

CPDP.ai 2025

Session Reports



Day 3

With thanks to our rapporteurs.

Enjoy the sessions like a podcast—
links can be found in [Recording](#).

Interview with Adele Zeynep Walton on The Human Cost of Our Digital World By Carissa Anderson, 23 May, Avatar.fm

Recording interview runs from 2:38:45 to 3:07:20)

Rapporteur: Ezgi Ercan

Moderator: Carissa Anderson

Panellist 1: Adele Zeynep Walton

Moderator's remarks

Carissa Anderson introduces Adele Zeynep Walton as the author of a new book titled "Logging Off: The Human Cost of Our Digital World". The interview quickly transitions to Adele Zeynep Walton discussing her background and the inspiration behind her book.

Panellists' contributions

The main point of the interview was to discuss Adele Zeynep Walton's book "Logging Off: The Human Cost of Our Digital World", exploring the negative impacts of digital technologies on society. Walton shared her personal journey from experiencing digital exclusion to becoming an online safety activist after losing her sister to online harms. She examined how social media platforms use addictive algorithms that particularly harm young people, especially women, through misogynistic and harmful content. The interview highlighted the importance of platform accountability, intentional digital disconnection, and the need for youth-led movements to challenge Big Tech's current practices. Walton advocated for a more ethical digital landscape that prioritises user safety and mental health over engagement and profit.

Summary of Q&A discussion

A participant asked about balancing professional social media use with the desire to disconnect. Walton acknowledged the challenge, also for her own profession, emphasising the need for gradual change and open conversations about social media's

issues. The interviewer suggested a design feature to hide short-form video content (Reels, YouTube Shorts) to reduce algorithmic distraction. This sparked a brief, collaborative discussion about user disempowerment in platform design. The atmosphere was collaborative and engaged, with participants sharing personal experiences and showing genuine interest in addressing digital technology's challenges. The Q&A section felt like a constructive dialogue between the speaker and audience, united by shared concerns.

DPAs and Certification Systems: How Good Are They as Compliance Instruments?, Friday 23.05, Class Room

Recording

Rapporteur: Ezgi Ercan

Moderator: Ivan Szekely - Central European University/Blinken OSA Archivum - Hungary

Panellist 1: Charles Raab - University of Edinburgh - United Kingdom

Panellist 2: Colin Bennett - University of Victoria - Canada

Panellist 3: Marit Hansen - Privacy Commissioner, Schleswig-Holstein, DE - Germany

Panellist 4: Sébastien Ziegler - Europrivacy - Luxembourg

Moderator's remarks

The moderator opened the panel by introducing the topic of GDPR certification mechanisms, as outlined in Articles 42 and 43. These provisions enable the use of accredited certification schemes to demonstrate compliance by data controllers and processors. The moderator highlighted the potential role of certification and standardisation in supporting data subjects' rights and effective oversight. Emphasis was placed on the importance of the involvement of supervisory authorities and EU institutions in shaping and regulating these schemes. The discussion was framed around key questions, including how certification schemes have developed in the EU, the challenges and opportunities, and the experiences of data protection authorities, data controllers, and certification bodies. The moderator also raised the role of civil society and consumer organisations in these schemes and their potential to enhance trust, transparency, and accountability.

Panellists' contributions

Panellist 1 (Charles Raab) discussed the historical evolution of privacy certification systems over the past 20 years. Raab explained the GDPR's framework for certification

through Articles 42 and 43 and detailed the UK's certification process, highlighting the role of the Information Commissioner's Office (ICO) and UK Accreditation Service. He underlined the complex multi-level infrastructure of certification systems and raised questions about the effectiveness of certification in truly protecting data privacy.

Panellist 2 (Colin Bennett) explained the evolution of privacy impact assessments into the regulatory toolbox. Bennett underlined precision in terminology, warning against interchanging standards and codes, and critiqued pure market incentives, suggesting additional motivators for certification, such as regulatory pressure, reputational management and contractual obligations. He discussed Canadian privacy law reform, noting a potential standards-based approach was never fully implemented due to Data Protection Authorities' scepticism, and highlighted potential risks in certification, including the potential for being locked into narrow legal interpretations and limitations of standards like ISO 27000.

