CPDP 2026

SINCE 2007 COMPUTERS, PRIVACY AND DATA PROTECTION 19TH INTERNATIONAL CONFERENCE

COMPETING VISIONS

SHARED FUTURES

CPDP 2026

Conference Partners

Ada Lovelace Institute

ADAPT Engaging Content Engaging People

European Commission

AI-REGULATION.COM

ALTI

FGV DIREITO RIO

CRISP CENTRE FOR RESEARCH INTO INFORMATION, SURVEILLANCE & PRIVACY

CEU Universidad San Pablo

eLAW LEIDEN

FIZ Karlsruhe Leibniz Institute for Information Infrastructure

Fraunhofer ISI

Georgia Tech College of Computing School of Cybersecurity and Privacy

Inria

ivir Instituut voor Informatierecht Institute for Information Law

KU LEUVEN CiTiP CENTRE FOR IT & IP LAW

dg Università di Torino Dipartimento di Giurisprudenza

MAX PLANCK INSTITUTE FOR SECURITY AND PRIVACY

Politecnico di Torino 1859

Washington University in St. Louis THE CORDELL INSTITUTE

Tilt Tilburg Institute for Law, Technology, and Society

UCL

uni.lu Université du Luxembourg

Utrecht University

DATA SCHOOL

VUB

Dear Friends of CPDP,

The world is moving fast, and in many directions at once. Hyper-datafication, shifting geopolitical alignments, and evolving regulatory landscapes are reshaping how we live, work, and govern. In such a moment, a space where our community can come together to think carefully together, is more necessary than ever. That is what CPDP has always tried to be, and what it remains today.

Organising CPDP in a fragmented world is challenging. Diverse, sometimes competing visions of digital governance are taking shape, reflecting different traditions, values, and political settlements. The desire, in such a world, may be to retreat into like-minded communities, to mistake agreement for progress. CPDP resists that tendency. What we strive for is not consensus, but constructive encounter. The value of bringing academics, lawyers, policymakers, civil society, and industry into the same place lies precisely in the friction. Competing visions, well articulated and seriously engaged, are a democratic resource.

For the data protection community, 2026 brings these tensions into particularly sharp focus. Ten years since the adoption of the GDPR, our work is far from done. This anniversary invites reflection on what has been achieved, what remains difficult, and what needs to change. Debates around “simplification” and the pressure to ease regulatory burdens in the name of competitiveness and innovation are part of that conversation, and they require serious engagement from all sides. What is beyond dispute is that the questions our community has been addressing at CPDP are growing more pressing, not less. Datafication touches every domain of life: from the design of public services to the future of the next generations to the conduct of war. The datafication of conflict is no longer a metaphor but a strategic and humanitarian reality. The exceptional programme of CPDP 2026 reflects a conviction that they are not technical compliance matters but live questions about power, dignity, and what kind of society we are building.

This year’s CPDP artwork, commissioned with renowned artist Simon Denny, offers a visual counterpart to these themes. Drawing on Italian Futurist imagery alongside contemporary venture capital branding and defence-tech aesthetics, it shows how competing ideas of progress are never fully separate but entangled, in tension, and drawing on a shared visual language across time. The coin or medallion-form reinforces this: value and futurity are continually negotiated through recurring historical motifs. The work echoes CPDP’s own premise: that shared futures are constantly being formed through the friction of competing visions.

True to its tradition, CPDP brings these conversations into the open. Across disciplines, sectors, and borders. We are glad you are here.

Paul De Hert

Thierry Vandenbussche

Jonas Breuer

Barbara Lazarotto

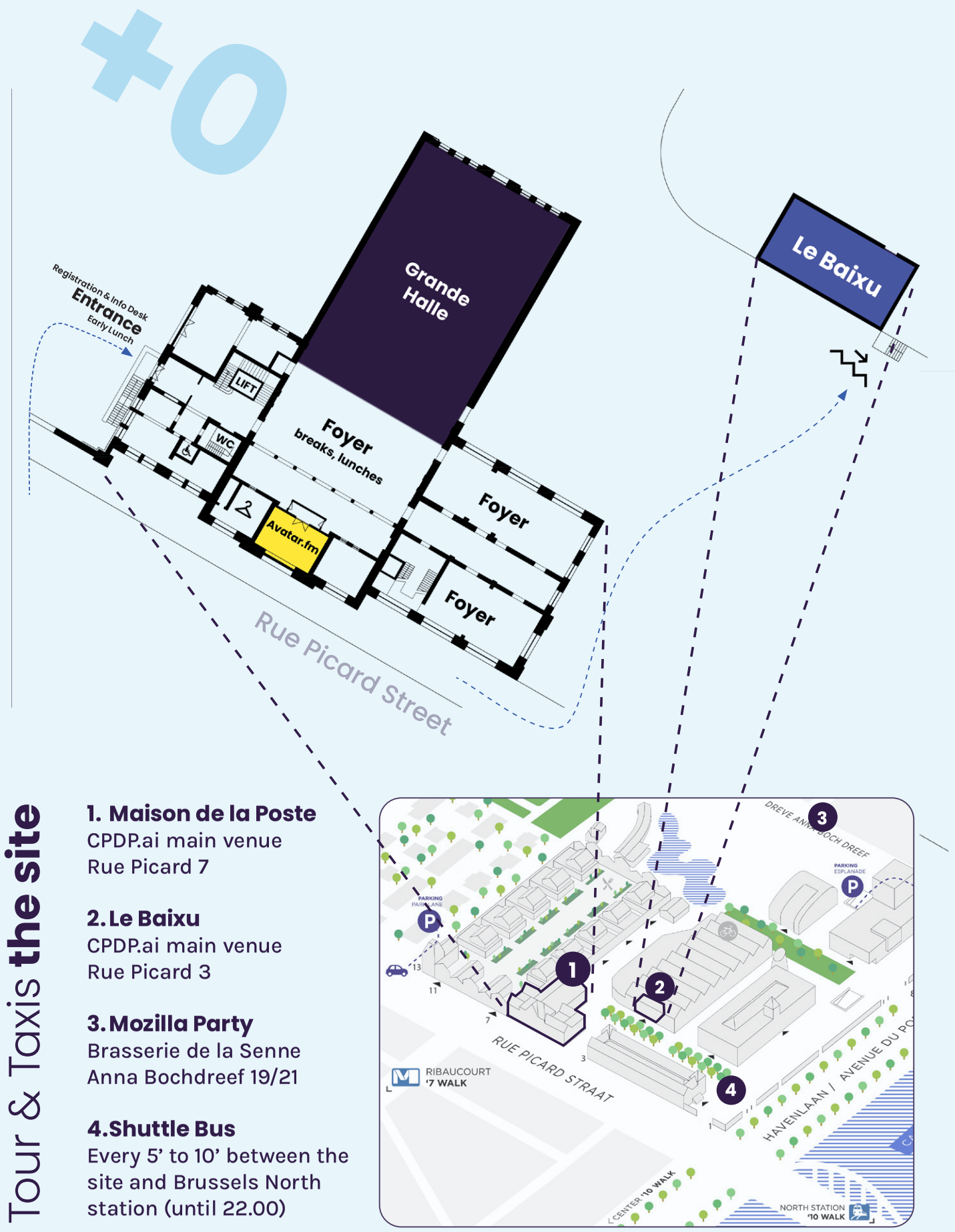
Tour & Taxis **the site**

1. Maison de la Poste
CPDP.ai main venue
Rue Picard 7

2. Le Baixu
CPDP.ai main venue
Rue Picard 3

3. Mozilla Party
Brasserie de la Senne
Anna Bochdreef 19/21

4. Shuttle Bus
Every 5' to 10' between the site and Brussels North station (until 22.00)



- **Panels**
- **Workshops**
- **Culture Club**
- **Avatar.fm (CPDP's live radio)**
- **Coworking**

General Congress Information

Registration and Name Badge

Registration opens on Tuesday 19 May at 4 pm in front of Maison de la Poste, inside Gare Maritime. From Wednesday 20 May to Friday 22 May, registration opens from 7.30 am. You will receive a name badge with the dates of attendance.

Information Desk

We provide general information about the conference and about Brussels at the registration desk outside Maison de la Poste in Gare Maritime.

CPDP 2026 introduces Print on demand

To support sustainability, this year, the CPDP programme – which is completely available online - will also be fully print-on-demand. You can print it at home, at your hotel, and you can even create a personalised version with the sessions and tracks you plan to attend during the conference. On-site printing with digital payment will also be available.

Venues

CPDP takes place simultaneously in two venues at Brussels' Tour & Taxis site. Most sessions will be held at the main venue: Maison de la Poste. Here, Grande Halle is located on the ground floor. The Maritime room is on level 1 and the Class Room and Orangerie are on level 2. All the Panels are organised at Maison de la Poste, as is the CPDP Culture Club, which can be found in the Cinema Room on level 3. Some workshops and the academic sessions take place in the revamped jazz bar Le Baixu, a stone's throw from Maison de la Poste. You can find an overview of all venue locations by consulting the map in the CPDP Magazine.

Lunch and Coffee Breaks

All lunches and coffee breaks will be held in the foyers at Maison de la Poste and in Gare Maritime. The early lunch will start at 12.30 pm outside Maison de la Poste in Gare Maritime. Regular lunch starts at 1.05 pm in the foyers.

Networking and Side Events

Cocktails will take place in Maison de la Poste starting around 6.40 pm on Wednesday, Thursday and Friday, with the Mozilla Party once again happening on Thursday evening. Don't forget to check out our exciting Culture Club Programme on the 3rd floor and the Avatar.fm live radio on the ground floor.

Video Recording and Photography at CPDP

Is CPDP watching you? Well... a bit. A professional photographer will be taking photos at the conference, including crowd shots, which may then be used for publicity. Please let us know during registration if you do not wish to be in these photographs. Panels will be filmed at the conference venue and uploaded to our archive and YouTube channel after the event (in case the speakers gave consent for the recording).

Shuttle Bus from/to Brussels North Station

A free shuttle service travels back and forth from Brussels North Station. Every 8 to 15 minutes, a bus leaves at the Tour & Taxis site or the station. Around midday, buses also go to the Rogierplein. Find the schedule by scanning the QR code.

Taxi

Please do not ask the information desk to call a taxi for you, kindly do this yourself. Why? Taxi companies like to know your name and phone number to avoid other people getting into the taxi that you booked. Taxis Verts: +32 2 349 4949. UBER and BOLT are also available.

Updates and Conference News

Please keep a close eye on email updates from us throughout the conference and contact the registration and information desks if you have questions. Our wonderful volunteers will be at the venue to help you find your way.

Photo © Nick Ash

Interview with

Simon Denny

Each year, we invite a leading contemporary artist to shape the visual identity of our upcoming edition, creating a distinctive black-and-white image - often a drawing or graphic work - that reflects the spirit of the program. This tradition has brought us the privilege of collaborating with a remarkable group of artists. Last edition, we had the honour of working with James Bridle, and in 2024 we commissioned work from Vladan Joler. Previous collaborations include Adam Harvey (2019), Scottish artist David Shrigley (2020, Particles of Truth), Romanian artist Taietzel Ticalos (2022, I'm Sorry), and Austrian artist Judith Fegerl (2023, Resistors).

This year, we are especially proud to be working with Simon Denny, an internationally renowned artist whose work critically engages with technology, power, and global systems. Given the relevance and influence of his practice, we felt it was essential to sit down with him for a conversation—both to reflect on his contribution to this year's identity and to gain deeper insight into the ideas that inform his work.

For two decades, CPDP has been bringing policy makers, academics, civil society and industry together around themes of digital governance. How do you position your work within such a field, where high level knowledge on legal or technical matters reign?

Very much as an artist, haha. I am interested by policy debates, academic discourse, conversations in various contexts around industry and society etc, even digital governance – but my output is always as an artist. I have a lot of respect for people working in these domains, but they're not mine. I see the strength of the artist position as one that can produce things that kind of transmit how things feel. When debates about new configurations hit these other domains, I think art can add value by sort of prompting an object, image or whatever to resonate with the vibe of what is going on in these domains, as they settle in wider worlds. It's great to be informed and I find the creative challenge of seeing what's being talked about in policy, academia etc and imagining how that might hit cultural norms as they are in the world as forever interesting and a good problem to focus on as an artist.

The theme (Competing Visions Shared Futures) emphasises that conflicting models do not disappear or don't eliminate each other, per se, but together shape the future. Do you look at your work as making these conflicts visible? Or do you try to take the viewer further, deeper or beyond the theme/topic of your work?

That model of how worlds are formed – different, possibly contradictory, forces acting at once – is one I find compelling. It resonates with ways that I approach making exhibitions. I feel that what I do functions best when competing narratives that are being championed by various actors are sort of refracted through the artwork. But it's important that the exhibitions I end up making don't behave as explainers for these forces. I am often hesitant to take a single position on the material I respond to. I see my artworks acting as propositions – prompting us to consider emergent things as if they were already further embedded in culture. Tactile, visual and structural aspects of what I make – like, the craft of the objects, narratives, timing and exhibition experiences that carry this through are the vehicle that does this. It's not about presenting information. At its best, the artwork should hit on a visceral level. It should feel resonant with emergent cultural signals as they're becoming perceptible.

When we first started talking about the possible connections between your work and CPDP, we bumped into Cory Doctorow's talk at Chaos Computer Congress '25 titled *A post-American, enshittification-resistant internet*. More specifically his proposal of countering Trump's tariff-bullying – as Doctorow calls it – with repealing the anti-circumvention law. This would allow EU-based technologists, companies, and hackers to modify, repair, or create interoperable tools for US-made tech products. Do you agree that this would be a strategic play for the EU, or is Cory Doctorow missing any important nuances?

With all the caveats I mention above about my knowledge level and role as an artist etc. – I do love this proposal. It feels clever, literate, strategic and simple, but it also opens the door to lots of creative opportunity for individuals or groups to find agency where they are. I think I particularly relate to the idea of opening-up things for doing versions and tweaks because that's an important part of my artistic process. I very often start with an existing object, image or narrative and then tweak and build it anew, with differences. Adapting and augmenting things is so productive for me. I also feel like this is just the way things really

I feel that what I do functions best when competing narratives that are being championed by various actors are sort of refracted through the artwork.

happen – any innovation in any domain starts with digesting the existing system and then sort of checking its adaptability to the contexts one acts oneself in. This is how things move, how new things are formed. I made an exhibition in 2017 in Shenzhen that started from speaking to various actors involved in that special hardware entrepreneurship ecosystem that existed and exists there. The official stories the state was telling seemed aligned with the experience of so many individual entrepreneurs who were making this or that product – from DJI drones beginning their near industry hegemony to smaller decentralized innovations like Karaoke speaker/mikes. There was this assumption there that innovation was too fast for copyright or patent law, that by the time the legal system got to challenging whatever infringement, then it would already be too late because the market would have acted. There was more at work than just these ideas, of course – but I saw the value of what ignoring or circumventing adaptation protections there was doing. Doctrow's proposition that the leverage the US used to keep this digital protection racket up has been wasted now Trump has deployed his tariffs seems also possible. I think for me it's just clear that the ability to tweak and build on existing things is exciting and is a wonderfully positive thing to advocate for.

