



ITU Kaleidoscope 2015
Trust in the Information Society

Regulation and Standardization of Data Protection in Cloud Computing

Martin G. Löhe and Knut Blind

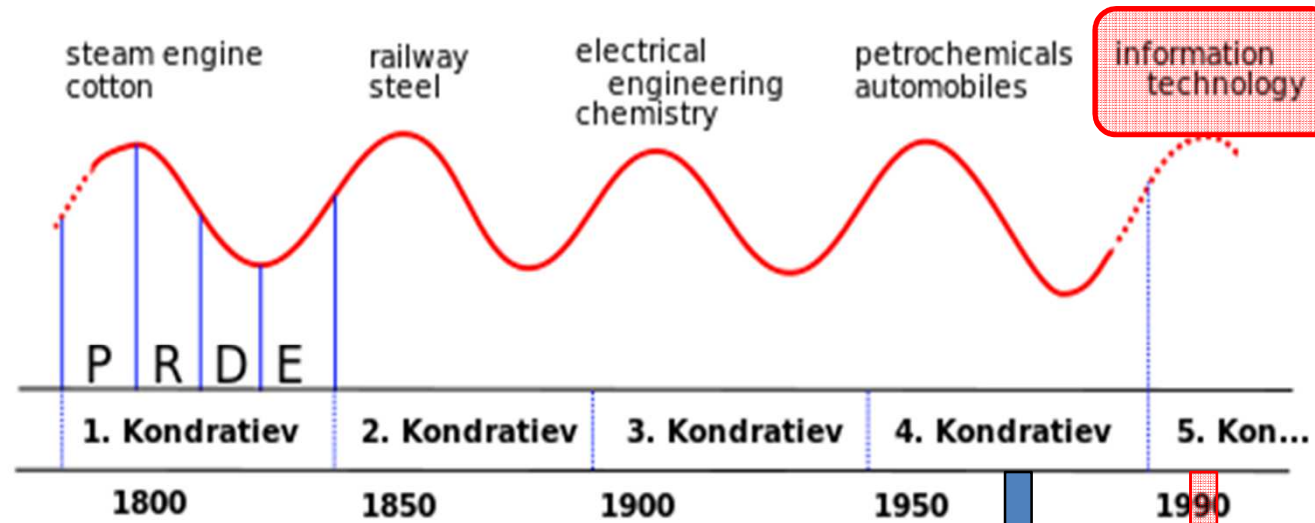
Technische Universität Berlin, Faculty of Economics and
Management, Chair of Innovation Economics