Panellist 3 (Marit Hansen) presented a critical view of data protection certification. Hansen highlighted the limited number of certification schemes (only nine as of 2025) and discussed the challenges of implementing meaningful certification. She explained that certification is not a guarantee of full GDPR compliance and raised concerns about the complexity of certification processes.

Panellist 4 (Sébastien Ziegler) discussed certification from an international perspective. Ziegler explored market incentives for certification and highlighted the potential of certification for reputation management. He noted the challenges of interoperability in certification systems and explained the need for clear guidelines and standards.

Discussion points from programme

The conference programme included four key questions for the panel. These were each addressed as follows.

Question 1: How have certification schemes developed in the EU?

- Speakers outlined the progression from pre-GDPR initiatives, such as national data protection seals, to the current GDPR-aligned certification framework. While the number of approved schemes remains limited (nine as of 2025), the discussion emphasised the foundational infrastructure now in place and the role of ongoing collaboration between national and European authorities. Early adopters and pilot schemes were mentioned having set useful precedents for others.

Question 2: What problems and opportunities have been encountered on the way to certification?

- Challenges such as implementation complexity, market hesitation, and standardisation gaps were acknowledged. However, emphasis was placed

on the benefits of certification, including its value as a visible sign of GDPR compliance, a tool for reputational enhancement, and a driver of organisational transparency. Speakers noted increasing interest from industry stakeholders and ongoing work to simplify the framework.

Question 3: What are the experiences of DPAs, data controllers, and certification bodies in the EU and elsewhere?

- Discussed from the UK and German perspectives. Panellists shared practical insights into the operational aspects of scheme accreditation and supervision. There was recognition of the learning curve for both authorities and certification bodies but also growing alignment on procedures and responsibilities. DPAs were described as key enablers in guiding certification development.

Question 4: What are the views of consumer and civil society organisations on such voluntary schemes?

- While direct representation was limited (no speakers from these organisations), panellists referred to the importance of stakeholder engagement and acknowledged the role of certification in enhancing public trust. Calls were made for stronger involvement of civil society in future discussions.

Summary of Q&A discussion

Q audience: “None of the panellists mentioned AI. Given the lack of DPA resources in the EU, could it be an idea that, when a DPA discovers a violation, they could impose an order requiring certification within two years?”

Response by Marit Hansen: Certification can play a role in such cases, particularly as a signal of compliance with the state of the art. She referenced recent CJEU rulings indicating that no compensation is due if state-of-the-art standards are met, highlighting how liability may be influenced. However, questions remain on enforcement and whether DPAs can or should act as third-party certifiers. Other discussion points included legal challenges around mandating certification, concerns about potential “privacy whitewashing,” and the need for clear, standardised processes. The role of DPAs in both facilitating and supervising certification schemes was emphasised, along with the broader aim of building public trust and accountability. The atmosphere during the Q&A was engaged and reflective, with critical yet constructive contributions from the audience and panellists.



Is My Boss a Bot? The Role of Data Protection in Algorithmic Recruitment and Employment, 23 May, Orangerie

Recording

Rapporteur: Ine van Zeeland (imec-SMIT-VUB / Hasselt University)

Moderator: Declan McDowell-Naylor (Information Commissioner's Office ICO)

Panellist 1: Aislinn Kelly-Lyth (Blackstone Chambers)

Panellist 2: Halefom Abraha (Utrecht University School of Law)

Panellist 3: Lindsey Zuloaga (HireVue; LZ)

Panellists' contributions

Aislinn Kelly-Lyth: We have a lot of substantive law in the EU, e.g. on discrimination and the GDPR. How does that translate into practice? Some key issues for worker surveillance:

- How are individual employees supposed to bring the evidence about employer surveillance to court, e.g. on discrimination?
- Even if employees were able to get the evidence, what are the procedural mechanisms in place for employees to bring their employers to court? *Article 80(2) GDPR allows associations to represent individuals' interests in court, but that hasn't been implemented in many Member States.*

Kelly-Lyth: We need to focus not only on the substance of the law, but also on the procedures to make the law possible in practice.