Your design for CPDP '26, being a clear reference to the rebranding of a16z, identifies and makes parallels between Italian Futurism of the past, and contemporary political developments. It highlights the revival within Silicon Valley venture capital, of the futurist dream of machinic speed, aerial traversal, and war. What does this tell us about the interlinked relationship between the military-industrial complex and aesthetics today?

This whole nexus of things fascinated me in the last few years – the fact that images published by top US Defense Tech companies like Anduril resemble so strongly the *Aeropittura* Futurusim of the 1920s-40s from Mussolini's Italy, and that influential VCs like Marc Andreessen are explicitly quoting Marinetti Futurist manifestos as inspiration for their own "American Dynamism". Given a position like mine, there's a lot to work with here. When we first started talking about logos responding to CPDP's idea of "Competing Visions Shared Futures", I immediately thought of the strange cultural refraction of investors reviving these kinds of narratives and aesthetics, that obviously originated in Europe adjacent to these enormous wartime moments, and have their own sort of story here of being remembered – even celebrated. A 2002 issue 20 cent Europe coin features Boccioni's poetically titled *Unique Forms of Continuity in Space* (1913) sculpture of a figure transformed through "lines of force" purposefully moving forward. Boccioni was killed while training to go to war – and was, as most of the Futurists were, extremely hopeful of what the Great War could bring. That the Metropolitan Museum of Art in New York has foregrounded this work over many decades as part of the building blocks of Modernism in their collection is also interesting, given this context. And a16z – the influential Venture Capital company co-founded by Marc Andreessen – rebranding itself with a sort of neo-Art Deco (although strangely postmodern, though I am sure that's not what its association is supposed to evoke) Futurist-ish relief, continued to give me material to work with. Their new logo reads as a kind of epic coin render, featuring a *moderne*-looking helmeted, classically robed figure holding a glowing orb and an abacus. I'm working on a diptych that starts with these two Futurist-inspired emblems of value. The fact that the dominant ends of the US technology and political spectrum are so adversarial towards Europe, yet kind of recycle culture that has its inception here feels paradoxical. Anyway, for CPDP I started prompting various US commercial AI models with mixes of this and a binary "choose your pathway" meme, and other iterations of these motifs and found the outputs pretty interesting. I felt somehow the shadow of American venture capital looms large in Europe (even our most supposedly autonomous weapons sector). Founders Fund and Sequoia have strong investments in Stark and Quantum systems.

The fact that the dominant ends of the US technology and political spectrum are so adversarial towards Europe, yet kind of recycle culture that has its inception here feels paradoxical.

Even Helsing, which is considered to be more EU-first, accepts venture capital from US firms. I thought the strange back and forth between Italian Futurism, sovereignty debates, the changing meaning of US capital and influence in Europe and vice versa was all kind of condensed in this strange coin form. My version for CPDP has two figures – sort of splitting the a16z figure into dissonant others. They're multiple and looking in different directions. They have some of the geometric *lines of force* that inform the Boccioni, and a kind of image sharding that is typical of some futurist work that attempted to capture movement – but its also kind of fake. The remnants of "slop" are there – which I would argue is also true in the original a16z branding. It also carries over some of the conventions of EU coinage. Is it a coin, a logo or a medallion? What are the resonances of the power of voices like Andreesen's doing in this context? I felt it hits on a number of problems that preoccupy my thinking that also seem like they're a focus for the CPDP community.

Your work *Secret Power (2015)* engaged directly with the visual and political fallout of the Snowden revelations. Yet in the decade since, the landscape has shifted considerably. The Wikileaks era was defined by the idea that radical transparency could expose state crimes and force accountability. Today, despite an abundance of evidence, often gathered by journalists risking their lives, impunity persists. The challenge seems less about exposing crimes and more about making them actionable within legal or political systems. How do you imagine the "Wikileaks spirit" and the role of technology evolving in this context?

Secret Power | Installation view at the Biblioteca Marciana, 56th Venice Biennale | 2015 | photo: Jens Ziehe | courtesy of the artist

Well, WikiLeaks is a complicated thing, right? Which is sort of how I felt at the time when the Snowden leaks became known, making my work for the 2015 Venice Pavillion for Aotearoa/New Zealand. In that project I responded to Snowden's leaks by finding the online profiles of an artist that publicly claimed he was the NSA Defense Intelligence's Creative Director and connected leaked NSA graphics with the work he self-published on social media. All this was presented in a historic Library in Venice, the Marciana, that is decorated in curiously similar imagery from the height of their empire moment by masters of the Renaissance. That project feels from today's vantage point like it's all about mistrust, disinformation, incomplete information and the ability of various actors to ignore norms and laws– governments, Snowden and Wikileaks, me as an artist – and whom that benefits. I think in the case of the actions of Wikileaks, it's clear that their disclosures in the medium term benefited adversaries of the US

Forces of the Unknown | Installation view at J W Marriott hotel, Berlin | June 2025 | photo: Nick Ash | courtesy of the artist and Kraupa Tuskany Zeidler, Berlin/Munich

like Russia, and sort of sowed the seeds of the institutional doubt that would be essential to the rise of figures like Trump in the following years. With my exhibition, I think the artwork involved quite an aggressive power play from my side – using the NSA artist David Darchicourt's work when I knew it put him, and my hosts the New Zealand Arts Council and to some degree the NSA, into a strange cascade of odd power stalemates. I interpreted his work without permission and concurrently surreptitiously commissioned new work for my pavilion from him. Everything I represented by Darchicourt was available online, through his own website – but it was intended for other contexts. Putting it in this context, presenting his work implicitly as "New Zealand culture", was a strange position to put the pavilion in. It highlighted uncomfortable adjacencies and overlaps with the power structure that governs New Zealand's sovereignty internationally (especially their security debt to the US). In short, I was unsure at the time of just how hopeful the "Wikileaks Spirit" was in the end – when really it could be seen as building the rails for the mistrust that became a clear vulnerability for global liberalism, to be exploited. I think my project also – in that it mis-used social media by weaponizing the disclosure that Darchicourt presented on his Linked-In and Adobe social accounts – anticipated something that's abundantly clear now about the operational nature of social media. There's analysis now like those by Daniël de Zeeuw & Sal Hagen that point to the idea that social media systems are adversarial by design – using Targets, Triggers and Tracking, for example as key metrics, which are all derived from the military. These pillars of design go towards shifting culture and sociality, and eventually the nature of information to that register as we all act downstream from those protocols. Working on that my Venice project definitely felt like that. I don't know if that answers your question, or where indeed we go from here but these are the things that resonated with me.

If CPDP focuses on democratic resilience through a plurality of perspectives, what role can art play that does not seek consensus but produces friction? And how do exhibitions offer another way to understand digital systems, beyond what governments and policies say?

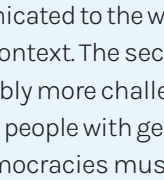
Great questions. I think the second one connects with what I mentioned in your first question about my activity and position, how I see my role. I think in general culture broadly, exhibitions – for those that go to them – are great for somehow reflecting how stuff feels. If you walk into an exhibition, and you're captured there by whatever the artist's craft is, and it engages you and resonates somehow with how the world feels: that's what art can do. And I think exhibitions are strong today in part because they exist in a particular social and contextual space. They're situated. You're in them. They're in a city at a particular moment and then never again. Even if you're texting or whatever while visiting exhibitions, you're there, local. When the Post-Internet art conversation started to happen – where the essential difference with Net-Artists the decade before us was that we were keen on making objects and integrating more with the workings of the mainstream art world. Artists described under that term were making exhibitions that addressed the cultural changes that were happening as digital systems further permeated and changed norms beyond the digital – in ways like what I mentioned above with the adversarial turn in communications media and how sociality is formed through socials.

Regarding the question about what role art can play for a value system that wants democratic resilience and plurality – I think art, and culture in general – is just such a good barometer for how things are, how people feel. These signals are important for feeling a public. I think in the US, to some degree, during the last election cycle, the Democrats seemed to speak to whom they wanted the constituency to be, not who that constituency really was. It was idealized. It felt to me as if they spoke to a world as they hoped it was – which is in some ways admirable but ultimately not effective. I think the world contains frictions, things that are uncomfortable and unresolved – and I think that culture that doesn't reflect that will feel propagandistic. I think work that contains friction has the power of feeling closer to the experiences of life. One doesn't need all artwork or culture to occupy this register, but I think equally one doesn't want a world that only privileges culture that reflects one worldview's ideals. This is part of what being plural – or valuing plurality – means to me. Even if more uncomfortable or even possibly harmful elements are rendered visible, have voice and resonate with some.

If we truly speak of "shared futures," who is systematically excluded from shaping that future today, what blind spot do you see in current debates on digital governance that both policymakers and academics overlook, and, on a more personal note, has your research made you more optimistic or pessimistic about the direction in which digital societies are evolving?

Systemic exclusion has been well documented by many scholars in the past decade. I learned a lot from thinkers like Kate Crawford or Wendy Chun, for example, who's work showed a lot about where AI was extrapolating from in terms of knowledge, culture and assumed subjects and how limited those pools were that they were generalizing into digital protocols addressing the world. We know that it's hard not to embed those kinds of exclusions in technology and social systems – but its good that those things, thanks to these thinkers and others, are known to many as part of what building systems mean. I also don't really have an overview of debates on digital governance in policy and the academy, really. I'm sure there's a lot going on that I don't know about and I assume (and hope?) the conversation is broad. I think from my perspective, the possible blind spots that I see in academic and policy contexts in Europe, particularly on the liberal side of things, are maybe two things. The first is an assumption that good, reasoned, well thought out debate will triumph in the end over incoherent vibes-based, affective messaging (which is demonstratively not true). I don't think that voids the value of reasoned debate and empirical research etc, – it just maybe challenges assumptions about how the findings of such things in policy and the academy are communicated to the wider public outside of the institutional context. The second is about numbers, and I think possibly more challenging. I think a liberal assumption that people with generally progressive values in social democracies must be somehow in the majority might not be the case at this moment. I think my question would be what if that's *not* the case – that this value set is one held by minority. I think a Bernays/Lipmann era US elite – to keep the analogy there – did not assume this, and strategised about what produced a liberal subject. I think a lot of people now would be uncomfortable claiming that kind of role, which opens up a lot of opportunities for the more illiberal world which is definitely not uncomfortable in this role.

And I would say that on the optimism/pessimism scale I am like pessimistic towards the macro, but optimistic in my everyday interface. We must meet the day as if it's possible to do things that we agree with, and live in a way that's aligned with our values. It could be that we're entering a macro where that is not dominant, where larger systems run counter to those values. But one can keep moving with those values to act with at a more local, immediate scale – the people in our immediate lives. ▪



One doesn't need all artwork or culture to occupy this register, but I think equally one doesn't want a world that only privileges culture that reflects one worldview's ideals.

Molly vs the Machines: Why Social Media Must Change

OPINION PIECE

Watching the documentary *Molly vs the Machines* is a shock to the system. It tells the story of Molly Russell, a young girl navigating a digital world designed to connect, entertain, and inspire—but too often shaped by platforms that are addictive, exploitative, and unsafe. While deeply personal, her story reflects a wider reality: social media engineered to capture attention at any cost, leaving children's wellbeing as an afterthought.

The film raises a question resonating around the world: how have social media platforms been allowed to evade accountability while systematically failing to protect children online? Across Europe, the UK, and the wider digital world, young users are exposed daily to products designed to maximise engagement, push harmful content, and generate profit. This is not accidental. Addictive feeds, algorithmic amplification, and exploitative advertising are deliberate design choices. Platforms are shaping childhood itself, embedding risks that families, teachers, and children struggle to manage.

Recent legal developments in the United States underscore the danger. In New Mexico, Meta was ordered to pay $375 million after a jury found the company deliberately exposed children to harm, misled users about safety, and failed to prevent abuse. In Los Angeles, another jury found Meta and YouTube liable for designing platforms that contributed to addictive use and mental health harms, explicitly citing "malice, oppression, or fraud." These verdicts confirm what the film dramatizes: harm is built into the product. Platforms are engineered to exploit young people.

For too long, debates about social media safety have focused narrowly on content moderation—what children see. The U.S. verdicts shift attention to product design and corporate accountability. Infinite scroll, autoplay, and recommendation algorithms are not neutral features; they are choices made with full knowledge of the harm they cause.

In every other area of childhood, products cannot reach children until they are proven safe. Toys, medicines, food—if these caused comparable harm, they would be withdrawn or redesigned. Social media can and must do better. Platforms must be held accountable and demonstrate they are safe for young users.

Awareness of these risks has grown. Many parents feel alarmed by what social media platforms are doing to children, yet much of today's debate remains stuck in a false binary: ban social media or not. This framing benefits tech companies by diverting attention from the business models and design features that generate harm.

We believe what is needed is a structural reset: a "licence to operate" model. Platforms would be required to demonstrate safety by design—removing addictive features, limiting harmful algorithmic amplification, and ideally, enabling interoperability so users can move their networks. Only those meeting these standards would operate responsibly. If harm is designed in, it can—and must—be designed out.

