Cloud Investigations by European Data Protection Authorities: An Empirical View

Dr Asma Vranaki

Post-Doctoral Researcher in Cloud Computing
Centre for Commercial Law Studies
Queen Mary, University of London

Cloud Computing: The Basics

Definition:

Delivery of computing resources (e.g. data storage, communication, and networking) as a service through a network (e.g. the internet) on a scalable and on-demand basis.

- ✓ Different Deployment Models (e.g. private, community, public clouds)
- ✓ Different Business Models (e.g. IaaS, SaaS, PaaS)

Cloud Computing in Europe

- Increasing Uptake of Cloud Computing in Europe

'Cloud Computing Could Contribute up to €250 Billion to EU GDP in 2020 and 3.8 Million Jobs,'

Bradshaw C et al, Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake, (IDC Research Report, July 2012)

Cloud Computing, Data Protection, Investigations by EU DPAs

- Data Protection Issues in the Cloud

E.g.

- Who is the 'data controller' in cases where > 1 CP involved in providing a service?

- Security Concerns (E.g. Hacking of LinkedIn in July 2012 with 6.5 million user passwords leaked)

- Increasing number of multinational Cloud Providers investigated by EU Data Protection Authorities ('EU DPAs')

Focussing on Cloud Investigations by EU DPAs

Main Lines of Enquiry: How and Why Cloud Investigations are being deployed as Regulatory Tools by EU DPAs?

Conceptual approach:

- ✓ Avoid a 'tools-only' perspective when analysing Cloud Investigations (Baldwin et al, 2012);
- ✓ Focus on the complex and dynamic ways in which multiple actors interact with each other and regulatory tools in practice (Raab and De Hert, 2008) (Murray, 2008);
- ✓ Do not analyse Cloud Investigations as flowing from one direction only (e.g. EU DPA to CP) or in normative terms only (e.g. doctrinal analysis of DPA powers) (Carey, 2007) (Kloza & Moscibroda, 2014);
- ✓ Here empirical focus is how Cloud Investigations are formed and performed in practice.

Methods

- Qualitative socio-legal research project
- Documentary analysis (e.g. DPD, data protection laws of relevant jurisdictions, GDPR, relevant press releases, published Cloud Investigation reports etc)
- 14 qualitative interviews:
  - ✓ 7 DPAs;
  - ✓ 4 Multinational Cloud Providers; and
  - ✓ 2 EU institutions.

Queen Mary University of London
Centre for Commercial Law Studies

Argument(1a): Cloud Investigations as Complex Regulation

E.g. Involve different co-operative relationships between distinct actors (e.g. DPAs, finance police)

- Co-operation between DPAs to ensure effective enforcement and application of shared DP principles
- Regulatory capacities: duty to co-operate between DPAs enshrined in applicable laws and conventions [e.g. Article 28(6) DPD]
- How are these collaborative relationships enacted in practice?
  - ✓ Meetings of the Technology Sub-Group ('TSG') of the A29 WP (4 out of 6 EU DPA respondents);
  - ✓ Information exchange during TSG about past/current CI;
  - ✓ Decision-making: CI at national or EU level? and
  - ✓ where an EU DPA considers itself the lead DPA for the European activities of a CP, TSG operates as a platform through which other EU DPAs can raise their national data protection concerns about this CP.

' …DPA E …oversee[s] them [the Cloud Providers] rigorously and in a way which takes into account the legitimate interests of other…regulators particularly in the EU.' (Interview 1)

'[The Lead DPA] often becomes …a proxy everybody [other EU DPAs] ha[ve] to go through… '
(Interview 3)

Queen Mary University of London
Centre for Commercial Law Studies

Argument(1b): Cloud Investigations as Complex Regulation

- ✓ **Facilitative instruments**
  - E.g. MoU governing specific collaborative tasks (including cross-border joint enforcement)
- ✓ **Multiple practices**
  - E.g. Discussions and deliberations by DPA to overcome to some extent distinct world views (e.g. political, legal etc) so that they can work in concert by focussing on shared data protection principles, common goals, similar regulatory powers.
  - Where not feasible, acknowledge specific differences and agree on specific strategies to manage them (e.g. work from common principles during the CI up to the stage where the final investigation report is drafted).
  - Discuss efficient allocation of tasks during Cloud Investigation (e.g. technical testing vs communication) by balancing several factors such as expertise pool, prior contacts with the CP, available resources etc.

'…you can use the analogy of football where you don't want everyone on the team all running to the ball at the same place or following the ball around the field. There is efficiency to be realised in identifying and playing positions. It can change for different investigations…' (Interview 15)

Queen Mary University of London
Centre for Commercial Law Studies

Argument (2a): Cloud Investigations as Dynamic Regulation

Continually Evolving Regulatory Styles:

- Current regulation literature: regulatory styles as escalating from soft to more coercive strategies as the regulatee persists in non-complying (Ayres and Braithwaite, 1992).
- Empirical data: regulatory strategies not deployed in a linear direction (i.e. from soft to hard) but rather dynamically (from soft to hard to soft again).
- Cloud Provider is not seen as a static actor (i.e. recalcitrant, incompetent or otherwise) but a dynamic one whose compliance profile changes during different stages of the CI
- E.g. Before the CI is formally triggered, most EU DPAs use soft strategies (e.g. explain, understand, persuade).

Queen Mary University of London
Centre for Commercial Law Studies

Argument (2b): Cloud Investigations as Dynamic Regulation

- If the CP becomes recalcitrant during CI (e.g. refuse to accept the recommendations of the DPA or refuse to propose a reasonable alternative) then the DPA can adopt harder strategies to generate compliance (e.g. economic strategies – inability to sell product in the jurisdiction unless specific data transfer guarantees are provided or more coercive legal strategies - e.g. threat of stronger enforcement action)

- If Cloud Provider responds then EU DPA usually de-escalates its regulatory style (e.g. soft again)

Conclusions

1. Cloud Investigations are complex regulatory processes:
   - ✓ Involves various co-operative relationships between multiple actors (e.g. DPAs, financial police) which are enacted through manifold interactions and practices (e.g. facilitative instruments, discussions, deliberations etc); and
   - ✓ Can manifest itself through other factors (e.g. budgetary constraints and pressures from stakeholders such as the press and NGOs). How such complexities are resolved during Cloud Investigations can often involve intricate and context-specific strategies, such as delegating action to a third-party.

2. Cloud Investigations are dynamic regulatory processes which involve constantly evolving regulatory styles, compliance attitudes. This means that the regulatory encounters between Cloud Providers and EU DPAs during an investigation often involve ceaseless change.

3. Cloud Investigations can, at times, be contested as EU DPAs and Cloud Providers attempt to resist each other in particular ways.

Queen Mary University of London
Centre for Commercial Law Studies

If you wish to read more about this!

Vranaki A, 'Cloud Investigations by European Data Protection Authorities: An Empirical View,' in Rothschild J (ed*) The Handbook of Electronic Commerce Law* (Elgar Publishing Forthcoming**)**

@Cyber_Panda_