Lindsey Zuloaga: HireVue is focused on assessing candidates fairly, using a mathematical basis for assessment processes. We use AI in hiring, which means we are scrutinised a lot. Our aim is to present a transparent system. We have done third-party audits, voluntarily. The process of the AI audit is not very well defined yet, even if we have been doing it for 5 years. There just are no clear definitions out there. We have also done an explainability statement, reviewed by the ICO. We are ready for the regulatory discussions because of all the things we have done internally. In the US, there is not much federal guidance around that, but we look to the EU for a lot of that.

Declan McDowell-Naylor: What is your definition of algorithmic hiring?

Kelly-Lyth: It is good to have a broad definition. It should include algorithmic monitoring systems and automated decision-making systems. An expansion of Article 22 GDPR will be needed.

Halefom Abraha: The Platform Workers Directive distinguishes algorithmic management (a delegation of managerial tasks to an algorithm, from hiring to firing and everything in between) from algorithmic monitoring. These types are not mutually exclusive: algorithmic management presupposes algorithmic monitoring.

Zuloaga: When people talk about algorithms, they often mean 'machine learning'. An algorithm may or may not be AI; algorithms can be very simple sets of rules. Simple algorithms can be just as harmful as more advanced machine-learning algorithms. It is important to differentiate that there is a lot of automation (that can be more or less problematic), there can be neural networks (which are mysterious and opaque), so there are different levels of problems associated with different types of algorithms.

Kelly-Lyth: Is (semi-)automating managerial tasks fair? That will be context dependent. If an algorithm is well designed and sensitively deployed, it can well be fairer than traditional management, as human managers and recruiters can be highly unfair and inconsistent. Human bias is a perennial issue as well, and inserting humans in the loop can be a source of bias. But do we want a system to be automated and lose human agency, even if we think it can lead to a fairer outcome? If we say: 'this algorithm is good at identifying a good employee' - what makes an employee good? Fairness and effectiveness must depend on what we compare it to.

Abraha: There is not enough empirical evidence that algorithmic management can deliver on the promise of reduced unfairness and improved neutrality. I don't think algorithmic management can be fair by design. If the developers of AI systems are predominantly from a certain age, gender or cultural group, it is possible that disparities can be built into systems inadvertently.

There are fairness issues also at the implementation stage. Whether AI systems can be fair depends on several factors. Do workers understand what is being monitored and do they know the categories that are used for management decisions? If criteria are not disclosed or are unclear to workers, we cannot speak of fairness. Can workers contest decisions and is there a clear procedure for them to verify and challenge decisions? Are work standards reasonable?

Zuloaga: There are a few fundamental fairness definitions, and they cannot all be satisfied with real-world data. This makes it much harder to regulate fairness. In hiring, the concept of adverse impact is well known. "Bias in, bias out" is a point: the quality of data matters a lot.

We do strive for more diversity in our algorithms, most importantly by focusing on what the important characteristics are for the job. Our algorithm is blind to such characteristics as gender or race. In the assessment, we include elements such as a virtual job try-out.

McDowell-Naylor: Do workers need new or different data rights?

Kelly-Lyth: The biggest problem with Article 22 is its vagueness. We have been looking at the automated screening of applicants; does that fall under Article 22 GDPR? Recital 71 GDPR refers to e-recruiting practices, but that is vague as well.

Assuming that we are within the scope of Article 22, we very quickly end up looking at the exceptions. This contains more difficult and vague questions on whether algorithmic assessment is necessary. When an employer receives thousands of applications, more than they can humanly process, would it then be necessary to use an algorithm?

We need particularisation of specific types of algorithmic decision-making that is always prohibited, such as automated firing. The Platform Workers Directive has in Article 10 a requirement of worker involvement in evaluating algorithms in use. There is also the requirement for human review, in Article 11.

