exact period.

The ECJ ruling - Conclusion

2014 ISSE

Summary:

No clear defined rules were governing the extent of the interference with fundamental rights (which, remember could be legal)

“Wide ranging and particularly serious interfernce with this fundamental rights”

The ECJ ruling - Conclusion

Data protection

- No clear safeguards for the protection of retained data were specified

(note that interference w/ freedom of expression was not even discussed)

Conclusion: the directive

"[...] has exceeded the limits imposed be compliance with the principle of proportionality [..]" and is declared invalid

The aftermath

2014 ISSE

Policy level

- Shows growing concern in the EU (at least the Court) for civil rights, online privacy and freedom.
- Step towards a more balanced view: we can acknowledge that terrorist is not the #1 threat for Europe (or maybe it is.... in the meantime new groups are born almost on cue).
- EU Co-legislators will have to take this into consideration in the “trilogue” for a new directive.
- First sign of a transatlantic “divorce”?

The aftermath

2014 ISSE

Legal

- All national legislations transposing the directive are still in place → Balkanizaton, not single market
- AT: repealed
- IE: repealed
- UK: DRIP!


theguardian

home › UK | world | sport | football | comment | culture | economy | life | fashion | all sections

UK news

National Crime Agency director general: UK snooping powers are too weak

Exclusive: Crime agency boss says he needs to persuade public to reduce digital freedoms

The aftermath

The network operators

- While nothing changes in the short term (maybe it has already) they will have to monitor closely evolving legislation in all member states...
- Higher costs?

The aftermath

Forensics and digital investigations

- Harder?
- It's true that digital investigations have leveraged Big Data techniques and the availability of huge datasets on online activities
- Alternatives are possible. More targeted and supervised, vs. dragnet

Proposals

It is a position paper so...

- Opinions are allowed
- A new directive is needed to harmonize legislation in Europe, involving all stakeholders and of course the co-legislators
- Consultation process involving all point of views to achieve a more balanced legislation (many forums exist, among others the CSCG, the MSP etc.)

Proposals

New directive:

- Shorter maximum retention period
- Accountable procedures for accessing data
- Retention limitations, targeted
  - Temporal
  - Geographical
  - Targets
- Provisions for “right to be forgotten”, if the persons is not subject to investigations

Thank you!
Any questions?

2014 ISSE

Contacts:

a.guarino@studioag.eu

@alexsib17

Full Paper is Freely Available at:
www.studioag.pro
(Information Security Blog)

StudioAG – Infosec Consultancy Firm
www.studioag.eu

References

CEN-CENELEC-ETSI Cyber Security Coordination Group: “Recommendations for a Strategy on European Cyber Security Standardisation”, 2014 (http://www.cscg.focusict.de)

European Court of Justice: “Judgment of the Court of 8 April 2014 in joined cases C-293/12 and C-594/12”

“Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provisions of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC”. In: “Official Journal of the European Union” 13.4.2006

Guarino, Alessandro: “Digital Forensics as a Big Data Challenge”. In: “ISSE 2013 Securing Electronic Business Processes”, Springer, 2013, p. 197-203.

Masys, Anthony (ed.): “Networks and Network Analysis for Defence and Security (Lecture Notes in Social Networks)”, Springer, 2014.