

Florence 11 July 2019

Comparing the EU and COE approach to big data

Professor Paul De Hert

Vrije Universiteit Brussels – University of Tilburg

Big data...

Big Data is an umbrella term for technological and societal developments that are already taking place (use of profiles, algorithms, cloud computing, machine learning, commodification of data, open access to governmental data, datafication, securitization and risk society).

Distinction big data collection & big data analytics
Is big data still big?

intriguing

- I heard somewhere following chronology
- 1995-2010: internet society
- 2010-2017 big data society
- 2017-future: algorithm society

What about Big Data in legal texts?

European data protection law, governed within the EU by the General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive, and within the Council of Europe by the 1981 Data Protection Convention and COE+.

While skimming through these basic texts, one is amazed by the lack of explicit consideration of the big data phenomenon.

Europe, to respond to the emergence of big data, has deployed two complementary strategies:


- Counting on the vitality of the existing principles to frame a new development and thus continuing a principle-abiding approach in reform times (while allowing some small changes) (*first strategy*)
- regulatory reform to enable big data developments based on a thorough re-evaluation of the regulatory principles (*second strategy*)

Europe, to respond to the emergence of big data, has deployed two complementary strategies

Both approaches co-exist, but due to a politics of scale strategy, they are kept separate: the first approach was followed in the classic realm of data protection law, the second approach pursued by other than the classical actors (for instance, other 'DG's' or departments within the EU). We will discuss six recent legal initiatives voted at the European level designed to facilitate the adoption of big data practices

Strategy 1: principle-abiding approach in reform times (while allowing some small changes)


- = the GDPR
- The Article 29 Working Party ((WP29) - was at the forefront in this campaign. In the crucial reform years of 2013 and 2014, it released a number of policy documents on Big Data, arguing several things at once: Big Data is nothing new, so no change is needed; Big Data has not achieved the promised results in terms of economy, security or science; even when Big Data delivers this does not mean that Europe with its fundamental right approach has to lower the protection of privacy given by the data protection framework and future developments *might* require innovative thinking on how some of the key data protection principles are applied in practice. The following quote gives a flavour of the general campaign:

- 
- “The Working Party acknowledges that the challenges of Big Data might require innovative thinking on how some of these and other key data protection principles are applied in practice. However, at this stage, it has no reason to believe that the EU data protection principles, as they are currently enshrined in Directive 95/46/EC, are no longer valid and appropriate for the development of Big Data, subject to further improvements to make them more effective in practice. It also needs to be clear that the rules and principles are applicable to all processing operations, starting with collection in order to ensure a high level of data protection”.
 - WP29, Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, Adopted on 16 September 2014, p. 2

This campaign against making Big Data an explicit regulatory target was overall successful.

only minor, but not unimportant Big Data-friendly amendments. We count at least four Big Data facilitators.

- 1. the general flexibility in the Directive 95/46/EC with respect to further processing of personal data for historical, scientific and statistical purposes is maintained and enhanced in the GDPR
- 2 recital propose a reasonable test to determine what personal data is. GDPR, Recital 26: ... To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

- 
- 3. Article 6(4) GDPR where criteria are given to assess the compatibility of the secondary use, including the flexible criterion of 'the existence of appropriate safeguards', understood equally as a soft enabling provision of Big Data practices.
 - 4. Role of 'consent' and 'necessary for the performance of a contract to which the data subject is party. Article 6.1.(a) and (b)

Strategy 2 (choose your battlefield) Seven examples

Example 1: The 2016 Law Enforcement Directive

Has important flexibilities with regard purpose limitation, sensitive data and with regard to data subject rights. All friendly towards big data policing

Some of the policy makers around the table were fully aware of police interest in big data mechanisms and small, but important deviations in the 2016 Data Protection Law Enforcement Directive as compared to the GDPR, together with regulatory silence on big data relevant processing practices (web crawling, data mining, data matching, etc.) indicate little data protection-resilience to the phenomenon.

Example 2 The European Commission Communication on a data-driven economy and Directive (EU)2019/770 (on Digital Content)

; The European Commission presented an updated version of its vision on the data economy in its 2014 *Communication on a data-driven economy*. The text presents data protection as an important tool to build consumer trust, but also announced that after the adoption of the GDPR and other EU reform text, the Commission would work on guidance concerning big data-related problems like on such as data anonymisation and pseudonymisation, data minimization. On these new battlefields, mostly steered by DG CNECT, data protection is just 'one' of the solvable issues within a wider discussion =EDPS against 1) contract law field and 2) data monetisation but marginalized

The Role of the EDPS

Significant is a Briefing note on the proposal for a Digital Content Directive by the European Parliamentary Research Service.

