

New Frontiers in Data Rights

Summary

On 6 December 2022, the **Law, Science, Technology and Society (LSTS) Research Group**, within the framework of the '**Articulating Law, Technology, Ethics & Politics: Issues of Enforcement and Jurisdiction of EU Data Protection Law under and beyond the GDPR**' (**ALTEP DP**) research project, organized the workshop entitled '**New Frontiers in Data Rights**'.

This workshop discussed uncertain and contested issues currently surrounding the exercise of data subject rights, and existing tensions between the different actors of data protection.

The workshop comprised two panels. The first session, entitled '**Synchronising data rights: An inevitable approach, or borderline practice?**' was moderated by **Gloria González Fuster** (VUB). Invited speakers were **Alexandra Giannopoulou** (University of Amsterdam - Digital Freedom Fund), **René Mahieu** (VUB), **Liesa Boghaert** (Timelex), and **Benny Rolle** (University of Goettingen).

Alexandra Giannopoulou discussed the potential of collective action as a means of redress against the harms of data-driven technologies, which are often in the hands of powerful actors, generating new risks and harms across the individual, collective, and societal levels. She highlighted the collective dimension of GDPR data rights, including synchronized exercise by multiple individuals vis-à-vis the same data controller, intermediary exercising data rights on behalf of many individual data subjects in front of the same data controller, procedural class action, and collective harm qualification in a complaint. However, the abstract phrasing and wide scope of data subject rights have downsides that push interpretation cost downstream to the parties invoking and accommodating data subject rights.

Giannopoulou concluded by noting the progressive case law addressing more cases related to collective dimensions of GDPR data rights but still lacks procedural clarity.

René Mahieu discussed three cases of collective exercise of data subject rights, highlighting the Schufa case where AlgorithmWatch organized thousands of individuals to send access requests to understand Schufa's credit-scoring algorithm, and the Dexia Bank Nederland case where consumers sent access requests to prove malpractice by the bank. He also mentioned the Saymine.com case, which allows automated right to be forgotten requests, but companies' DPOs questioned their validity.

Mahieu emphasized the role of technology as a "template" in these cases and the need for the right to explanation of automated decision making to function properly. The cases show the importance of collective action to put data protection

issues in the political agenda and build pressure, as well as the need for the right of access to be exercised to prove non-compliance by data controllers.


Liesa Boghaert introduced Rightso, a free online tool developed by Timelex that simplifies the process of generating GDPR requests and responses. The tool was created to address the difficulties and costs associated with addressing data subjects' rights requests, including lack of knowledge, time and practical resources. Rightso allows individuals to easily generate a request and send it to a data controller, who can then generate a tailored response in a few clicks using the tool's questionnaires. The benefits of Rightso include ensuring that requests meet minimum legal requirements and responses cover the entire request, privacy-friendliness, and control remaining with individuals and organizations. Timelex does not monetize the tool, and personal data is encrypted and stored on EU servers.

Benny Rolle referred to his research entitled 'Organized/Large-scale enforcement of compensation claims' with a focus on the situation in Germany. In the light of the art. 82 GDPR, he started by distinguishing between the entitlement to compensation -comprised of the causal link between damage suffered and a data protection law infringement- and enforcing compensation, which includes proving the damage, proving the infringement, and proving causality.

Rolle referred to certain problems related to proof of damage (legal uncertainty, the existence of "severe enough" damage), proof of the infringement (it often requires internal knowledge), and proof of causality (especially for data breaches, which are hard to prove). Given this, the probability of success of individual enforcement is difficult to predict.

Rolle also compared the individual enforcement model with legal tech/specialized law firms' data breach campaigns, in terms of ensuring that consumers receive "full and effective compensation" (as envisaged in rec. 146). In this regard, individual enforcement could enable the data subject to receive "full" compensation but implies litigation risks and stress. As a counterpoint, legal tech/specialized law firms' enforcement can simplify access to justice without litigation risk for data subjects but by providing them with a "not full" compensation (they charge a fee or commission in the case of success). Rolle concluded by welcoming the 'legal tech companies' approach to more effective law enforcement, but he argued that the barriers to individual enforcement of compensation claims need to be lowered as well.

The second session, entitled **Data subject rights & damage claims: What do we (not) know?**, was moderated by **Michalina Nadolna Peeters** (EDPS). Invited speakers were **Tim Walree** (Radboud Universiteit), **Suzanne Vergnolle** (Le Cnam), **Peter Hense** (Spirit Legal).



Tim Walree discussed the challenges of establishing damages claims for data breaches under liability law and the GDPR. While GDPR sets important values, the concept of harm remains abstract and vague, making it difficult to apply liability law to these cases. Walree referred to several court cases, including the EBI (Dutch Court) cases such as Hoge Raad March 15, 2019, ECLI:NL:HR:2019:376, which allows for compensation of immaterial damages resulting from data breaches, and the ABRvS case (1 april 2020, ECLI:NL:RVS:2020:898-901), which emphasizes the need for an autonomous interpretation of damages while respecting the principles of the GDPR. These judgments show that, in principle, concrete harm is required. This is problematic, given that GDPR violations mostly affect abstract/immaterial/intangible interests.

Walree's conclusion related to the Opinion of AG Campos Sánchez-Bordona (in Case C-623/17), where the latter referred to a lack of compensation if there is no harm, on the basis that the GDPR does not allow for punitive damages and in this context the mere loss of control of data in the sense of "informational self-determination" or "having a say over one's own personal data" cannot be a compensable harm. Instead, Walree proposed that loss of control over personal data is a harm in itself, as it undermines the principles of transparency, purpose limitation and confidentiality of processing set out in the GDPR, though he supports the 'de minimis' threshold, meaning that not every breach of the GDPR has to be a loss of control. It must at least be a violation with a certain gravitas. Minor violations should not be compensated, unless this minor violation leads to concrete harm which a data subject can substantiate.

Suzanne Vergnolle focused her speech on the legal remedies available to data subjects against data controllers and processors where harm is caused by their processing. Two types of potential legal claims were distinguished: individual and collective.

Three conditions are governing this legal action: the existence of harm, an infringement of the GDPR, and a causal relationship between the two.

Vergnolle then distinguished this action from the traditional privacy infringement in the French system which allows anyone to go to court for a privacy violation without having to prove harm (the infringement automatically opens a legal claim). On the contrary, for data protection claims, plaintiffs must prove harm. To help plaintiffs, Vergnolle discussed a taxonomy she created of non-material damage resulting from a data protection infringement, that includes emotional damage, exposure damage, tracking damage, and reputational damage. There is no minimum threshold in France for legal action, and the procedure can be targeted to stop the infringement and claim compensation for the harm.

Peter Hense discussed the effectiveness of Data Protection Authorities (DPAs), citing a report from the European Data Protection Board (EDPB) that shows many DPAs consider they lack sufficient resources to perform their missions. He believes that the current situation creates a false sense of security and that infringing data protection has become part of business risk for many companies. Sanctions are

not seen as a deterrent, and effective enforcement can take up to five years. However, Hense is optimistic that damage claims will become the new 'emission claims', and emphasised that global solutions are required to address these issues. He also referenced recent judgments by the EU Court of Justice, which stress the responsibility of data controllers to prevent breaches and comply with GDPR principles.

Finally, Hense posed a thought-provoking question about why compensation should not be obtained in the case of data protection infringements, given that data is the new oil.