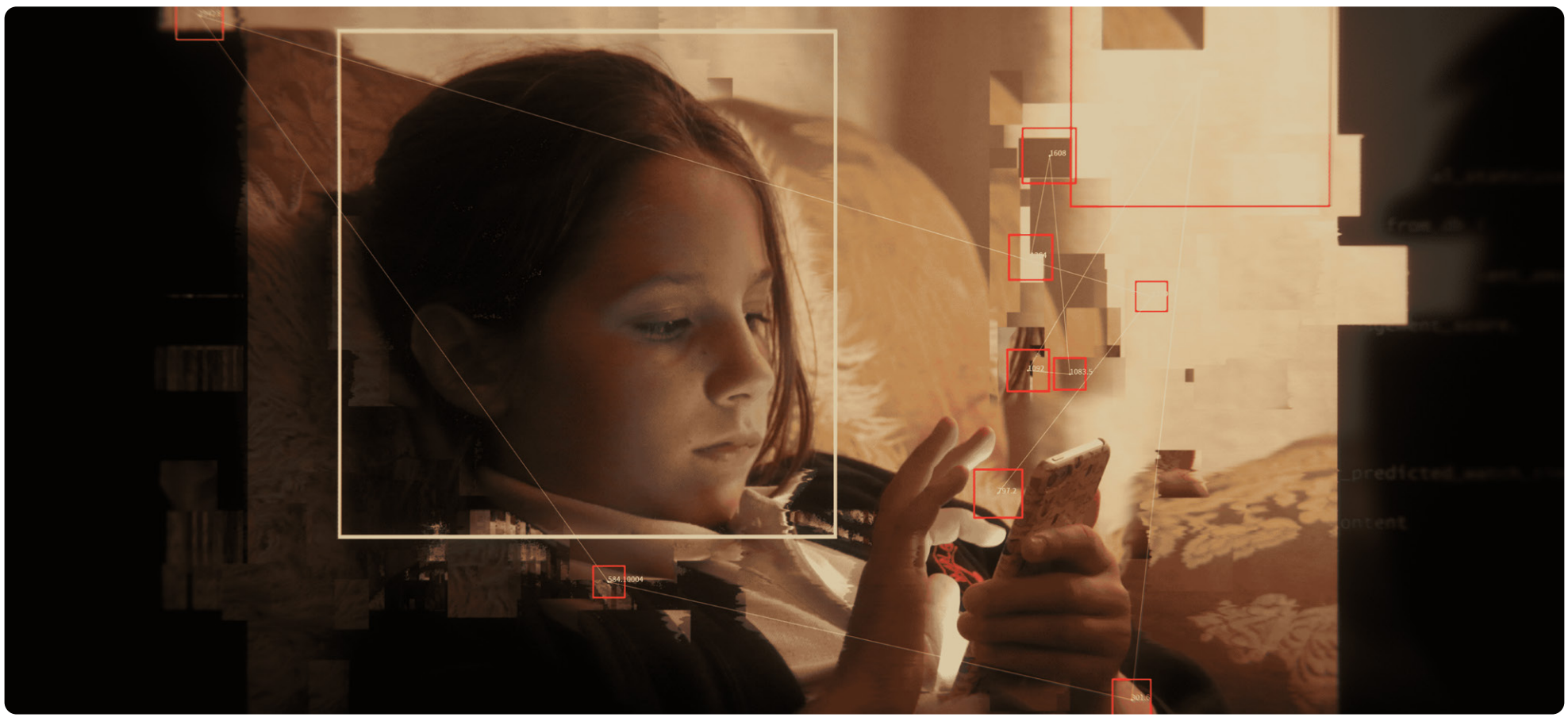
Europe is already pointing the way forward. The Digital Services Act represents a major shift from voluntary self-regulation to enforceable accountability, requiring the largest platforms to assess systemic risks, limit harmful design, and protect children. On paper, it is a breakthrough. But recent evidence presented at a European Parliament hearing shows a persistent gap between what platforms claim they do to keep young users safe and what young people actually experience.

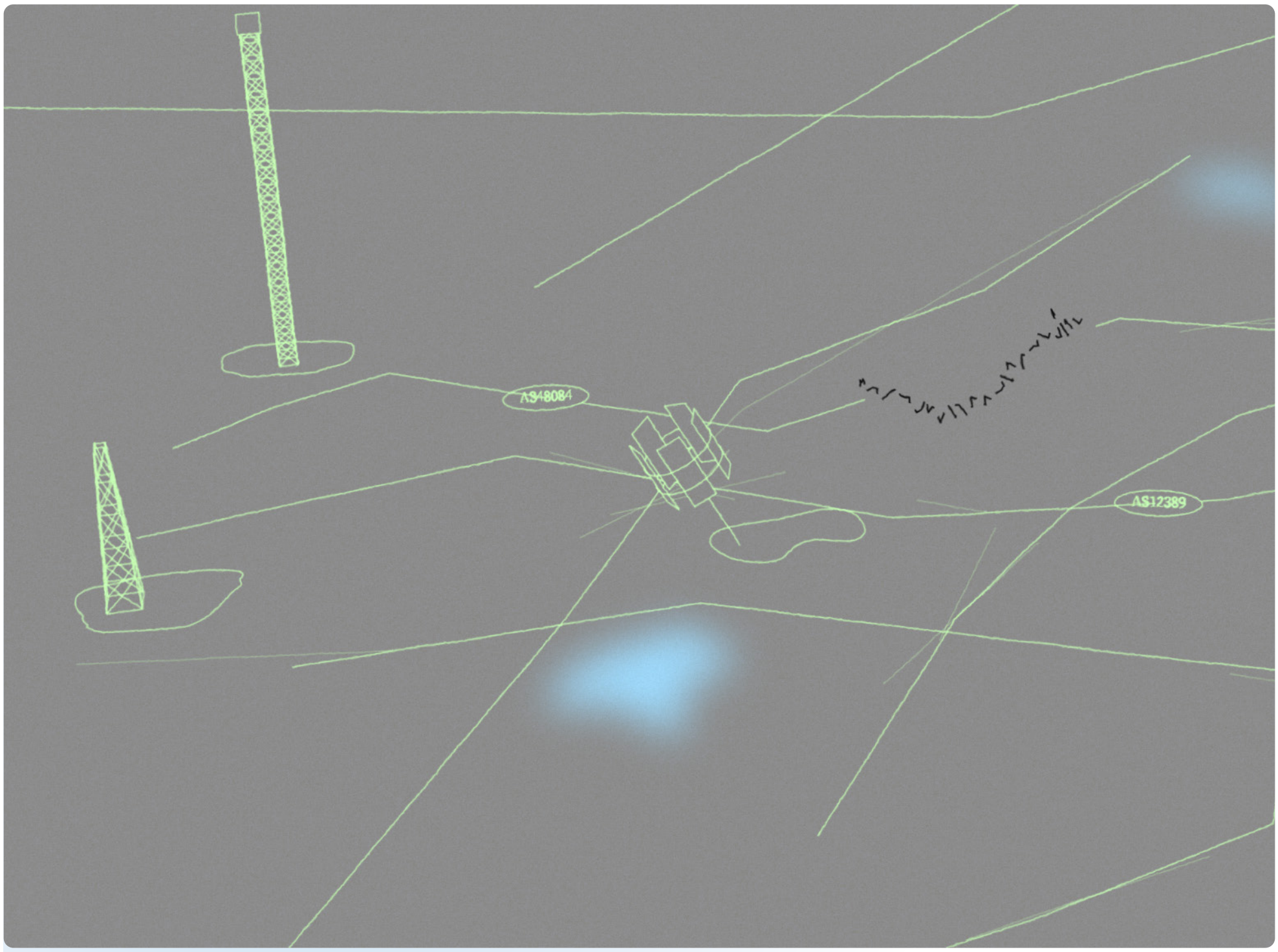
Crucially, this does not undermine the DSA—it underlines its importance. The law provides the tools to act, and there is growing political consensus that enforcement must now go further, confronting the business model itself and requiring real "safety by design." With the European Commission signalling stronger action ahead, including new rules on addictive features, the DSA should be seen not as the end point, but as the foundation for a more ambitious approach.

People vs Big Tech is hosting a screening of *Molly vs the Machines* at the CPDP Conference on Wednesday 20 May, alongside award-winning filmmaker Marc Silver. Bringing the film into this space—where policymakers, regulators, academics, and civil society convene—creates a vital opportunity to connect lived experience with policy action. It is a chance to reflect on Molly's story, confront the urgent need for systemic reform, and build momentum for making digital platforms safer for children.

The experiences of Molly—and millions of young people—show that the current model is failing. The question is no longer whether platforms should change, but whether regulators will require them to do so. Will governments enforce meaningful accountability and systemic reform, or allow harmful-by-design systems to operate without consequence?

Nienke Palstra - Campaigns and Policy Director, People vs Big Tech





Courtesy of the artist

Flickering in the infinite loop of machine-human mimicry

OPINION PIECE

(after "On Being Emotional Infrastructure")

fantastic little splash is a collective comprised of journalist/artist Lera Malchenko and artist/director Oleksandr Hants. fantastic little splash combines art practice and media studies to research collective imagination and emotions appropriation in technosocial systems.

"Modern war is a cyborg orgy," stated Donna Haraway, adding, "The main trouble with cyborgs, of course, is that they are the illegitimate offspring of militarism and patriarchal capitalism, not to mention state socialism[1]." Her cyborg is a figure for the collapse of stable boundaries between organism, machine, and system. And these days, happily or not, all the dangerous possibilities still need the political work she also insisted on in 1985.

1 A Cyborg Manifesto, Donna Haraway, 1985

In our essay "On Being Emotional Infrastructure,"[2] we tried to describe and trace specific trajectories not only of these transgressed boundaries, but also of attempts to militarise them. It sews together academic views, premonitions, and subjective interpretations, technical and legal data, and art sketches in order to reveal the mechanism of transforming emotions into infrastructures for cyberwar propagation. It was also an attempt to map Russia's tactics and techniques involving the occupation of ordinary citizens' imaginations to reinforce its control in areas that it cannot destroy, erase, or capture physically, during its physical occupation of Ukrainian Kherson in 2022.

Cyberwar is known not only as a matter of cyberattacks on networks or the circulation of information threats as propagandistic content. It also works through the patterned activation of human reactivity. Preferences, vulnerabilities, and social pain points[3] are identified to segment audiences, and propose "relief", often in the form of protest, physical damage, or even a terroristic attack. Cyberwar moves through these infrastructures by shortening the time between human impulse and digital transmission.

The ultimate goal of this militarised marketing funnel[4] is physical occupation. The occupation of Ukrainian Kherson in 2022 by the Russian army made this especially visible. Once military control is established, internet traffic is rerouted, mobile operators replaced, media ecosystems seized, movement monitored, and institutions absorbed into the extrastatcraft administrative grid. Emotional infrastructures do not disappear at that point. They are rebuilt to maintain fear, hopelessness, and the sense that there is no alternative[5]. Direct repression and affective management begin to work together.

Physical occupation, however, is not always the immediate goal. Emotional infrastructures can sustain remote influence for years, keeping populations susceptible to later activation, as is happening now in the EU. These infrastructures can be activated from election to election to polarise societies and radicalise regular democratic processes. In a way, we are talking about the occupation of the collective imagination, which potentially enables physical occupation.

Many of these techniques were first refined in commercial environments rather than military ones. For instance, an emotional contagion experiment conducted by Meta in 2014[6], where participants weren't aware they were participating. Digital platforms learned to trace, provoke, and monetise emotional intensity – to generate engagement – to generate value. Emotional contagion, behavioural profiling, algorithmic targeting, and audience segmentation were systematised within platform capitalism as methods for keeping users reactive and measurable. And then Russian Foreign Information Manipulation and Interference campaigns (FIMI)[7] show how easily these commercial architectures can be reused for geopolitical and military use. What was built to capture attention can also be used to occupy perception.

In the essay, we have also tried to document approaches of the Kherson region residents to counteract the infrastructuralisation of feeling structures from within: SIM cards purchased through another person's documents in order to protect volunteers or people-to-people sharing of news got from non-occupied territories. These acts were fragile and local, but they show that emotional infrastructures are never seamless. They can be disrupted by counter-networks of trust, anonymity, and mutual relay.

The same approaches are also troubling us these days beyond the formally occupied territories, including the EU, across both aggressive marketing strategies and FIMI campaigns, all of which reinforce one another in a Möbius-strip dynamic. If you check out a few recent NATO StratCom public reports, you will find that this is indeed the case, as all of them are about cognitive warfare. Cyberwar is expanding, penetrating investment markets and requiring quick automated tech solutions, all of which will be built on our behaviour — or just marketing assumptions about it.

And now we are not just Harraway's cyborgs, we are Lydia H. Liu's Freudian robots[8]. Liu shows that the machine does not merely extend the political body but begins to serve as a model or mirror for structures of subjectivity. Human subjectivity in 2026 is an expanded, hybrid entity that flickers within a continuous loop of mutual imitation between humans and machines. Can you still distinguish your desires from algorithmically generated recommendations? In Liu's view, the threat lies not in the complete disappearance of the subject, but in the fact that technomedia regimes of repetition are increasingly colonising the conditions under which the subject can even recognise itself as non-automatic.

This is not an argument for recovering "human purity without machines." That fantasy is neither possible nor useful. It is a warning: although the machine enters into the production of the subject, it does not yet exhaust it, and we are still capable of distinguishing different modes of agency within the distributed mediated unconscious that is forming right now.

We are still capable of preserving this fragile mode of reflection, responsibility, and self-relation within technical systems. We can still interrupt modes of automated execution that use our feeling experiences as emotional infrastructures [until all of them become indistinguishable statistical truths in the depth of the training datasets].

fantastic little splash
(Lera Malchenko and Oleksandr Hants)

This opinion piece was commissioned by Privacytopia – the artistic programme organised alongside CPDP by the Privacy Salon NGO - as part of its research on Post-Soviet artists working in and reflecting on the digital realm.

2 On Being Emotional Infrastructure, fantastic little splash, 2024,
3 The Lure of War, Lesia Kulchynska, 2025
4 Protest Funnel: How a Marketing Model Helped Organize a Rally in Support of Artem Riabchuk, Lera Malchenko, 2022
5 Terror Environment, Svitlana Matviyenko, 2024
6 Experimental evidence of massive-scale emotional contagion through social networks, Adam D.I.Kramer, Jamie E. Guillory, Jeffrey T. Hancock, 2014
7 Beyond Disinformation - What is FIMI?, EEAS Europa, 2023
8 The Freudian Robot: Digital Media and the Future of the Unconscious, Lydia H. Liu

Interview with

Andrei Zakharov

Andrei Zakharov is an independent investigative journalist and author known for his in-depth reporting on Russia's surveillance infrastructure, including the troll farm operations linked to Yevgeny Prigozhin. For his work, he has been designated a "foreign agent" by the Russian government. In November 2025, he published *The Russian Cyberpunk. How the Kremlin Builds a Digital GULAG — And Who Is Resisting It*, a book that examines the expanding architecture of digital control in Russia and the individuals pushing back against it.

We'd like to talk about Russia's "grey" and "dark" data market, particularly *probiv*, which you discuss in your book. Probiv is a type of cybercrime that appeared in the late 2010s and became popular in Russian-speaking underground forums in the early 2020s. It involves illegal services and Telegram bots that let users search large databases of leaked or illicitly obtained personal information, often used for doxxing, scams, and blackmail. How does probiv differ from a typical data leak?

We all know that personal data leaks are everywhere now. Let's say you live in the US or elsewhere: you hear about a leak, go on the darknet, and download it. Then another leak appears, so you look for that too. Sometimes you have to buy it. To actually find anything, you open one leak, then another, or you build your own system to aggregate them all.

Russia is the only country where it's this easy to access leaked data, and there are two kinds of probiv. The first is what I call 'grey OSINT'. There are aggregators, often on Telegram, sometimes just websites. You go there, enter a surname, email, phone number, or even a number plate, and you get a huge amount of information on that person. It pulls from leaks going back to the early 2000s, sometimes even the late 1990s, and you get all of it for almost nothing—say 10 cents per person, even for a child. If someone has ever lived in Russia, their data is likely there: my daughter is 10, she left Russia when she was 7, but there's still a lot of information about her, including where she lived and even medical data. This is what I call grey OSINT, or grey probiv, because it relies on leaked data. For journalists, the question is how to use this data responsibly, when public interest is clear. Grey probiv is not really up-to-date data—it's only accurate at the moment it was leaked, right?