- The Briefing note is one big loud hurrah
- the many enthusiastic institutional and non-institutional stakeholders
- only one critical voice marginalized at the end of the note: EDPS. A closer look reveals that the objections of the EDPS are substantial

European Parliamentary Research Service, Contracts for the supply of digital content and digital services, *Briefing EU Legislation in Progress*, February 2018, 12p. with a discussion of the European Commission's proposal for a directive regulating the private-law aspects of contracts for the supply of digital content and digital services in the internal market, COM(2015)634

Example 3 Directive (EU)2019/790 (Copyright Directive)

- Well known about its filtering provisions (11 and 13) that might impact fundamental rights
- Article 3, contains an exception for TDM (text and data mining) for the purpose of research, including Big Data.
- This provision was heavily contested by the TDM community, including the academic community, who saw the exception as too narrow (For instance, the League of European Universities (LERU))
- Small alternative ; EP added Article 3(a), allowing Member States and publishers to create further exceptions and to decide whether they would allow TDM beyond research organizations
- = battle between big data and IPRights, almost no involvement of dp community (EDPS only discussed art. 13)

Example 4: Open Data and Directive (EU) 2019/1024 (Re-Use of Public Sector Information) (new PSI directive);

=Responsible DG: CNECT

Idea? the idea that (government) data should be placed in the public domain.

- Directive 2003/98/EC of 17 November 2003 on the re-use of public sector information (PSI Directive) in Jan 19 replaced by new PSI Directive. That Directive intends to address some issues, mentioned in its evaluation report, partly to accommodate Big Data developments. The objectives of this reform are the increase of the supply of high-value public data for re-use, limits to the use of exceptions to the principle of charging the marginal cost, and more real-time access to dynamic data via adequate technical means.

- The new PSI directive acknowledges the existence of the GDPR and the risk of placing personal data in the public domain. The new Directive therefore proposes a primacy principle of data protection stating that any PSI law has to be applied in coherence with data protection law and cannot create exceptions, as the protection of personal data is recognised as a fundamental right. In practice this means that EU member states and PSI re-users must consider the principles and obligations of data protection law when applying or implementing the PSI Directive. However, this does not imply that PSI that contains personal data cannot be opened, it rather demands a thorough assessment under which conditions the opening is lawful. In order to support the opening of PSI while protecting personal data, the PSI directive establishes such an (triple) assessment grid. (For a short discussion, see 'The PSI directive and GDPR' via <https://www.europeandataportal.eu/en/highlights/psi-directive-and-gdpr>).
- What we see is a fine example of using the GDPR as a reference point, while in the same time using specific laws to open up the GDPR protection in the name of big data. Note that the initiative has been thoroughly scrutinized by the EDPS in its Opinion 5/2018 EDPS Opinion on the proposal for a recast of the Public Sector Information (PSI) re-use Directive (11 July 2018). Several of its recommendations were followed in the final draft.

Example 5: Free Flow of Non-Personal Data and Regulation (EU)2018/1807 (Framework for Free Flow)

= DG CNECT

- To incite cross-border data flows across Europe in order to boost the development of artificial intelligence and supercomputers.
- The EDPS complained about the negative definition of non-personal data, which is likely to be very difficult to apply in practice, since the definition of personal data is broad and context-dependent. Moreover, the EDPS argued that the Regulation would automatically create a tension with the GDPR and would result in legal uncertainty as to which legal framework should apply in a given situation

Example 6: Directive (EU)2015/2366 (PSD2 Directive on Payment Services)

:

= DG FISMA

obliges banks to pass on customer account information to other companies, provided that customers explicitly give their consent.

- 'a blind belief in everything that is called innovation and offers freedom of choice' behind the PSD2, but expects that this supposedly consumer-friendly law will ultimately weaken consumers' position towards ICT giants like Google. 'In practice, everyone just clicks 'agree' to be able to continue on a website or app and the grip on our data by tech giants such as Google and Apple will only expand'.
- Sophie in't Veld sees no harm since GDPR still applies but has major concerns with some of the basic data protection requirements in the interplay between the GDPR and the PSD2, such as the choice of the legal basis, the so-called silent party data and the PSD2 notion of explicit consent, which appears to be different from the notion of explicit consent in the GDPR.
- EDBP new actor, new voice?!!! No opinion of EDPS

Example 7: Ethics Guidelines (8 April 2019),

- June 2018, the Commission established a High Level Expert Group on Artificial Intelligence (HLEG), composed of 52 expert representatives from academia, civil society, as well as industry. In its first year of operation, the HLEG issued Ethics Guidelines (8 April 2019),
- focus on developing the principles and requirements of ethical Artificial Intelligence,
- Commission endorsed but called all the ethical principles 'already existing law'

Many possible lessons, for instance about the Role of the EDPS

Attention needs to go to the role of the EDPS.