Do workers need different data rights? Not necessarily in the context of automated decision-making, but we need rights at the collective level. We need participatory oversight, which is a way in which collective rights can be realised. Another great point of the Platform Workers Directive is that representatives that do evaluations can ask for expert support (if necessary, e.g. for complicated systems). Transparency is needed: data are only really valuable when aggregated. Employees can only hold their employers to account when they have collective access and transparency.

Abraha: Article 22 GDPR is the most relevant and important protection we have so far, because the Platform Workers Directive is not relevant in all work environments. It provides a set of individual rights (the right to contest a decision and the right to an explanation, for example). But all these rights depend on transparency and the contestability of the system.

Article 22 GDPR protections and safeguards are subject to layers of exceptions and caveats that eventually weaken the protections. It applies only to "significant decisions", which is not always clear - various insignificant decisions taken together can have significant results.

The nature of the relationship of employment is not the same as the one between data subject and data controller. It is a relationship of power, fundamentally different than the power dynamics in data controller-data subject relationships. As consumers, we have the freedom to choose the type of product we want. Workers do not have such freedom, that is a different power balance. Moreover, if you delegate an employment decision to an algorithmic system, it depersonalises that decision.

Labour law prioritises collective solutions and is aimed at standardised solutions at collective level. The underlying principle is to rectify power problems. Most, if not all labour laws predate algorithmic systems, so they do not include data protection concerns. Because of the centrality of data in algorithmic decision-making, data protection is an important regulatory response to the risks created by new technologies. However, the way data protection laws are designed is not appropriate for the workplace. Data subjects are seen as a kind of consumer or user. The employment relationship is treated in the same way as the relationship we have with an app.

Discussion points from programme

Questions on the programme:

- Can algorithmic management of workers be effective and fair?
- Is Article 22 GDPR sufficient to protect workers from unfair AI-driven employment practices?
- What does AI explainability mean in the workplace?
- Do workers need new or different data rights?

Summary of Q&A discussion

Question from a student in the audience: Finding a job in the Netherlands is becoming more difficult because of applicant screening systems and nobody knows how it works. As an applicant you must jump through so many hoops and people are trying to game the system with tricks like white text on white background. Most candidates do not think that data are processed fairly.

Zuloaga: This problem has been around for a while. It is tough for candidates because of the volume issue, not so much the automation of the AI. AI may or may not have been used. It is not fun for a candidate to apply for loads of jobs and never hear anything back. A lot of employers are still using bad algorithms. If you use keywords to analyse applications, that does not tell you much. It is an easy way to filter people but does not tell you anything about fitness for the job.

Abraha: I think this is an issue of explainability. People do not know why they do not get hired. If the employer cannot explain or justify AI decision-making, this is a legal problem. Such systems should not be used in the first place.

Kelly-Lyth: We have not mentioned the AI Act yet. The technical documentation that needs to be provided by developers to deployers can help with that. Then there is still Article 22 GDPR that requires an explanation. If you cannot provide that, you should not be allowed to use the system.

Question: Can it ever be fair to use a hiring algorithm that makes decisions based on criteria that were not mentioned in the job advert?

Zuloaga: I haven't heard anyone discuss that as a set of criteria. Job adverts are often horribly phrased. People usually write job descriptions, but do it even match the actual job, and does it include all the requirements?

Abraha: The problem with AI is that it is supposed to solve the implicit bias problem of humans. But if we do not know which criteria the AI uses to evaluate applicants, that is a problem. We need a clear explanation of how each criterion influences the outcome.

Question: How to calibrate standards on the role of humans in hiring decisions?

Abraha: In the work context, the Platform Workers Directive requires four levels of transparency for different actors.

Zuloaga: Human review introduces human biases. Live interviews are a huge problem, e.g. they are often unstructured.