But if you need something deeper, you can go to dark probiv, or dark OSINT. It's again on Telegram, sometimes Signal, but you have to find contacts on the darknet, through anonymous middlemen who can sell data from state databases, police, tax services, land registries, banks, or telecom companies. It's a kind of corruption, because these middlemen have inside contacts. You can buy actual data, for example for investigations about some "bad guy." And there have been many investigations like this, and journalists use the dark probiv market: a good example is the investigation into Navalny's poisoning. (*Editor's note: this refers to the joint Bellingcat and The Insider investigation into Alexei Navalny's poisoning in August 2020*). Both grey and dark probiv are in fact criminal cases, but the second one is kind of more so, right?

How did the market of probiv appear?

So, when the first leaks happened, maybe at the beginning of the century or even earlier, some companies appeared—let's call them aggregators or B2B companies. They collected the data and had good sources in the police or state companies. They built systems to aggregate it, and you could buy disks with these systems or even a single database anywhere. There were many such disks and databases online, and we, journalists, used them. It is a bit tricky when you have disks with databases. I still have one I can show you, with, I think thousands of databases (*showing the disk*). The thing is I can just put in a name and get all the data from these leaks. I use it only for my investigations, of course, when there is a public interest. Most of these leaks are also available online.

In 2020 or 2021, the first Telegram bots appeared. The earliest one came out of a darknet market called Dark Money. The idea was simple, to buy leaked databases or just download them, since many were easily available on torrents, and turn that into a service on Telegram. That was a kind of revolution. Before that, as a journalist, I had mostly exclusive access to this kind of data. Then everything changed: once these tools moved to Telegram, everyone started using them, policemen, criminals, journalists.

Why does someone use *probiv*, who has access to it, and what determines that access?

What do they use it for? Take a simple example. Here in Bulgaria, someone parks their car and blocks you in. What can you do if there's no phone number? In Russia, people would go to these bots, enter the license plate, get a phone number and call the person to say, "Hey, please move your car." There are many situations like this, so it's not only for criminal use.

There was an article from a police university, a survey among officers, and about 80% of them said they had used Eye of God. Why? Because if you have a suspect, you often need to know where they actually live, not their official address. People don't always live where they're registered, but when they order food or open a bank account, they often provide their real address. In most other countries, the police would have to send an official request to a bank or a telecom company to obtain that information. But in Russia, however, there's no need: officers could just go to the bot, Eye of God, and pull the data from leaked databases. The funniest thing is police got free access, often without even knowing who ran the service.

The title of your book is *The Russian Cyberpunk: How the Kremlin Builds a Digital GULAG — And Who Is Resisting It*. The subtitle seems to suggest that cyberpunk is already here, while the GULAG is yet

If someone has ever lived in Russia, their data is likely there: my daughter is 10, she left Russia when she was 7, but there's still a lot of information about her, including where she lived and even medical data.

to come. Why do you think "cyberpunk" is the more accurate term for Russia at this point?

In Russia, almost everything is officially prohibited, but you can do almost anything until the state decides to prosecute someone. Buying personal data is illegal, but the police and everyone else do it, so the strictness of the laws is offset by the fact that they aren't always enforced.

Another part of the market, dark probiv, is based on corruption: people like local police officers have access to large amounts of data, and there are weak controls over how that access is used. A man in a bank has access to all data of his clients and it's very easy to get information from these databases. They are not afraid of being prosecuted; the prosecution is very soft for selling data. Banks and telecom companies, sometimes with their security partners, would find the people selling data and just fire them without taking it further, because they didn't want scandals.

And this is part of this idea of total control. The Russian state wants more and more control over data, building what I call a digital gulag (*Editor's note: the accumulation of large quantities of data in centralised systems*). But the other side of this system is that it produces more and more leaks of sensitive data, both on the grey market and on the black market.

So why didn't the state shut this market down?

This is again part of what I call Russian cyberpunk. After every major investigation, some of the people selling data were arrested. The market adapted. Now it's harder, for example, to get information on someone you can easily google. Two years ago, a new law was introduced, making systems like Eye of God explicitly illegal.

And what happened? The black market still exists. It's now much harder to buy data on well-known figures, but it hasn't disappeared. So why does it still exist? Because policemen, people in banks, and others still have access to all the data. Their salaries are low, so they need money. Prosecution doesn't really stop them; some aren't afraid of a year in prison. That's why this market exists.

And then there's the grey data market. Eye of God was shut down, and there's a criminal case against it. But what happened? Some of the service owners in Russia were arrested, others moved abroad. They used to try to stay closer to the "white zone" and cooperate with the police. Now they don't have to anymore. I understand there's no white zone in a market where data is being sold illegally, but you know, somewhere there is a white zone, right? So, most of the services that two years ago tried to stay closer to the "white zone" have now, after moving abroad, opened their APIs to criminals and scam call centres. Therefore, there is an epidemic of phone scams due to the large amount of personal data lying around.

Has the Russian invasion of Ukraine in 2022 changed the situation?

It's not just a hot war, but also a cyber war. Ukrainian hackers and activists, with support from around the world, attacked many systems, including databases, banks, and other companies. In many cases, they just published these databases on Telegram. Now there are Telegram bots containing only leaks from this war period, and you can still find almost anyone there. For Ukrainian call centers, it became part of their effort in the war.

How do you reconcile the professional use of *probiv* with your personal views on privacy and data access?

Perhaps the final point, or disclaimer, is this: as a journalist, I use such information because there is a public interest; I use it for my investigations.

For example, yesterday I published an investigation showing that Putin has shares in a state-backed app. I contacted his nephew, as the shares were registered in his name. For Western journalists, finding such information could take weeks, but it took me only seconds. However, this is not something to be proud of. The information is simply lying around, easily accessible. In a way, criminals are exploiting other criminals. There is nothing positive about that — data is just out there, available to anyone. Two years ago, there was a major leak from the Russian border police. Aggregators now show border crossings from 2014 to 2023. The leak came from an FSB (Federal Security Service of Russia) database, not hacked but sold on the market. I wrote an article reporting it as the largest leak from FSB systems ever. The data aggregator owners were alarmed and removed the database from their system.

My colleagues asked, 'What have you done?' Many wanted to use the database for investigations. For me, it was the first time I thought: citizens should know that such leaks exist, and in a normal country those responsible would be prosecuted. Journalists, as well as policemen, should investigate these markets. But, in a situation where we, as journalists, are labelled as foreign agents, we have to leave the country, and some public records are now closed. In this context, public interest is on our side.

Because of my investigations into this market, for example, we lost access to the FSB data leak for some time; now it is available through other aggregators. On one hand, public interest says you should investigate who is behind the market and write about these leaks. On the other hand, public interest says not to, because journalist-investigators will lose access.

The theme of CPDP 2026 is *Competing Visions Shared Futures.* Do you see the "cyberpunk-to-digital-GULAG" trajectory specific to Russia's context, or does it carry broader risk that other highly digitalised societies could also face?

Sometimes in the world I recognise some Russian vibes. For example, maybe you know the story that ProtonMail was about to leave Switzerland last year because of a new law that was going to appear (*Editor's note: The Swiss law proposed in 2025 would have required encrypted messaging services to retain or share certain user data with authorities*). The CEO of ProtonMail, in his interview, said, 'The law you are going to take—there is only one place in Europe with the same law.' How do you think—which country did he give as his example?

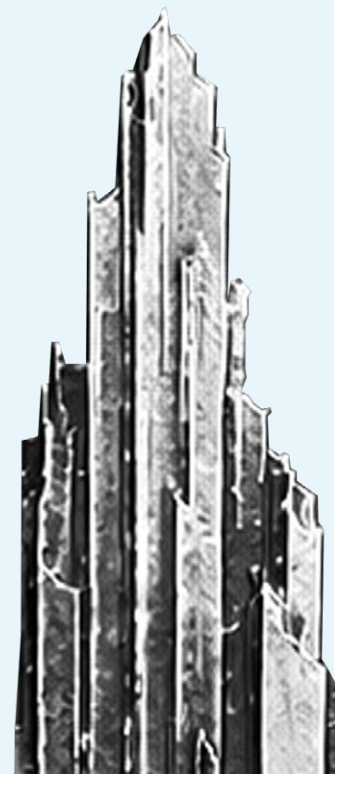
Russia.

Or take chat control. *(Editor's note: "Chat control" refers to proposed EU legislation that would require platforms to scan private digital communications—including encrypted messages and images—to detect illegal content such as child sexual abuse material, raising significant concerns about privacy and mass surveillance.)* When I look at it now, it reminds me of how things started in Russia. The argument is always the same: it's only about targeting terrorists, or just "bad people." Fifteen years ago, after the first protests against Putin in 2011, a blacklist law was introduced to block websites with child abuse, drugs, and, I think, suicide. People said, 'This is bad,' and it is. Everyone should admit that. But you know, now there is an instrument to block sites, right?

Okay, maybe now you think you can control this situation, right? Maybe now you think you're struggling for good. But if you give this instrument to the police, tomorrow your local Trump could use it against you. The idea of the book is to show how it started in Russia and where we are now, with all this blocking, the state going after our data, our chats, and so on. I don't like these Russian vibes I see everywhere now. ▪

This interview was organised by Privacy Salon NGO as part of Privacytopia—the artistic programme developed alongside CPDP. It forms part of their ongoing curatorial research into artists and practitioners working within, and critically reflecting on, the Russian digital landscape.

Buying personal data is illegal, but the police and everyone else do it, so the strictness of the laws is offset by the fact that they aren't always enforced.



Conversation with

Dara Hallinan & Barbara Lazarotto

Over the past 15 years, Dara Hallinan has been a central figure in shaping CPDP's programme. Since joining the team in 2012, Dara has contributed not only with his expertise but also with his distinct perspective on the interaction among law, new technologies, in particular ICT, and biotech.

Throughout these years, Dara played an important role in shaping CPDP's direction during a period of significant regulatory change, marked by the enactment of the GDPR and the broader development of the EU's digital regulatory framework. His contributions ensured that the conference remained connected to evolving debates on data protection, governance, and the future of digital regulation.

As Dara steps back from his role to focus on his research, the programming team welcomes a new member. Barbara Lazarotto now joins the programming team. Barbara is a researcher affiliated with the Law, Science, Technology and Society Research Group (LSTS) of Vrije Universiteit Brussel, where she researches the intersection of data protection and data governance regulations.

To reflect on this moment of transition, Dara and Barbara sat down to discuss the past and future of CPDP.

Barbara: We're marking almost ten years since the adoption of the General Data Protection Regulation, which feels like a good moment to both look back and look ahead. You've been closely involved in this space for quite a while now... Looking back over the past decade - or even a bit longer - what stands out to you about how data protection, and the GDPR in particular, has evolved?

Dara: *There are, of course, numerous specificities which might be discussed regarding the development of EU data protection law, and the GDPR specifically, over the past decade and beyond. I would maybe just mention one holistic change here, and one that is not necessarily linked to the specifics of the law itself: the degree to which the phenomenon and risks of personal data processing, and with that the content of EU data protection law, have entered common conversation and common consciousness.*

Barbara: Indeed, it feels quite interesting today how present data protection has become in everyday conversations. The other day, I was at the Post Office, and someone mentioned their GDPR rights to the attendant. Do you think the growing centrality of data protection in society will also impact future changes, for example, in the GDPR and other regulations?

Dara: *I find it hard to talk about future changes in the GDPR... There are, of course, concrete propositions on the table in the form of the digital omnibus proposal. But beyond these, the future is hard to predict. This is an inevitability owing to the prominence of data processing as a determining feature of modern societies, and the fact that the future developmental trajectory of data processing technologies, their implementation, and their social implications, are highly uncertain. It is worth remembering, however, when looking forward, that despite the turbulence of its subject matter, data protection law in the EU has, over the past 30 years or so, retained a significant degree of stability.*

I feel that over time, the conference has become much more multi-stakeholder.

Barbara: Talking about changes, you've been involved with the CPDP for many years now. Looking at the conference itself, did you see it transform over time?

Dara: *The transformation of the conference was evident in many ways. First, naturally, there were thematic evolutions that reflected technological, legislative, and political development. For example, AI has appeared as the dominant technological theme of the conference in the last three or four years. Second, there were developments in terms of the public at the conference. I feel that over time, the conference has become much more multi-stakeholder. I think there is a greater NGO presence now than there was, for example, 10 years ago, as well as a greater corporate presence. Equally, there has been a significant development in the aesthetic of the conference, especially over the years since Thierry has been in charge. The range of art, and cultural side events available under the CPDP banner is now astounding, and I think adds real value to the event. Finally, I would highlight that the conference has grown and grown and grown over the past decade or so. From a conference with 3 parallel tracks to a conference now with 6 parallel tracks and a dizzying number of satellite events is a huge increase!*

Barbara: Indeed! I have been joining CPDP consistently for the last years, and the changes have been incredible. The art and the addition of workshops have brought more nuances to the conference. How do you think that evolution fed into your own work, both intellectually and in terms of organizing the programme?

Dara: *Thematic developments and developments in the participants at the conference have certainly helped broaden my perspectives as to the topics and the perspectives on these topics, which are, at any moment in time, relevant within our community. This has been especially valuable as an academic lawyer, where a holistic perspective on themes not directly related to one's own work, and on perspectives from outside the legal bubble, is invaluable!*

These developments have also required that the conference programme be managed in different ways. In particular, with the developments in size came the need for clearer and more defined communications and administrative structures. Whereas previously it had been possible to take a more informal and ad hoc approach to the organization of the conference, with the number of panels now hosted and the degree of coordination necessary between panels, speakers, organizers, sponsors, etc., structures for communication and interaction became much more important. Beyond this, the integration of a greater range of perspectives into the conference required a development of our ability to appreciate the needs of different stakeholders, and as to how these could be effectively integrated into a multi-stakeholder forum without disappointment.

Barbara: What would you say you are most proud of in this trajectory?

Dara: *I'm quite proud that we have managed, for the most part, to maintain the spirit of CDPP over the past 15 years. I think it's still essentially the same conference it was back then! We have done that whilst, for the most part, retaining the interest and participation of all the different perspectives within the community.*

Barbara: I would like to steer our conversation towards CPDP topics. This year, just a few days after CPDP, marks ten years since the adoption of the GDPR, a milestone that invites reflection on how data protection has shaped the European digital landscape over the past decade. At the same time, we seem to be entering a new transition period in EU digital regulation. Dara, you have been part of the CPDP programming team for 15 years, including during the period when the GDPR was adopted and later implemented. How did this process shape the discussions and panels at CPDP?

Dara: *The thematic area covered by the conference moves extremely fast, and accordingly, the topics represented at the conference are shaped to a large extent by high-profile legislative or technological developments, which then function as the centre of mass for discussion. So, prior to the adoption of the GDPR, a significant portion of panels at the conference focused on the novelties and*

the controversies around the GDPR and its content. Following the GDPR, a significant portion of panels began to focus on the interpretation of the provisions of the GDPR as well as on their implementation. Some four years after adoption, I would say, one then noticed a change in discussions away from the specifics of the GDPR, and towards the new raft of legislative proposals, as well as the emerging issues around AI.