loehe@tu-berlin.de

Barcelona, Spain
9-11 December 2015



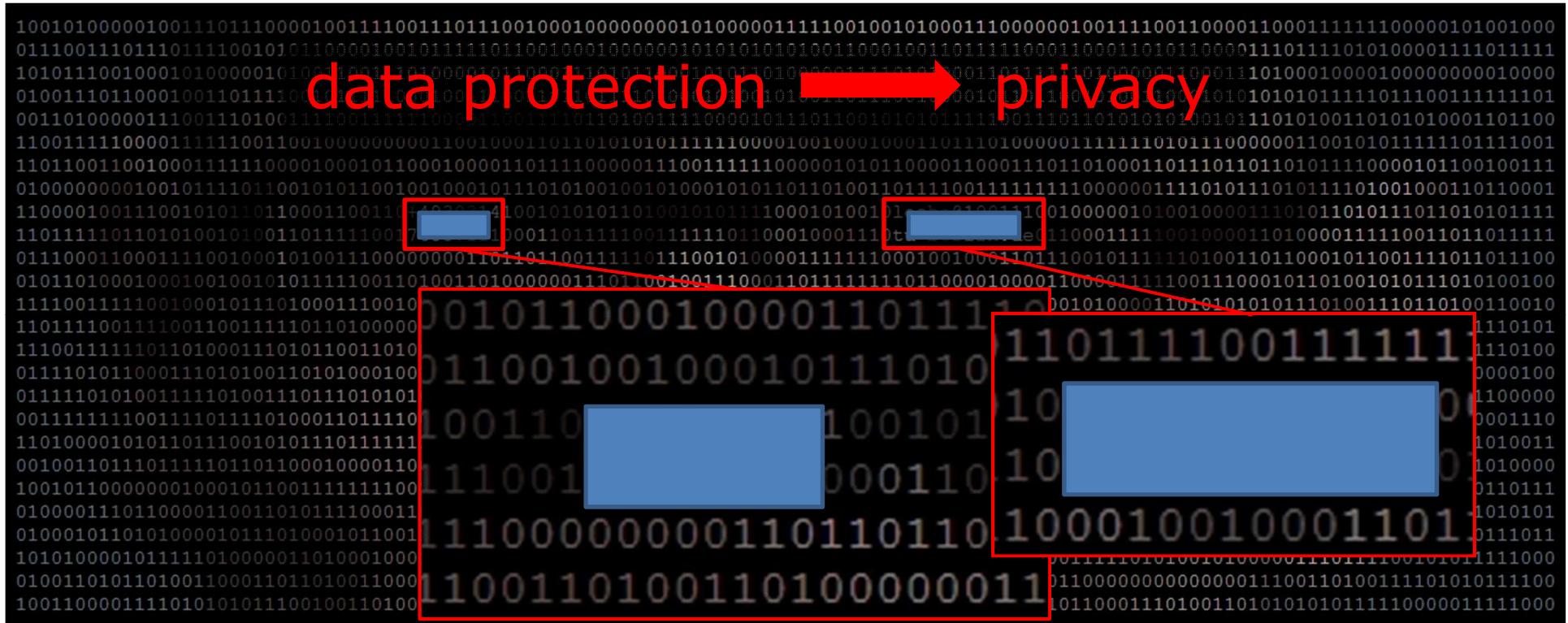
The Importance of Data



Economic Perspectives on Data

- If data is the new oil, data protection is an *economic* issue.
- Data (and also personal information) is *traded* on markets.
- Regulation of data protection is a form of *market regulation*.

Data Protection and Privacy



- Most jurisdictions have rules (laws, constitutional rights, etc.) on data protection and privacy.

The example of cloud computing



- Cloud computing: IT services virtualized by a network
- Allows an efficient management of IT resources and data.
- Facilitating use
- Preventing “oil spills”

Goals of ISO/IEC 27018: addressed issues

- **B2B** standard for protecting **customers'** assets
- Easier compliance with law
- More transparency
- Easier outsourcing
- Compliance verification by audits.

How to use it...

- Risk assessment
- Select measures from controls
- Get certificate

Challenge: Worldwide data – national regulation

How can worldwide usable cloud computing be effectively regulated?

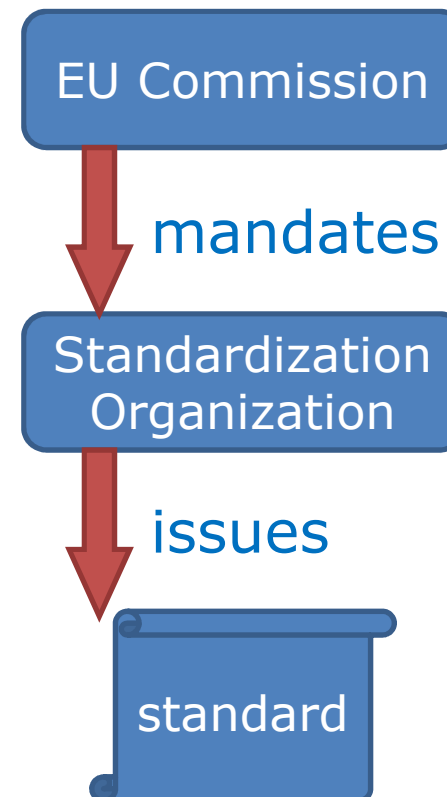
- Hypothesis: Regulation could be performed by **standards**. Because...
- ...standards have legal *effects*,
 - ...standards can fill blank spaces and gaps of laws and
 - ...standards can diffuse across borders.

Regulative Options and Interrelations

Functional view on regulation: All regimes that constrain (or enable) action options are regulation

- Statutory law / hard law (legislation, court verdicts, EU regulations, ...)
- Self-regulation
- Multi-stakeholder regulation

Top down approach
(„New Approach“)