GDPR and Collective Redress

23 May, Grande Halle

Recording

Rapporteur: Liubomir Nikiforov, BPH

Moderator: Jennifer Baker, Freelancer

Panellist 1: Max Schrems, noyb

Panellist 2: Sean O'Sullivan, Barrister

Panellist 3: Ianika Tzankova, Tilburg University / Rubicon Impact & Litigation

Panellist 4: Charles Demoulin, Deminor

Moderator's remarks

Moderator Jennifer Baker opened the session by noting that, although the EU Collective Redress Directive is now transposed in most Member States and several courts have begun recognising non-material damages for GDPR breaches, a “wave” of privacy class actions has not materialised. She framed the panel around three questions printed in the CPDP programme: *What is coming in the next few years? Will GDPR enforcement shift from Data Protection Authorities (DPAs) to the courts? What is holding back litigation so far?* Baker underlined that the discussion would blend activist, academic, practitioner, and litigation funding perspectives and asked the speakers to remain practical, focusing on real obstacles and realistic timelines rather than hypothetical scenarios.

Panellists' contributions

One theme unified the panel: collective redress privacy actions are coming, albeit more slowly and unevenly than predicted. Each speaker explained that trend and offered a distinct point on what must change for mass GDPR claims to become routine.

Max Schrems

Max Schrems sketched the activist strategist view. Years of *noyb* complaints have convinced him that representative suits are “inevitable but slowburn” because the prerequisite architecture, qualified entities, clear standing rules and workable damage metrics, was only finalised in 2024. He expects an initial wave of injunction only filings over the next 18 months, followed by a second, damages-oriented wave once the Court of Justice clarifies that even modest ‘loss of control’ harm meets Article 82. Schrems sees courts not as rivals to DPAs but as “pressure valves” that can step in when regulators stall, provided Member States adopt harmonised opt-out and disclosure rules to prevent forum shopping.

Sean O’Sullivan

Sean O’Sullivan offered the barrister’s lens from Ireland, where most tech giants are incorporated. The Representative Actions Act 2023, he noted, creates a skeleton mechanism but leaves certification tests, cost allocation and contingency fee caps hazy. Combined with Ireland’s high bar for proving “serious and credible” non-material damage, these gaps deter plaintiff firms. O’Sullivan nonetheless predicts test cases within two years — likely piggybacking on landmark Data Protection Commission (DPC) infringement decisions to shortcut liability proof — because any Irish judgment against a Big Tech defendant will ripple across Europe.

Ianika Tzankova

Ianika Tzankova presented the academic practitioner perspective from the Netherlands, which already hosts several privacy class actions under the WAMCA (Dutch Act on Representative Actions) regime. She credits Dutch momentum to three ingredients: opt-out design, permissive funding rules and courts seasoned by competition and securities mass claims. Yet even in Amsterdam, she warned, quantifying aggregate moral damages and orchestrating cross-border claimant pools remains difficult. Tzankova called for an EU level specialised chamber — analogous to the Amsterdam Court of Appeal for securities cases, to centralise complex privacy disputes and streamline settlement approval.

Charles Demoulin

Charles Demoulin spoke for the litigation funding community. Capital is available, he said, but funders impose tough metrics: clear liability (preferably via a DPA finding), a claimant pool above 100 000, and per capita damages of at least €50–100. Until European courts award more than token sums for non-material harm, many privacy cases are “economically underwater.” Demoulin forecasts hybrid models in which ESG-minded investors partner with NGOs to derisk claims and broaden the case pipeline once damage jurisprudence solidifies.

Together the contributions painted a realistic but cautious roadmap: the legal tools now exist, funding is circling, and the first decisive CJEU ruling on moral damages could tip collective privacy enforcement from theory into mainstream practice.

Discussion points from programme

What is coming up the next years?

A measured but unmistakable expansion of representative GDPR claims. In the near term (2025-26) most filings will target injunctive relief — cookie-banner and dark-pattern cases, unlawful ad-tech tracking, and data-scraping for AI training — because injunctions require no individual damage calculus and are attractive to funders testing a new forum. Mid-term (2027-28) a “damages wave” is expected once (i) the CJEU clarifies non-material harm thresholds, (ii) two or three landmark settlements prove monetary upside, and (iii) more qualified entities complete the 12-month eligibility period. The speakers highlighted Ireland (Big-Tech HQs, high publicity), Netherlands (opt-out + WAMCA familiarity), Austria (consumer-protection pedigree) and Germany (Bundesverband model) as early laboratories. A longer-range trend is the bundling of privacy harms with competition or consumer-product claims, creating mixed “omnibus” actions that deliver economies of scale for litigation funders.