Despite all of the above, CPDP, throughout its lifetime, has always tried, and with I think a certain degree of success, to avoid solely discussing the big theme-of-the-day, and to ensure the presence of more abstract, niche, and forward-looking panels.

Barbara: Were there moments when you could clearly see the conversation shifting, for example, in the kinds of panel proposals, speakers, or debates that were coming into the programme?

Dara: *Yes, these shifts in topics present at the conference tend to reflect general discussions around data processing in society, and specific high-profile political developments in the EU. So, for example, in the years leading up to the adoption of the GDPR, it was inevitable that panels would reflect discussions about the content of the GDPR. In the years of CJEU rulings on international data transfers, panel discussions focused more on international data transfers.*

Now let's switch to you... as you mentioned earlier, we also seem to be entering a new phase in European digital regulation at the same time you are joining the programming team. What stood out most about the process and what were the challenges you faced considering this particular moment?

Barbara: I was particularly impressed by how quickly the themes evolve. Even within a single programming cycle, you can see certain topics gaining prominence, others fading, and new tensions emerging. That makes the process quite dynamic, but also quite demanding, because you are not just organising content, you are, to some extent, curating a snapshot of an ongoing and very fluid debate.

One of the main challenges was precisely working within that dynamic context while still contributing something coherent. We aim to respond to what is currently salient and to ensure that the programme remains diverse, while navigating the conference's multi-stakeholder nature.

Dara: *Given the constant need to balance what is emerging with continuous relevant topics, when you look ahead, what do you hope CPDP will contribute to these shared futures?*

Barbara: Looking ahead, I would hope that CPDP continues to function as a forum where competing visions can be articulated clearly and confronted constructively. That, to me, is what allows "shared futures" to emerge in a meaningful way... through engagement across differences.

Since it is my first year as a director... do you have any practical tips? How did you approach the programming process?

Dara: *I always approached the programming as an exercise in diplomacy and balance. The aims of the conference and the specific aims of panel organizers and speakers are not always aligned, and it is important to try and understand their perspectives so as to come up with a result that everyone is happy with. In turn, from a more holistic perspective, for CPDP to work, balance needs to be struck between a whole host of factors including, for example: the need for stability, and the need for development; the need for participants to feel represented/at home, and the need for divergent viewpoints; the need to discuss pressing high-profile issues, and the need to make space for more theoretical, niche, or forward-looking, discussions.*

Barbara: What tended to be the most difficult trade-off when you were putting the programme together?

Dara: *The trade-off between structure and specificity. It's simply not possible to integrate all individual requests and retain the structures that allow the conference to function, even when these requests make complete thematic and organizational sense. The hard part is working out how much useful novelty can be integrated whilst retaining the necessary structure.*

Looking ahead, I would hope that CPDP continues to function as a forum where competing visions can be articulated clearly and confronted constructively.

Barbara: Talking about balance... what, in your opinion, makes a perfect panel?

Dara: *The speakers! In particular, the degree to which speakers are selected who have: competing visions around a theme; are able to present their perspectives in a way which allows those with potentially competing approaches to understand an alternative point of view; and are willing to engage with each other in the spirit of mutual respect and constructive criticism. Of course, it really helps when the topic under discussion is gripping!*

Barbara: If you had to boil it down, what's one piece of advice and one warning you'd give to me?

Dara: *Be as generous as you can in your perception of what people are doing in relation to the conference. They are almost always trying to do something good! Regarding the warning... I think I would warn about being too zealous in the imposition of structure on the conference. Structure is naturally very important, but so are quality and evolution, and these may require a degree of variation from structure. There is always the need to consider panels in light of the specifics of their topic, aim, composition etc.*

Barbara: Putting myself a bit on the spot here... what do you hope I would change and would I take it forward?

Dara: *I hope you manage to take a more active role in shaping the specifics of the conference programme, such as planning really novel/special panels centrally. Building the necessary communications and administrative structures to make sure the conference could continue with the available resources meant this was not always possible to the degree I would have liked.*

Barbara: Thank you, that's very encouraging, especially given your many years of involvement in shaping the conference. I'm looking forward to building on the foundation you've put in place. ▪

Digital Youth Futures: Good Intentions, Fragile Foundations?

OPINION PIECE

Caring for the next generation means more than worrying about screen time. Too often, concerns are blurred together: "a conflation is often observed between digital tools (smartphones, screens, etc.), systems (the Internet), services (social media), and the uses that can be made of them."[1] The real challenge of the coming years is ensuring that children and young adults inherit a digital environment that does not systematically undermine individual and collective autonomy and entrench exposure to online harms.

CPDP welcomes the Digital Youth Futures track for the first time in 2026, co-curated by **Sophie Stalla-Bourdillon** and **Bárbara da Rosa Lazarotto** (co-directors of the Brussels Privacy Hub). The regulation of minors' online experience and protection remains deeply complex and contested. It spans a broad spectrum of issues, from age-appropriate design and age assurance mechanisms to highly politicised and potentially intrusive interventions. This track will dive deeper into these debates and contested topics, to foster cross-disciplinary dialogue on the online protection of minors, their rights, and well-being. CPDP asked Sophie Stalla-Bourdillon for an opinion.

Encouragingly, the protection of minors remains one of the few issues that still sustains genuine dialogue across policy communities. Recent transatlantic policy roundtables in 2025 showed a shared willingness among regulators, scholars, and civil-society actors to find workable solutions for safeguarding children online, even where broader digital policy debates remain polarised.[2] Globally, the G7 Data Protection and Privacy Authorities confirmed in July 2025 that protecting children online was one of its top two priorities.[3]

Across Europe, new legislation and regulatory initiatives consistently foreground minors as a priority category requiring enhanced safeguards. In the United Kingdom, recent amendments to data-protection rules explicitly place the "the children's higher protection matters" at the centre of data protection-by-design obligations.[4] The UK Data Protection Authority, the Information Commissioner's Office, has been reviewing platform practices,[5] and reported "strong progress on its Children's code strategy" in December 2025.[6] In February 2026, fines have been issued against players such as MediaLab and Reddit.[7]

Monitoring processing practices involving data relating to minors has been a priority for data protection regulators in the European Union as well.[8] In 2025, "several mobile applications and online games, a significant proportion of whose users are minors, were ordered [by the CNIL] to strengthen user age verification and improve transparency in order to better protect minors' data."[9] Monitoring actions have targeted education contexts specifically. By way of example, the Danish Datatilsynet banned use of Google Chromebooks and Workspace in a municipality's primary in 2022.[10]

Concerns about minors are increasingly surfacing in legislation beyond the traditional domains of privacy and data protection. In the European Union, sustained inclusive policy efforts have culminated in the adoption of European Commission guidelines adopted in October 2025 under Article 28(4) of the Digital Services Act[11] and in requests for information and formal proceedings,[12] while the proposed Child Sexual Abuse Material Regulation[13] has progressed despite ongoing civil society concerns.[14] In the UK, Ofcom has been busy specifying how legal duties to protect children online must be fulfilled under the Online Safety Act.[15]

Despite what current policy and legislative trends might suggest, regulators and courts are however still grappling with what child-centred design actually requires in operational terms.

This uncertainty reflects several structural tendencies. One is a recurring "outrage-driven policymaking," in which public outrage drives rapid legislative responses before technical and legal details are fully resolved. Another is the tendency to delegate responsibility to private platforms without establishing effective transparency and accountability mechanisms. In the early 2000s, EU policymakers had attempted to resist turning intermediaries into de facto regulators. But as digital markets centralised and the myth of platform neutrality eroded, attitudes shifted. Judicial bodies such as the European Court of Human Rights hinted in this direction years ago with Delfi v Estonia,[16] and a recent ruling from the Court of Justice of the European Union seem to confirm it.[17] Yet, as two decades ago, important operational questions remain unresolved, raising the risk that well-intentioned child-protection rules could harden into regulatory anti-patterns.

Political consensus often exists at the level of principle: few lawmakers oppose protecting children. But consensus tends to weaken when discussions turn to operational details. One striking trend is the growing reliance on age-assurance systems as the cornerstone of regulatory strategies, although a better approach is to view them as targeted complements to age-appropriate design requirements.[18] These mechanisms are increasingly proposed, and adopted, to restrict minors' access to certain online services, particularly social media. National debates in countries such as Australia[19] and France[20] illustrate how access bans have emerged as the dominant response to online harms.

This trend deserves closer scrutiny, however. Data breaches, including high-profile incidents affecting platforms like Discord, repeatedly demonstrate how fragile digital infrastructures can be.[21] There are warning that large-scale identity or age-verification databases create attractive targets for attackers.[22]

Privacy-enhancing-technology experts likewise caution that real-world implementations of age-assurance systems often fall short of their theoretical promises and can generate externalities, particularly in terms of digital sovereignty.[23]

A significant number of scholars who study children online practices and digital rights tend to oppose blanket social-media bans, arguing that exclusionary approaches may undermine participation, education, and social development.[24] What is more, evidence as to the benefits and harms associated with platform usage is contrasted. "Although many policy makers, schools, and parents are primed to believe arguments that smartphones and social media are inherently harmful, the evidence about their overall effect on children is not clear cut."[25] A cross-disciplinary and long-term approach is crucial, as illustrated by research from the CNIL Innovation Lab,[26] and should continue to inform the ongoing work of regulators. Besides, bad practice by intermediary age assurance providers has already been flagged despite the adoption of binding standards.[27]

What tends to be missed in current policy debates and is emerging when dialoguing with youngsters, who should be included in the debate, is nuance of online practices, poor investment in the offline conditions that actually improve children's digital lives, e.g, access to quality education, safe in-person times and spaces, attentive caregiving, as well as basic online safeguards that should be there for everyone and are still missing.[28] Even if the current normalisation of giving smartphones and access to social media calls for careful consideration as pointed by many doctors, scientists and practical experts particularly

in the Netherlands, [29] this does not necessarily mean that a legally binding blanket prohibition operationalised through an obligation imposed on platforms to put in place age assurance techniques is the way to go. Generally speaking, focusing upon reducing screen time for all age ranges is likely to be distracting.[30]

When governments push legislation forward without first establishing the institutional and technical infrastructure required to effectively support the youth, they risk exacerbating the very problems they aim to solve. For example, if age assurance is considered to be a techno-legal fix, this can lead to stagnation, or even decline, in the safety of mainstream services, while pushing users toward less regulated and potentially more hazardous platforms. In turn, this may intensify profiling practices and create incentives for actors to process sensitive data with weak security standards.

Making children rights effective online is too important to be governed by slogans or symbolic regulation. If policymakers truly want to secure a healthier digital future for the next generation, they must resist the temptation of quick fixes and instead commit to rigorously exploring age-appropriate safeguards. The stakes are too high for anything less.

Sophie Stalla-Bourdillon

1 Anses, 'Usages Des Réseaux Sociaux Numériques et Santé Des Adolescents - Avis de L'Anses Rapport d'expertise Collective' (2025) <https://www.anses.fr/system/files/AP2019-SA-0152-RA.pdf>.

2 Michèle Ledger, 'Transatlantic Cooperation on Protecting Minors' (14 January 2026) <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/transatlantic-cooperation-on-protecting-minors-online/?utm_source=chatgpt.com>.

3 G7 Data Protection and Privacy Authorities, '2025 G7 Data Protection and Privacy Authorities Roundtable Statement' <https://www.priv.gc.ca/en/opc-news/speeches-and-statements/2025/js-dc-g7_20250619/>.

4 See Article 25(1) UK GDPR.

5 ICO, 'Annex: Table of Observations from Our Review of a Sample of Social Media and Video Sharing Platforms' (*Information Commissioner's Office*) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy/children-s-code-strategy-progress-update-march-2025/annex/>.

6 ICO, 'Children's Code Strategy Progress Update - December 2025' (*Information Commissioner's Office*, December 2025) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/protecting-childrens-privacy-online-our-childrens-code-strategy/children-s-code-strategy-progress-update-december-2025/>.

7 See ICO, 'Imgur owner MediaLab Fined over Children's Privacy Failures' (*Information Commissioner's Office*, 5 February 2026) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/02/imgur-owner-medialab-fined-over-children-s-privacy-failures/>; ICO, 'Reddit Issued with £14.47m Fine for Children's Privacy Failures' (*Information Commissioner's Office*, 24 February 2026) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/02/reddit-issued-with-1447m-fine-for-children-s-privacy-failures/>.

8 See e.g., CNIL, 'CNIL Investigations in 2024: Minors Data, Olympic Games, Right of Access and Digital Receipts' (*CNIL*, 8 February 2024) <https://www.cnil.fr/en/cnil-investigations-2024-minors-data-olympic-games-right-access-and-digital-receipts?utm_source=-chatgpt.com>.

9 CNIL, 'Sanctions and Corrective Measures: CNIL's Actions in 2025' (*CNIL*, 9 February 2026) <https://www.cnil.fr/en/sanctions-and-corrective-measures-cnils-actions-2025>.

10 Marcelo Corrales Compagnucci, 'Danish DPA Banned the Use of Google Chromebooks and Google Workspace in Schools in Helsingor Municipality' <https://arxiv.org/abs/2407.19377>.

11 European Commission, 'Commission Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online Pursuant to Article 28(4) of Regulation (EU) 2022/2065' (2025) Communication from the Commission <https://digital-strategy.ec.europa.eu/en/library/commission-seeks-feedback-guidelines-protection-minors-online-under-digital-services-act>.

12 E.g., European Commission, 'Commission Opens Formal Proceedings against TikTok under the Digital Services Act' (19 February 2024) <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926>; 'Commission Preliminarily Finds TikTok's Addictive Design in Breach of the Digital Services Act' (*EC*, 6 February 2026) <https://digital-strategy.ec.europa.eu/en/news/commission-preliminarily-finds-tiktoks-addictive-design-breach-digital-services-act>.

13 The Council has reached its common position on 13 November 2025. Council of the European Union, 'Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse' (2025) 2022/0155 (COD) <https://data.consilium.europa.eu/doc/document/ST-15318-2025-INIT/en/pdf>.

14 Chiara Castro, '"It's Just Smoke and Mirrors" – Over 500 Cryptography Scientists and Researchers Slam the EU Proposal to Scan All Your WhatsApp Chats' [2025] *techradar* <https://www.techradar.com/computing/cyber-security/its-just-smoke-and-mirrors-over-500-cryptography-scientists-and-researchers-slam-the-eu-proposal-to-scan-all-your-whatsapp-chats>.

15 Ofcom, 'Protection of Children Code of Practice for User-to-User Services' (205 AD) <https://www.ofcom.org.uk/online-safety/protecting-children/protection-of-children-duties-under-the-online-safety-act>; Ofcom, 'Protection of Children Code of Practice for Search Services' (205 AD) <https://www.ofcom.org.uk/online-safety/protecting-children/protection-of-children-duties-under-the-online-safety-act>; Ofcom, 'Guidance on Highly Effective Age Assurance - For Part 3 Services' (2025) <https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/part-3-guidance-on-highly-effective-age-assurance.pdf?v=395680>.