-has mandate to deliver opinions on everything nearby or far away to data protection at the level of the EU. -via these opinions that some unity will be created or that the possibility will be created to produce unity.

-most of the acts discussed got good scrutiny by this organ.

The newsletter of this EPS and its opinions published on its website allow us to monitor these documents.

-BUT EDPS is not involved in all developments. For example when expert bodies are set up outside data protection realm, for instance, new expert bodies, and these bodies deliver opinions, there is no guaranteed reaction of the EDPS.

Conclusion: EDPS does not control everything happening in this cold or landscape of regulation or can be undersnowed in fora where there are many other stakeholders

Main lesson today

Detailed regulatory approach in GDPR has proven to be insufficient. GDPR was only starting point for further regulation

One can hardly call this process properly coordinated

On the regulatory approach of the EU, - regulatory law rather than coherency law -, see Roger Brownsword, *Law, Technology and Society: Reimagining the Regulatory Environment* (Routledge, 2019) 341. The author nicely explains why experience teaches us that the EU is not keen on integrating novel laws in their context (the coherency approach), but almost always regulates from scratch having only little attention for existing (domestic and European laws).

Lesson not adressed today: big data futre proof GDPR?

Is GDPR big data proof (phantasy papers; sensitive data; goverments use of big data; collective threat ignored?; broad use of consent and privacy contracts; fairness only understood as transparency as opposed to fairness in consumer law)

- Negative view: GDPR is not only ignored, but also intrinsically not futre proof and does not consider risks beyond scope of individual rights
- Optimist view : first better understanding: brakes and a steering wheel will be more effective if we have a speedometer, a roadmap and a compass

= Time will tell and interesting (in the light of COE apparatus) will be the strenght of the EU softlaw system

If we then turn to COE108+

- Convention 108+ follows a similar approach as the GDPR. This (first) strategy - upholding and enriching the principles while opening up to Big Data mechanics

For example, the principle of purpose limitation and permitted further processing are defined in the same way. More importantly, Convention 108+ adds a new Article 10 (Additional obligations), embedding at least four additional data protection concepts potentially open to Big Data processing – the principle of accountability, the data protection/privacy impact assessments, data protection by design and the risk-based approach.

Complemented with guidelines : big data guidelines (2017)

- Principle based approach in basic legal text complemented with soft law texts in this case the guidelines on Big Data (2017) and the recent guidelines on AI (2019),

The central message of the Guidelines on data protection in a world of Big Data is that basic data protection principles and Big Data processing can exist in a symbiosis, if the controllers take the responsibility on their shoulders and at the same time follow the same steps as in the GDPR – data protection should be built in the early stages of the design of the processing; the controller should carry out an initial risk assessment; should follow up with a proper risk management policy and concrete efforts to minimize the risks; and should carry out a privacy impact assessment, if it is likely that the processing will affect the rights and fundamental freedoms of data subjects, etc.

the novelties of the AI Guidelines are:

- Not only a DPIA (as per the GDPR) but a Social and Ethical impact assessment as well needs to be run;
- Controllers should apply technical measures to assist individuals (notification buttons, online consent forms etc)
- Adopt by-design solutions, such as simulations of processing before running on a large scale
- Keep the impact assessment and all other relevant information open on the internet for everyone to see
- Specific guidance to developers and governments !!!!

=In this way the Council adopts more specific solutions for big data than the GDPR and the EU

Lesson not adressed today: is COE108+ big data future proof ?

- Possibility of finding all GDPR weaknesses again: (phantasy papers; sensitive data; governments use of big data; collective threat ignored?; broad use of consent and privacy contracts)
 - Principles more than details can serve as a roadmap and a compass
 - More study needed: but but proportionality check on consent and other grounds for processing! (art. 5,1 COE+108) and perhaps dignity humain bringing us beyond individual rights perspective
-
- Time will tell

literature

- P. De Hert & Juraj Sajfert, 'Regulating Big Data in and out of the data protection policy field: Two scenarios of post-GDPR law-making and the actor perspective', *EDPL*, 2019, vol. 5/3, 338 - 351
- Rhoen, Michiel, *Big Data, Big Risk, Big Power Shifts*. Evaluating the GDPR as an instrument of risk control and power redistribution in the context of big data, Leiden, 2019, 210p.
- A. Mantelero; 'Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework', *Computer Law & Security Review*, Volume 33, Issue 5, 2017, p. 584-602
- A. Mantelero, 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment', *Computer Law & Security Review*, Volume 34, Issue 4, 2018, p. 754-772
- P. De Hert & V. Papakonstantinou, 'The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition', *Computer Law & Security Review*, Volume 30, Issue 6, 2014, p. 633-642

Thank you!