Will GDPR enforcement move from DPAs to the Courts?

Complementarity, not substitution. Collective actions act as “pressure valves” when DPAs are back-logged, politically inhibited, or limited to administrative fines. Injunctions can stop ongoing processing much faster than the GDPR cooperation/consistency mechanism, and civil courts can award compensation that DPAs cannot. Yet private suits often rely on DPA findings as quasi-estoppel to establish liability, and funders treat a final decision from a lead authority as de-risking “gold.” Several panellists predicted closer procedural choreography — e.g., Dutch courts awaiting AP decisions, or Irish High Court adopting DPC factual records — rather than an outright hand-off of responsibility.

What is holding back litigation so far?

Obstacles fall into four clusters: (i) Procedural fragmentation: 27 versions of opt-in/opt-out, certification, disclosure, and cost shifting; claimants must engage in forum shopping, which itself raises fairness concerns. (ii) Economic friction: Loser-pays exposure, caps on contingency fees, and damage awards that still hover at €50–€200 per person, often below funders’ break-even point. (iii) Standing & organisational hurdles: Few qualified entities exist; the Directive’s 12-month activity rule and governance requirements slow newcomers. (iv) Evidentiary & cultural barriers: Courts still grapple with quantifying non-material harm, and European corporate culture defaults to “fine-then-comply,” reducing voluntary settlement incentives. Speakers agreed that

incremental solutions — harmonised minimum procedural safeguards, calibrated cost-shifting, and a clearer CJEU doctrine on moral damages — would unlock a “tipping point” rather than a sudden U.S.-style class-action surge.

Summary of Q&A discussion

Question 1: University of Maryland: Does reliance on well-resourced NGOs create selection bias and leave small national breaches unnoticed?

Max Schrems: Bias is possible, but any qualified entity may file once funding matures; collective suits are not limited to big-ticket cases.

Ianika Tzankova: More national entities will appear as economics improve, widening the case mix.

Sean O’Sullivan: DPAs remain the back-stop for purely local or low-value infringements.

Question 2: Can collective actions recognise societal harm rather than just individual loss?

Ianika Tzankova: Courts should allow aggregate moral-harm models; digital infringements are inherently collective.

Max Schrems: Expects forthcoming CJEU case-law to endorse uniform “token” awards (low three-digit euros) across the class.

Question 3: Are Binding Corporate Rules an effective shield against collective-redress claims?

Sean O’Sullivan: No. BCRs sit parallel to litigation; once an infringement is alleged and certified, BCRs offer little protection.

Question 4: Which DPAs are most supportive of collective-action work?

Charles Demoulin: Attitudes vary: some DPAs welcome private enforcement as workload relief; others fear loss of relevance. Courts in the Netherlands and Austria currently cooperate most smoothly with claimants.

Question 5: Private-international-law scholar (audience): Is forum shopping a problem or a feature?

Ianika Tzankova: It is a feature; claimants should, like corporations, choose the venue that maximises efficiency. Harmonised rules could curb purely tactical manoeuvres.

Question 6 NGO lawyer: Do you expect the CJEU to set a uniform minimum for moral damages?

Max Schrems: Yes: Case C-300/21 and an upcoming Article 82 referral signal that 'loss of control' alone can justify modest per-capita awards.

Question 7 Insurance counsel: How can defendants estimate exposure when claimants hail from 27 jurisdictions?

Ianika Tzankova: A tiered damages matrix (residence X data sensitivity) plus a single settlement fund overseen by one court can manage exposure.

Question 8 Start-up DPO: Won't mass actions bankrupt SMEs?

Sean O'Sullivan: Funding economics favour systemic, high-volume breaches; SMEs typically face individual claims or DPA fines, not EU-wide class actions.

Question 9 Academician: Could platform discovery become more like U.S. practice?

Charles Demoulin: Unlikely; expect targeted disclosure orders under regimes such as the Dutch WAMCA or the forthcoming reforms in Germany.