16 *Delfi AS v Estonia* [2015] ECtHR Application no. 64569/09, ECLI:CE:ECHR:2015:0616JUD006456909. But see

17 *X v Russmedia Digital SRL, Inform Media Press SRL* [2025] CJEU C-492/23, ECLI:EU:C:2025:935.

18 The Article 28(4) guidelines endorses such an approach.

19 Many social media platforms are required to take reasonable steps to prevent Australians under the age of 16 from having accounts. This law came into effect on 10 December 2025.

20 Morgane Tual and Violaine Morin, 'France's Assemblée Nationale Approves Social Media Ban for under-15s' *Le Monde* (27 January 2026) <https://www.lemonde.fr/en/france/article/2026/01/27/french-lawmakers-approve-social-media-ban-for-under-15s_6749844_7.html>.

21 Dan Goodin, 'Discord Says Hackers Stole Government IDs of 70,000 Users' [2025] *ars Technica* <https://arstechnica.com/security/2025/10/discord-says-hackers-stole-government-ids-of-70000-users/>.

22 Mike Masnick, 'Hackers Expose The Massive Surveillance Stack Hiding Inside Your "Age Verification" Check' [2026] *techdirt* <https://arstechnica.com/security/2025/10/discord-says-hackers-stole-government-ids-of-70000-users/>; Lauren Leffer, 'Online Age Verification Laws Could Do More Harm Than Good' [2024] *Scientific American* <https://www.scientificamerican.com/article/online-age-verification-laws-privacy/>.

23 Eliza Gkritsi, 'Resist "Dangerous and Socially Unacceptable" Age Checks for Social Media, Scientists Warn' [2026] *Politico* <https://www.politico.eu/article/age-check-social-media-scientist-warning/>.

24 See e.g., Emily Setty, 'I Research the Harm That Can Come to Teenagers on Social Media. I Don't Support a Ban' (*The Conversation*, 21 January 2026) <https://theconversation.com/i-research-the-harm-that-can-come-to-teenagers-on-social-media-i-dont-support-a-ban-273835>; Sonia Livingstone, 'The UK Shouldn't Rush to a Social Media Ban for Children under 16' (*LSE British Politics*, 23 January 2026) <https://blogs.lse.ac.uk/politicsandpolicy/the-uk-shouldnt-rush-to-a-social-media-ban-for-children-under-16/>; Gurvan Le Guellec, 'Anne Cordier, Sociologue : « L'interdiction Des Réseaux Sociaux Aux Jeunes Me Paraît La Fausse Bonne Idée Par Excellence »' [2026] *Le Nouvel Obs* <https://www.nouvelobs.com/societe/20260114.OBS111489/anne-cordier-sociologue-l-interdiction-des-reseaux-sociaux-aux-jeunes-me-parait-la-fausse-bonne-idee-par-excellence.html>; Sander van der Linden, 'Social Media Bans for Teens Lack Evidence' (*nature health*, 25 February 2026) <https://www.nature.com/articles/s44360-026-00083-4>.

25 Victoria A Goodyear and others, 'Approaches to Children's Smartphone and Social Media Use Must Go beyond Bans' (2025) 388 BMJ e082569 <https://doi.org/10.1136/bmj-2024-082569>.»plainCitation»:»Victoria A Goodyear and others, 'Approaches to Children's Smartphone and Social Media Use Must Go beyond Bans' (2025

26 LINC, '[Dossier] Minorité Numérique' (*LINC*) <https://linc.cnil.fr/dossier-minorite-numerique>.

27 AI Forensic found that the AgeGO age-verification system, used on xnxx.com, xvideos.com, and tnaflix.com, collects both the website and the exact URL of the content users attempt to access, and fails to inform users that, if they choose the "Selfie" verification method, their webcam stream will be transmitted to Amazon Web Services. AI Forensics and Paul Bouchaud, 'Technical Report: AgeGO' (2025) <https://aiforensics.org/work/agego-porn-platforms>. But see ARCOM, 'Référentiel Déterminant Les Exigences Techniques Minimales Applicables Aux Systèmes de Vérification de l'âge Mis En Place Pour l'accès à Certains Services de Communication Au Public En Ligne et Aux Plateformes de Partage de Vidéos Qui Mettent à Disposition Du Public Des Contenus Pornographiques' (2024) <https://www.arcom.fr/presse/acces-des-mineurs-aux-contenus-pornographiques-larcom-publie-son-referentiel>.

28 See e.g., Sherry Turkle, *Reclaiming Conversation - The Power of Talk in a Digital Age* (Penguin Books 2016). See also EDRi, 'Breaking the Extractive Digital Business Model: A Rights-Based Digital Fairness Act' (2026) Position Paper <https://edri.org/our-work/breaking-the-extractive-digital-business-model-a-rights-based-digital-fairness-act/>.

29 'Een Oproep Om de Negatieve Impact van Schermgebruik En Sociale Media Op Kinderen En Adolescenten Daadkrachtig Aan Te Pakken' (*SMARTPHONEVRIJ OPGROEIEN NEDERLAND*, 26 May 2025) <https://smartphonevrijopgroeien.nl/brandbrief/>.

30 Unicef, 'Childhood in a Digital World - Screen Time, Digital Skills and Mental Health' (2025) <https://www.unicef.org/innocenti/reports/childhood-digital-world>.

Interview by **Sophie Stalla-Bourdillon**

Protecting Minors Online: Regulation, Rights, and the Limits of Age Verification

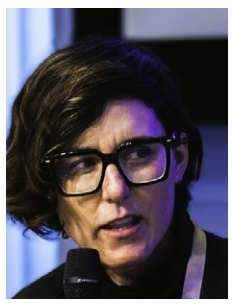
This interview is part of our Youth Safety Online Track, which brings together experts to examine how digital environments can better protect and empower younger users. It reflects our continued commitment at CPDP to place children's rights at the centre of debates on platform regulation, data protection, and online safety. By fostering dialogue across policy, technology, and civil society, we aim to ensure that measures designed to protect minors also uphold their fundamental rights.

Owen Bennett

Owen is an independent tech policy expert. He has spent his whole career working in technology policy, particularly platform regulation in the UK and Europe. His most recent in-house role was head of international online safety at Ofcom, which is the UK's communications regulator. There, he built and led the function, which was developing Ofcom's international strategy for how it would approach the Online Safety Act and its regulatory powers under it. Prior to that, he worked at the Mozilla Corporation, the not-for-profit tech company and the maker of the Firefox web browser.

Simeon de Brouwer

Simeon is a policy advisor at EDRi, working mostly on age verification and the eID regulation, the eID wallet. Using a rights-based approach, he has been analysing the proposals to protect young people using age verification, particularly the eID wallet. Simeon coordinates EDRi members on these topics, who bring their technical expertise and their national point of view.



Interviewer: Sophie Stalla-Bourdillon

Sophie spent a decade as a tenured track professor of Information Technology Law and Data Governance at the University of Southampton, where she held the Chair in IT Law and Data Governance from 2018 to 2022. She is now visiting professor within Southampton Law School. Since 2023, she became Co-Director of the Brussels Privacy Hub (BPH), an academic research hub at VUB within the wider LSTS research group. Alongside her academic career, Sophie has extensive industry experience, having worked at Immuta for six years, where she led the Legal Engineering team. In this role, she focused on the legal and ethical implications of data operations in analytics and AI environments, as well as the impacts of compliance automation. Sophie has served as editor-in-chief of the Computer Law and Security Review, a leading international journal of technology law, and is now honorary consulting editor.

Sophie: Is the law, e.g., the Online Safety Act in the UK (OSA), the Digital Services Act (DSA) in the EU, effectively achieving its goal of protecting children?

Owen: It is still too early to assess whether the OSA is delivering its intended outcomes. This framework is designed to drive long-term cultural change, shifting away from a reactive model, where companies only engage with regulators after something goes wrong, toward a proactive duty of care. This kind of transformation takes time.

A key challenge is that legislation alone is not enough. Regulators such as Ofcom must translate legal obligations into tangible improvements in people's online experiences. That requires developing clear strategies, enforcement priorities, and what might be called a "theory of change." As a result, progress is likely to be incremental rather than immediate.

Simeon: From the EU perspective, the main issue is insufficient enforcement. The Commission has taken relatively cautious steps, and national Digital Services Coordinators have been slow to act. This means that many DSA violations remain unaddressed.

Even in cases of clear non-compliance, enforcement has been fragmented. For example, ensuring that platforms provide non-algorithmic feeds has required litigation at the national level, leading to outcomes that apply only within a single Member State. Without stronger, centralised enforcement, the DSA risks not achieving its full potential.

Sophie: What indicators should we use to measure success of the Act?

Owen: The most meaningful metric is whether users feel safer, more empowered, and more in control online. This requires long-term, longitudinal research rather than short-term compliance checks.

There are also useful upstream indicators, such as reductions in the prevalence of illegal or harmful content, or observable design changes, for instance, when platforms remove or limit features like infinite scroll for minors. These signals can indicate that regulation is starting to influence platform behaviour.

Simeon: We need to be careful not to equate success with exclusion. Counting how many users are blocked or prevented from accessing services is not a meaningful metric. The real question is whether we have made the environment itself safer.

A useful analogy is road safety: we do not ban children from cycling, even though it is risky. Instead, we make roads safer and equip children with the tools and skills they need. The same logic should apply online, focusing on systemic improvements and user empowerment rather than restriction.

Sophie: What is being mandated in terms of age assurance?

Owen: The OSA adopts a targeted, content-based approach. Pornographic services must ensure that children cannot normally access their content, while user-to-user platforms must implement age assurance where they host certain categories of harmful but legal content, such as content promoting self-harm or eating disorders. Ofcom has chosen a principles-based approach, setting requirements such as effectiveness, robustness, accessibility, and non-discrimination, rather than mandating specific technologies. In practice, many services are turning to age estimation methods, partly because users are reluctant to share formal identification documents.

Simeon: In the EU, age assurance is currently a targeted, optional and context-dependent measure, under frameworks such as the GDPR, the DSA, and the Audiovisual Media Services Directive. The logic is that platforms should provide enhanced protections where they know, expect or suspect that users are minors, rather than systematically verifying everyone's age.

However, there is a clear shift in ongoing policy discussions toward widespread, mandatory age verification, particularly for services such as social media, AI tools, and messaging platforms. The EU is also exploring

The most meaningful metric is whether users feel safer, more empowered, and more in control online.

Social media bans are not the solution. Protection should come from making services safer and supporting users, not excluding them.

privacy-preserving solutions, such as digital identity wallets, as an alternative to more intrusive approaches like biometric age estimation.

Sophie: Are current age assurance technologies meeting regulatory standards?

Owen: This remains an open question. While many major platforms have begun deploying age-assurance systems, particularly in the UK, there is limited evidence about their actual effectiveness or compliance with data protection and cybersecurity requirements.
Public trust is fragile. A single high-profile failure could significantly undermine confidence in these systems and in the broader regulatory approach.

Simeon: No technology currently on the market meets EU regulatory standards. Even the upcoming eID wallet risks falling short from the legal framework it is built on, as its implementation is pitched to involve a weakening of some the safeguards preventing tracking and ensuring pseudonymity.
For example, requirements to "prevent" linkability are watered-down to merely measures that "hinder" it, which could allow for tracking in practice. Similarly, the system as last presented to the public does not ensure that platforms only require users to disclose their legal identity where this is justified. These developments raise important questions about whether implementation will remain aligned with the original principles. The Wallet will in any case not be accessible to everybody - you need to own a smartphone, for instance, to use it.

Sophie: How should regulators balance minor protection with the full range of fundamental rights?

Owen: There is a growing need for coordination between online safety and data protection regulators. Poor implementation of age assurance can lead to over-blocking or unnecessary restrictions, including on legitimate content.
We have already seen cases where platforms restricted access to lawful information, such as content related to LGBTQ+ communities, due to overly cautious interpretations of their obligations. Regulators need to ensure that safety measures are applied proportionately and do not undermine fundamental rights.

Simeon: From our perspective, exclusion is not an effective form of protection. Restricting access may delay or displace risks, but it does not address underlying problems. It also actively harms children and many adults, by limiting their access to information, participation, and social interaction.
We advocate for systemic improvements that make online services safer for everyone. Many of the protections currently discussed for children, such as limits on manipulative design, would benefit all users, highlighting the need to avoid a two-tier system.

Sophie: Are platforms meaningfully changing their practices?

Owen: So far, changes have been limited and largely incremental. A key issue lies in what might be called corporate psychology: when faced with new regulation, companies rarely start from "what does the law require?" Instead, they begin with what they already do and then adjust or reframe existing practices to demonstrate compliance.
This is particularly true for principles-based frameworks like the OSA and the DSA, where obligations are broad and flexible. As a result, companies can point to a wide range of existing trust and safety measures without necessarily making fundamental changes to how their services operate.
The challenge for regulators is therefore to move beyond what companies say they are doing and assess whether these measures actually translate into meaningful improvements in user experience and risk reduction. At present, there is limited evidence of this. This is precisely why the European Commission has issued numerous requests for information under the DSA: the real impact of mitigation measures remains unclear.
Where progress is most visible is in the management of illegal content: for example, improved reporting tools, content classification, and takedown mechanisms. However, there has been far less movement on systemic design changes, even though these are central to many of the risks identified by regulators.
That said, this may begin to shift. Ongoing investigations, such as the Commission's work on platform design, could mark a turning point. More broadly, the DSA appears to go beyond safety alone, aiming at accountability and better platform governance, whereas the OSA remains more narrowly focused on user safety, potentially setting a higher threshold for intervention in platform design.

Simeon: It is still too early to expect meaningful structural change, as the DSA has not yet been fully enforced. The pace of progress is affected by several factors, including limited enforcement resources, institutional constraints, and geopolitical considerations.
A key structural issue is that enforcement under the DSA is centralised in the European Commission, which is not an independent regulator in the same way as data protection authorities are. This makes enforcement more politically sensitive and, at times, slower or more cautious. This has led our members to take matters in their own hands and go to court themselves.
However, there are indications that stronger enforcement could drive real change. For example, the Commission's preliminary findings in ongoing investigations suggest that, if fully implemented, the mitigating measures required under the DSA could significantly improve platform safety without resorting to user exclusion.

Sophie: Do you see the UK moving toward social media bans or stricter access restrictions for minors?

Owen: There is a growing sense, particularly in the UK, that social media platforms are not currently safe for children, and that voluntary efforts by companies have been insufficient. This has created political pressure for stronger measures, including bans.
The situation is reminiscent of earlier regulatory moments, where governments adopted restrictive laws despite known risks to fundamental rights because they felt they had no viable alternatives. A similar dynamic may now be emerging with social media bans.
However, this is a problematic trajectory. The existing rulebooks provide plenty of levers through which safety can be improved, but to make a difference, these depend on more ambition from regulators and greater commitment from platforms. Without this, policymakers may increasingly see bans as the only remaining option.

Sophie: What trends are emerging at EU Member State level?