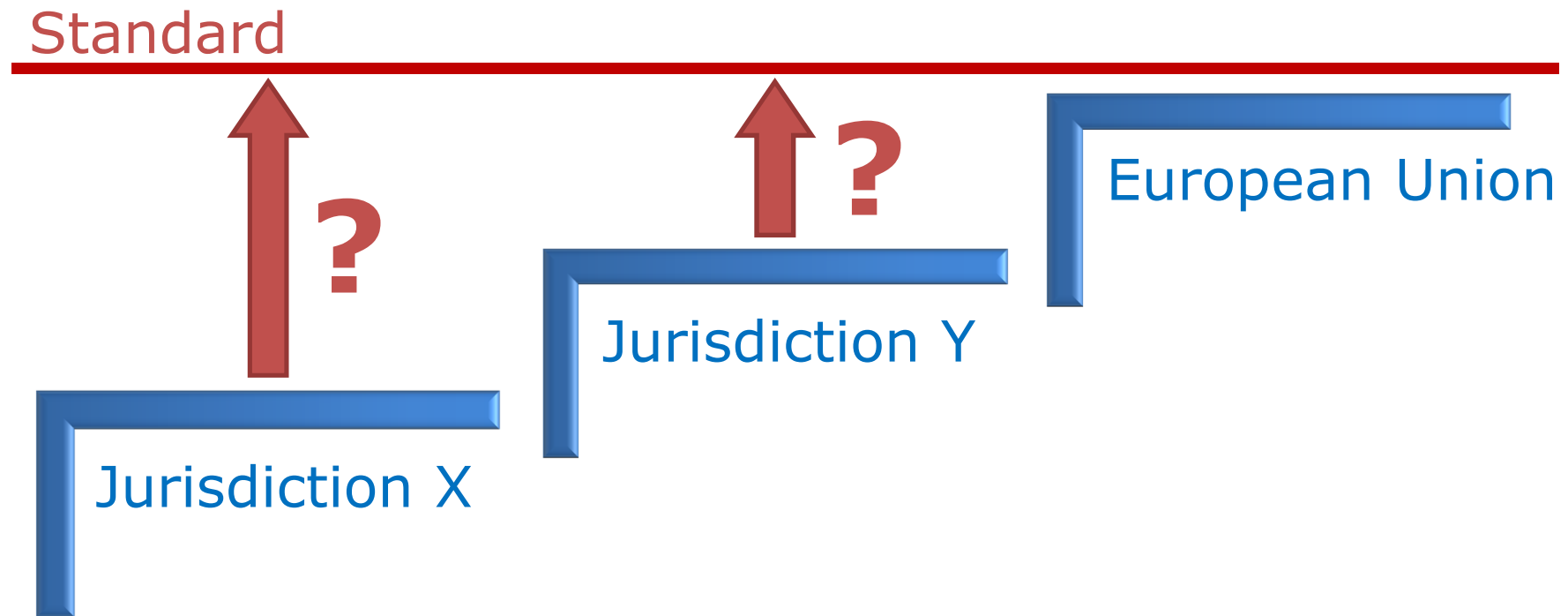


The Genesis of ISO/IEC 27018

- Industry seeks legal compliance of cloud services
- EU legal system on data protection is governed by 95/46/EC (data protection directive).
- All EU member states have to implement it.
- Article 17 contains a vague legal concept:
 - compliance problems!
 - liability risks!
- Assessment of the legal situation in the EU and its member states.

Potential Effects and the Regulative Landscape

- Possible international alignment of legal rules around the standard (which reflects a comparatively high level of protection)



Conclusion & Future Research

- Comprehensive approach
 - Influence **of** legal regulation / legal link
 - Potential for harmonization.
 - Influence **on** legal regulation.
-
- Case studies in social media: How is ISO/IEC 27018 applied? What are the actual effects?

References

- [1] “Kontradiev wave” in Wikipedia, https://en.wikipedia.org/wiki/Kondratiev_wave, 2015.
- [2] Šmihula, Daniel: “The waves of the technological innovations of the modern age and the present crisis as the end of the wave of the informational technological revolution.” *Studia politica Slovaca* (Bratislava) 2009 (1): 32–47.
- [3] Westin, Alan F., “Privacy and freedom,” Atheneum, New York, 1967.

Picture credits

- [2]
 - https://commons.wikimedia.org/wiki/File:Kondratieff_Wave.svg, by "Rursus", CC BY-SA 3.0
 - <https://pixabay.com/de/%C3%B6l-bohrer-rig-erd%C3%B6l-kraftstoff-29956/>
 - https://commons.wikimedia.org/wiki/File:DARPA_Big_Data.jpg
- [4]
 - Own work based on © www.rainerkurzeder.com
- [5]
 - https://commons.wikimedia.org/wiki/File:Cloud_computing_icon.svg, by 百樂兔, CC BY-SA 3.0
 - <https://pixabay.com/de/vorh%C3%A4ngeschloss-gold-sperre-147913/>
- [8]
 - Own work
- [9]
 - Own work
- [10]
 - Own work