Simeon: Two notable trends can be observed. First, some Member States are adjusting data protection rules, such as raising the age of consent under the GDPR. However, these measures are not addressing the root of the problem and divert attention toward regulating young people instead of ensuring platform accountability.
Second, there are more concerning developments. In some cases, child protection arguments are being used to justify restrictions on lawful content or on encrypted, privacy-preserving services. Hungary, for example, has relied on national laws and the Audiovisual Media Services Directive to attempt to restrict access to LGBTQ+ content.
These examples highlight the risk that child protection measures, if broadly framed, can be misused or lead to democratic backsliding, a concern that should be kept in mind in ongoing debates on age verification and access restrictions.

Sophie: Are social media bans the right approach?

Owen: I do not support social media bans for several reasons. First, they are difficult to define and enforce: users can easily migrate to other services outside the scope of the ban, as already observed in some jurisdictions.
Second, they risk lacking legitimacy. Social media plays an important role in education, communication, and access to information, and restricting access may lead to widespread circumvention, including with parental support.
Third, enforcement would likely require restrictions on tools such as VPNs, which would have negative implications for privacy and security.
Finally, bans could have unintended global effects. If major markets exclude children, platforms may have fewer incentives to invest in age-appropriate design, potentially weakening protections elsewhere.
At a deeper level, bans risk signalling that we have abandoned the goal of making online spaces safe for children, which I do not believe is justified. We have not yet fully explored or implemented the regulatory tools available to achieve this.

Simeon: Social media bans are not the solution. Protection should come from making services safer and supporting users, not excluding them. Beyond unduly restricting everyone's ability to exercise their fundamental rights, the risk is also that we will completely fail to protect young people AND to hold the culprits accountable, while also lending legitimacy to the same harmful practices where they target adults.
The focus should be on addressing harmful practices at their root and ensuring a high level of protection for all users, while empowering children to navigate digital environments safely and autonomously. ▪

Interview by
Pablo Rodrigo Trigo Kramcsák with

Andrés Chomczyk Penedo

Andrés Chomczyk Penedo is a postdoctoral researcher at Universidad Pontificia Comillas (ICADE) with an international career spanning Brussels, Barcelona, and beyond. His work sits at the intersection of financial regulation and data protection, with a particular focus on how individuals can be meaningfully empowered in data-driven financial systems—from open banking to broader open finance frameworks. A former Marie Skłodowska-Curie Fellow at Vrije Universiteit Brussel's LSTS group, he has contributed to multiple EU-funded projects and continues to engage with the Brussels Privacy Hub as a senior fellow in digital finance. He was interviewed by his friend and colleague Pablo Rodrigo Trigo Kramcsak from LSTS/VUB.

Pablo: The conference topic for this year is "Competing Visions Shared Futures". For outsiders to the digital finance arena, there is a seemingly sense of shared approaches to new developments: from open banking to CBDCs or even cryptoassests regulation. In your view, does reality correspond to this, or is there a global competition over financial standards that shapes the future of digital rights? Do these differences amount to a form of regulatory competition actively shaping financial data infrastructures, and if so, how do distinct data governance models translate into concrete financial governance strategies?

Andres: Finance seems to be a sort of unknown lands for those not familiar with its dynamics; to some extent, even for those of us who have been working in the field for some time it also remains as such. While money and financial transactions have become global and the means used to move value across the world have become common, giving away a sort of shared present and future, reality is far from it.

In this sense, a bank transfer might look like the same from outside but the plumbing used to achieve this is very different depending on where we are located; in some cases, this connection between systems is not possible at all. Perhaps recent years of geopolitical struggle, with tariff wars to actual armed conflicts, have bring this back to the front again but there has always been a constant competition between how to design and govern the financial system. As such, this ongoing battle between nations is mirrored by how money can be moved from one place to the other. For example, the war in Ukraine lead to Russian banks being blocked from accessing the SWIFT network, one of the main communication systems for financial transactions.

Despite these tensions and others, there is a substantial amount of work done by international bodies, such as the Bank for International Settlements or the International Organization of Securities Commissions, to work for shared layers of financial infrastructure or, at least, common standards to ensure interoperability across systems. However, as the era of physically moving money and other monetary tokens has largely been superseded, the transfer of digitized information constitutes the status quo. In this respect, it is only logical that one of the consequences behind this approach is that when information about a natural person is involved, the application of data protection rules becomes a relevant legal and policy matter.

As such, i**n financial services, these competing visions are found in both sector-specific governance schemes but also in how regulatory data governance is construed in a given country**. In this respect, **scholars have identified that the three big approaches to data governance and privacy can also be found in financial services, presenting an interesting overlap between regulatory techniques across different fields.** Namely, the roles of the European Union, the United States and China, each with its own clear data governance formula, are repeated in the field of financial services. This, in turn, causes some frictions with the standardization attempts mentioned above.

For example, we can take open banking and open finance policies and regulations as a clear example of this. For those not aware of them, these solutions imply the possibility of sharing data across different financials service providers for the rendering of alternative products and services. This trend started in the payments sector to enable users to make payments and track them without having to rely exclusively on the entity that keeps an account for them. In this respect, and while most countries have moved forward with this model, the possibilities and limitations emerging from local or regional data protection frameworks have conditioned how this approach takes form. Just to name a concrete debate in this topic, the EU adopted its open banking scheme under the Payment Services Directive 2 and prescribed that any data sharing activity would only take place under the 'explicit consent' from the user; the exact meaning behind this term causes debate among scholars and authoritative bodies as the implications on whether a financial services or data protection law interpretation should take prominence.

Pablo: In your previous research, you've often looked at finance not just as a tool for trade, but as a critical piece of infrastructure for power. If we treat financial data as infrastructure rather than input, who currently sets the terms of access, visibility, and control, and does that leave any meaningful space for newcomers to reshape the system?

Andres: As with any law and technology matter, it is necessary to look beyond what a legal rule says to properly understand a phenomenon. In this respect, **social scientists focused on money and its characteristics have looked beyond its typical functions (namely, store of value, unit of account and means of payment) and view it as a concrete element of exercising power, particularly to convey ideas and allow the free expression of individuals in a market-based socioeconomic paradigm**. For example, contributing to a political party or a religious organization represents the exercise of a fundamental right, be it the expression of political opinions, the right to profess a religious belief, etc.

At the same time, a financial transaction by itself is an informational record that reveals, at least, the identity of two parties, a demonstration of financial capacity or an expression of wealth, the time and date reference and so forth. Moreover, if we add into the mix the factor that financial transactions have been slowly but steady digitized over the last decades, particularly accelerated by the COVID19 pandemic, the persistence of this information and the possibilities of analysing large amounts of information at the same time, puts a lot of pressure on

There has always been a constant competition between how to design and govern the financial system.

the expected responsibilities for those controlling the flow of information/money.

As such, it is critical to understand who and how acts as a gatekeeper within this architecture of visibility. In this respect, we can pinpoint to three main categories of gatekeepers: (i) incumbent financial institutions; (ii) new entrants, such as fintech companies but also BigTechs; and (iii) the government and its different bodies that have some degree of authority.

Legacy banks and other companies have one of the strongest positions out of all these players as people already are engaging with them for their daily activities; these have the largest datasets about users' transactions. This position has been put under 'check' (but not yet in checkmate) by, for example, open banking and open finance policies and regulations that force opening up these dataset to new entrants, who are keenly interested in combining such information with their own datasets and, therefore, blending the borders between financial services and the rest of our societal interactions. In the middle of this intersection, regulatory bodies, policymakers and legislative bodies have to balance between a trilemma of enabling innovation while also securing market integrity but keeping rules relatively simply for their implementation and oversight.

I have left out users on purpose outside of this classification as their voice has been silenced so far in the debate and only given a testimonial place. However, it is also possible to identify some trends that seem to revert this situation, such as the current approach for open finance in the European Union, which relies on certain technological developments, known as permission dashboards. This would act as a sort of personal information management system for users to oversight how their information is moving across the field.

Pablo: As we move toward a "cashless" society, how do we prevent financial infrastructures from becoming a permanent "Surveillance by Design" mechanism for both states and corporations? For example, the European Central Bank promises "controlled anonymity" for the Digital Euro. Is it technically and legally possible to build a shared financial future that respects the anonymity of cash while satisfying the transparency demands of Anti-Money Laundering (AML) laws?

Andres: So far, I have been discussing mostly about data-related issues in the financial services sector. However, another right that should also be taken into account for is the right to privacy. While people might not be so inclined to acknowledge the connection between this right and money, the bond has long been there before our eyes. After all, in a cash-based transaction, in principle, only the person paying and the person receiving the banknotes or coins are aware of the existence of the operation: only they know about the when and the where the transaction took place, the value paid for a seemingly unknown product or service, and even who were involved.

This right to financial privacy has a necessary connection with the function of money as the enabler to exercise other rights. Only when a person is sure that they might not suffer consequences for supporting, for example, a political party as their actions will remain private, they might be willing to act as so. Therefore, any cashless policy and regulatory action taken can be seen, again in principle, as an attack on this paradigm.

However, a concrete limitation should also be factored in this analysis. A cash-based transaction can only get a person so far: the physical elements is both a protection for their privacy but also a limitation for the exercise of their rights. In this respect, the emergence of intermediaries helped to overcome constrains and flourish socio-economic activities at the expense of introducing a third party in financial transactions. At the same time, governments have taken advantage from this by delegating certain oversight and control obligations and powers into these entities, particularly those pertaining to anti-money laundering and counter terrorism financing. Their success, however, has long been criticised in specialized literature with regards to the vast amount of information requested against the actual criminal activities prevented.

In this context, data protection rules can contribute to mitigate this. While private financial institutions have been, to different degrees, held accountable for violations to these rights, the introduction of publicly controlled financial infrastructure to conduct payments shakes the foundations of this analysis. The proliferation of central bank digital currencies (CBDCs) embodies this problem and call for the need of institutional safeguards to prevent an abuse from public bodies and the possibility of holding them accountable. For example, the fragmented nature of the current financial system would be concentrated in single choke points where users cannot escape the control for criminal-related activities and the potential situations for exclusion. We only have to remember the perils that government controlled anti-fraud systems can have on citizens when performing flawed analysis as revealed by the SyRI case in the Netherlands.

In this respect, and while an initial wave of CBDCs projects were focused on delivering a form of digital cash to citizens for retail purposes, current approaches seem to focus on creating a common currency infrastructure settlement layer at central bank level for wholesale transactions. In this respect, the previously identified data governance approaches have a considerable influence on how these projects are being translated into concrete legislation. For example, privacy and data protection concerns in Europe are being contemplated in the discussions about the digital euro project. Some research, as that conducted at the Bank for International Settlements, show that there is potential for privacy-friendly solutions for CBDCs; however, in my opinion, I believe that we still owe a proper discussion about the very necessity of these systems vis-à-vis the existing financial infrastructure.

Pablo: Debates on digital finance tend to focus on payments, banking, and crypto-assets, while adjacent sectors such as insurance, credit scoring, and risk modelling receive less systematic attention. These areas increasingly rely on granular and sometimes cross-sectoral data, including behavioural or mobility data. To what extent do these developments signal a shift in data-driven financial decision-making? And how should we assess their implications for traditional principles such as risk pooling and financial inclusion?

In my research, I often point out that when we treat data as an infrastructure for power, 'inclusion' can quickly become 'predatory inclusion'. This provides another venue for cross-collaboration between fields.

Andres: The adoption of risk-based approaches in regulatory techniques has gained significant traction in the last decades in different fields. However, the conceptualization of risk has not been done in the same manner. For example, financial services have long relied on the notion of market stability to organize how should risk should be managed; with the ability to analyse individuals' cases and their impact on the larger scale, risk might not be pooled anymore but rather isolated and contained. On the other hand, data protection, at least in its European perspective, would be organized around the notion of risk to a right. In the situation of financial services, there have been attempts to introduce elements from one regime into the other by incorporating lessons learnt in one field to the other.

In other words, there is a clear distinction between group or collective approaches on the former with individual-focused approaches on the latter, despite some attempts to bridge between them. Nevertheless, an integral and coherent approach should try to close gaps.

For example, we can take the insurance industry to showcase this tension between legal regimes. The bedrock of the insurance industry has always been risk pooling, a form of social solidarity where the many cover the few, protected by a 'veil of ignorance'. When we introduce granular, cross-sectoral data, we thin that veil. As risk modelling becomes hyper-individualized, and AI can predict a specific individual's risk with high certainty using behavioural data, this risk distribution effectively evaporates. Those who need protection the most are either priced out or 'de-risked' (excluded) entirely because their data doesn't fit the desired profile.

In this new paradigm, insurance and credit aren't just safety nets; they become tools for social engineering. We see this in 'pay-as-you-drive' or 'pay-as-you-live' models, where financial access is conditional on maintaining a specific, data-verified lifestyle. In my research, I often point out that when we treat data as an infrastructure for power, 'inclusion' can quickly become 'predatory inclusion'. This provides another venue for cross-collaboration between fields.

Pablo: CPDP embraces competing visions as a democratic strength. Which overlooked development in digital finance and data governance do you think poses the greatest risk to democracy?

Andres: My reflections have left out on purpose the whole dimension of cryptocurrencies and its strong base of relevant stakeholders as they represent a truly different alternative perspective for understanding the relationship between finance, data protection and privacy. When implemented in proper decentralized and distributed manner, they put forward a vision where certain values, such as data protection and privacy by default and by design, are deeply engrained within the very fabric of these financial infrastructures. With their focus on peer-to-peer interactions, they constitute a paradigm shift that can bring together the far reaching capabilities of data-driven financial services with the level of protection granted by early monetary instruments, such as cash.

At the same time, the key lays in the idea of 'properly implemented' as these technologies are being hijacked by both incumbent financial institutions as well as governments to fit their own agenda. For example, we can take different CBDC projects that are being portrayed as the digital equivalent to cash just because they operate on distributed ledger technologies just like cryptocurrencies. What governments do not tell about this is that these CBDCs are not like the latter as they do grant the same characteristics as cryptocurrencies as the infrastructure layer is not the same. For example, in Bitcoin are no barriers to enter the ledger from any position, beyond meeting concrete technical (and basic) requirements; almost anybody can set a Bitcoin node and have a full copy of its ledger to oversight transactions while at the same time they can just download a wallet to obtain bitcoins on a peer-to-peer exchange. In a CBDC project, only vetted entities can engage with the ledger directly and the distribution of the tokens is channelized through specialized actors.

As such, and in my opinion, the biggest risk to democracy is the marketing by both public and private actors of certain projects as equivalent to technologically beneficial solutions that are designed with data protection and privacy ethos embedded in them from the start. As such, the issue of trust come to the foreground and constitutes the frontier to be explored from a scientific perspective. In other words, whether people are trusting these solutions offered by public and private actors or rather they want to explore alternatives based on truly peer-to-peer paradigms. In this sense, future editions of the conference might prove a valuable venue to start addressing the future of finance. ▪

As such, and in my opinion, the biggest risk to democracy is the marketing by both public and private actors of certain projects as equivalent to technologically beneficial solutions that are designed with data protection and privacy ethos embedded in them from the start.

Dedicated Tracks

With over 120 sessions and more than 500 speakers, CPDP offers a rich programme that can sometimes feel overwhelming. Dedicated Tracks provide orientation through curated pathways across key themes, bringing together panels, workshops, and discussions. Co-developed with domain experts, they foster deeper exchange within and across professional communities. In recent editions, we expanded this approach with new tracks such as Digital Youth Futures, IT Security, and Engineering Privacy and Data Protection, alongside the DPO and Computer Science Tracks. Looking ahead, we are beginning to shape a new track focused on the future of finance, assembling a team to develop it in a meaningful and forward-looking way.

From Past Technologies to Technodiverse Futures

OPINION PIECE

At a recent event dedicated to digital justice, someone asked me: *'Do you know Project Cybersyn? And do you think we could replicate it today?'* This was not the first time I was asked about Project Cybersyn—not even close. The more often someone asks if we could replicate this relatively obscure Chilean project from the 1970s today, the more compelling I find the question. Why does Cybersyn continue to fascinate people, especially in Europe and North America? Why is it viewed as somewhat of a prototype for a progressive technological future?

In 1970, Salvador Allende became the first socialist president of Chile. As he entered into office, he began working on bringing about a socialist transformation within a democratic framework. In order for Allende to pursue this political project, he knew that creating and maintaining a thriving economy was key. Through the nationalisation of the economic sector, the government would be able to control raising industrial production levels. But this transformation would not come easily, as Chile was facing various economic challenges, including rising inflation rates and economic restrictions imposed by the United States.

Among the people tasked with executing Allende's economic policy programme was a young man named Fernando Flores. Trained as an industrial engineer, Flores looked to the then relatively unknown field of cybernetics for inspiration. In cybernetics, Flores found a form of management that balanced centralised and decentralised control, and was thus fully aligned with Allende's socialist values. Through cybernetics, he hoped to organise a participative, decentralising, and anti-bureaucratic form of economic management.

Within a matter of months and with the support of Stafford Beer, a British management consultant, Flores had drawn up the plans for Project Cybersyn. In its entirety, this project consisted of a five-tiered computer system that combined telecommunications networks, a mainframe computer and software. The purpose of the system was to collect, read and analyse up-to-date data from factories across the country. Should any problems arise on the factory floor, this data would enable the government to intervene immediately and ensure the continued production of goods.

On 11 September 1973, a military coup brought a violent end to Allende's government and life. Project Cybersyn was never fully implemented, and it is impossible to know whether the project would have been successful in achieving all of its objectives.

Perhaps it is because of its abrupt and unfinished ending that people today are drawn to Project Cybersyn, that they are tempted to dream about not only what could have been, but also what our lives would look like if we were to replicate it today.

***

In recent years, countless long reads, books and podcasts about Project Cybersyn have appeared in English-language media. I understand where this is coming from, and I share the craving for vision for technology that exist outside the current paradigm of techno-capitalism. Still, I am not sure wether this contemporary infatuation with Project Cybersyn really does us much good. For one, nostalgia is rarely a trustworthy guide for navigating the challenges of the present. But most of all, I think that dreams of replicating Project Cybersyn today are contradictory to the lessons we should actually take away from this project.

Dreams about replicating Project Cybersyn are often underpinned by the assumption that its systems relied on very advanced technologies. This is in part due to the imagery that typically accompanies contemporary retellings of the project's story; photos showing Project Cybersyn's central ops room, which was designed to look cutting-edge and to invoke associations with science fiction.

But while Project Cybersyn was innovative in many ways, it was not, in fact, built using cutting-edge technologies. During the early 1970s, there were no more than 50 computers across Chile. And due to economic restrictions imposed by the US government, the Chilean government was not able to import the component parts it may have wanted to construct computer systems.

In 'Cybernetic Revolutionaries: Technology and Politics in Allende's Chile', Eden Medina provides a detailed historical account of Project Cybersyn. In the book, Medina highlights that the project's technological innovations were only possible thanks to political innovations. What made Project Cybersyn innovative was not necessarily its underlying tech. It was innovative because of the political vision it played a part in executing, and because the project was underpinned by the goals and principles of Allende's political project in every step of its design and implementation. In other words, it showed that technology can be a way for us to see political ideas and goals transformed into practice.

***

Stories about Project Cybersyn often pay a great deal of attention to Stafford Beer, a British cybernetician and close collaborator of Fernando Flores. This is not necessarily a bad thing, as Beer played a pivotal role in the project (I myself am very grateful that I was able to learn a great deal about Project Cybersyn by combing through his personal archive in Liverpool). But it's important to remember that Project Cybersyn is not a story of imported knowledge or technologies. It is the story of a team that was able to be creative with what they had, despite facing heavy restrictions. And while they were not able to use technologies that were cutting-edge, they were able to put them together in ways that had never been seen before.

The value of Project Cybersyn's story lies in the fact that it shows us the importance of localised technologies. In a sense, the project embodies what the philosopher Yuk Hui means by his call for 'technodiversity': a move away from the Western notion that technology is universal and can only evolve in one direction. According to Hui, we have to make room for diverse forms of technology that stem from diverse local knowledge and need.

***

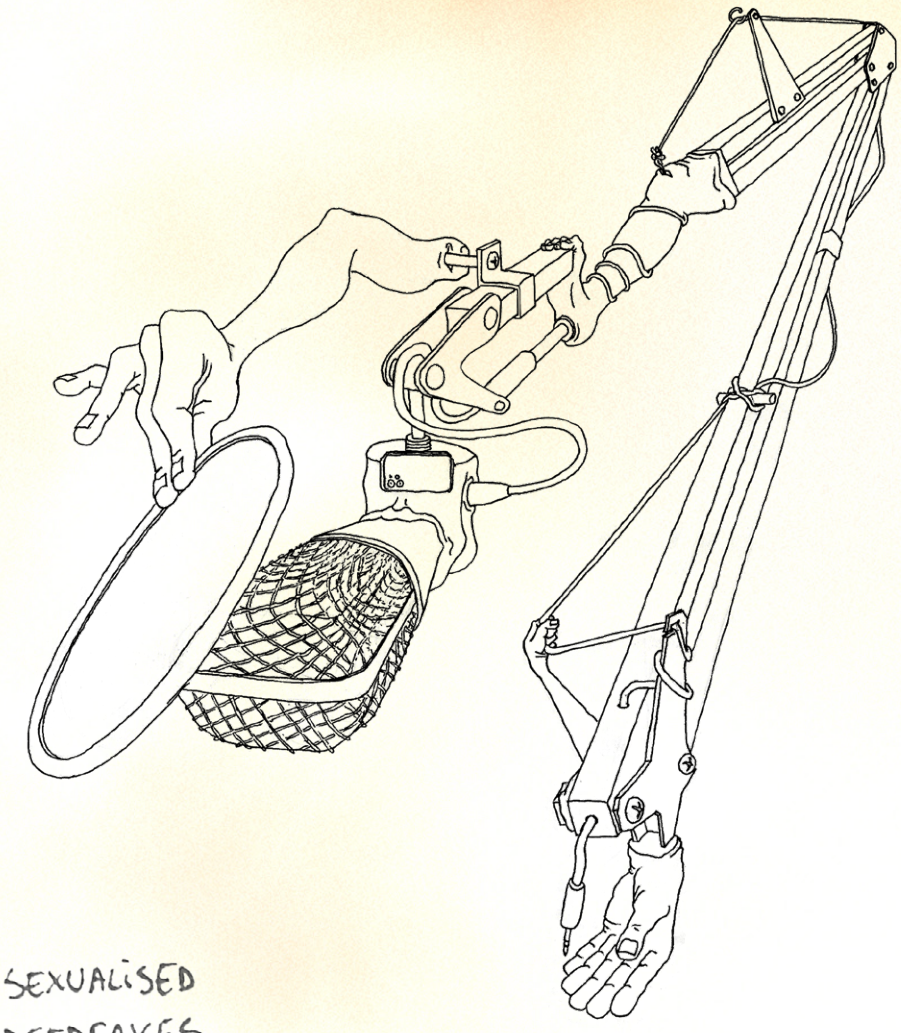
As tempting as it may be, I don't think that we should be modelling our technological future on a technological past. Especially if that past is not even our own. If anything, Project Cybersyn showed that we do not have to follow the technological paths that already exist. Instead, it showed us that we can and should forge our own.

Paola Verhaert

Paola Verhaert is a Brussels-based digital rights researcher and practitioner. She is the author of Technologie is politiek, a philosophical introduction to the concept and practice of digital justice. She was invited to contribute an opinion piece in the context of her participation in the CPDP Culture Club panel, where we bring together After Scarcity - a recent sci-fi video essay by Bahar Noorizadeh tracing Soviet cyberneticians from the 1950s to the 1980s - with a discussion on Project Cybersyn (Thursday 21 May).

CPDP • Live Radio • 3 Days • On-site at CPDP • Live Radio • 3 Days • On-site at CP

AVATAR.FM



- on air 12pm–6.30pm

Avatar.fm gives a voice to the young and new generation of privacy, data protection, AI, and computer science heads, amplifying stories and testimonials of students, junior researchers, artists and activists.

AUTHORITARIAN REGIMES & ABUSE OF DIGITAL SYSTEMS

SEXUALISED DEEPFAKES

SEX WORKERS RIGHTS

FEDIVERSE

PSYCHOLOGICAL EFFECTS OF AI USAGE

POTENTIAL SOCIAL MEDIA BAN IN EUROPE

RE-DESIGNING THE FUTURE

YOUTH MENTAL HEALTH & SOCIAL MEDIA

WOMEN IN GOVTECH

TRANSFEMINIST DIGITAL CARE

VOICE CLONING, INTIMACY & DATA SONIFICATION

DATA FEMINISM

YOUTH MENTAL HEALTH & SOCIAL MEDIA

BEYOND SURVEILLANCE CAPITALISM

CHILDREN'S USE OF GEN AI

Location:
in front of the Grande Halle

photo © Ruben Tsangaris

Check out the programme at www.cpdpconferences.org/avatar-fm

Tune in live at www.gimicradio.com

GIMIC × Privacy Salon

n-site at CPDP • Live Radio • 3 Days • On-site at CPDP • Live Radio • 3 Days • On-

Cinema • 3rd Floor **CPDP** 08.45 -18.45

CULTURE CLUB

Jonathon W. Penney • Marc Silver • Geeske Janßen • Judith Blijden Aurelia Tamò-Larrieux • Leandra Barrington-Leach • Lorenzo Dalla Corte • Ido Sivan-Sevilla • Aleksandra Kuczerawy • Paola Verhaert • Sarah Sharma • Gala Hernández López • Virginia Mahieu • Andrei Zakharov • Tatsiana Ashurkevich • Nora Ni Loideain • Niovi Vavoula • Christopher Docksey • Laura Drechsler • Konrad Kollnig • Simone van der Hof • Stephan Mulders • Anastasia Karagianni • Mark Cinkevich • Alexandre Alaphilippe • Elora Fernandes • Isabela Rosal Santos • Demetra Tzanaki • Paulien Broens • Salomé Lannier • Ava Lee • Gayle Brewer • Sreyan Chatterjee • Sean Mulcahy • Joel Baumann • Laura Därr • Kimon Kieslich • Pia Groenewolt • tba

	08.45 -10.00	10.30 -11.45	11.50 -13.05	14.15 -15.30	16.00 -17.15	17.20-18.40
WED 20		10.00 - 11.15 *ARTIST SCREENING + DISCUSSION* **Artistic Encounters with Human–AI Relationships**	*BOOK SESSION* **CHILLING EFFECTS, REPRESSION, CONFORMITY, AND POWER IN THE DIGITAL AGE**	*BOOK SESSION* **INSUFFERABLE TOOLS – FEMINISM AGAINST BIG TECH**	*SCREENING* **MOLLY VS THE MACHINES**	*DISCUSSION* **MOLLY VS THE MACHINES**
THU 21	*BOOK SESSION* **THE DARK SIDE OF ACADEMIA: COMPETITION, INEQUALITY, AND VIOLENCE IN THE IVORY TOWER**	*BOOK SESSION* **EU DATA PRIVACY LAW AND SERIOUS CRIME**	*ARTIST SCREENING + DISCUSSION* **LIKE MOTHS TO LIGHT + Cognitive Warfare**	*ARTIST SCREENING + DISCUSSION* **AFTER SCARCITY + PROJECT CYBERSYN**	*BOOK SESSION* **THE RUSSIAN CYBERPUNK. HOW THE KREMLIN BUILDS A DIGITAL GULAG — AND WHO IS RESISTING IT**	*DISCUSSION* **IVIR SCIENCE FICTION & INFORMATION LAW WRITING COMPETITION**
FRI 22	*WORKSHOP* **ALGO-RHYTHMS: HOW DATA-DRIVEN SYSTEMS PERPETUATE UNNECESSARY SUFFERING**	*SHORTFILM PROGRAMME* **ONSET, CHRONOSPHERE, THE PEGASUS STORIES**	*DISCUSSION* **OSINT AS ARTISTIC AND LEGAL TOOL FOR RESISTANCE**	*BOOK SESSION* **THE APP ECONOMY: MAKING SENSE OF PLATFORM POWER IN THE AGE OF AI**	*DISCUSSION* **CODE: Reclaiming Digital Agency**	*SCREENING* **DISCO & ATOMIC WAR**

Thursday Lunch session
13.05 - 14.15

BOOK SESSION
GENERAL LAW ON THE PROTECTION OF PERSONAL DATA/ *LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS COMENTADA*

MORE INFO: CPDPCONFERENCES.ORG

Call for Chapters — Join the Next Volume of the CPDP Book Series

Published since 2009, the Computers, Privacy and Data Protection series brings together academics, lawyers, practitioners, policy-makers, industry, and civil society in the spirit that defines CPDP itself. We are now inviting contributions to Volume 19: Data Protection, Privacy and Artificial Intelligence: Competing Visions Shared Futures.

This volume grows out of CPDP 2026 and its central question: who gets to define the digital future, and on whose terms?

Submissions should engage broadly with the themes explored during this year's conference.

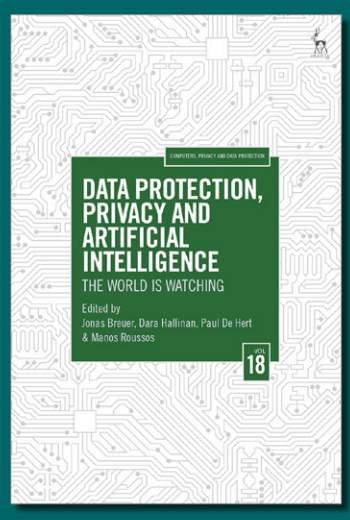
Academic contributions should be between 5,000 and 12,000 words and will undergo a blind peer-review process. We also welcome shorter pieces for the Practitioners' Corner — accessible reflections from professionals directly engaged with the issues we explore at the conference.

The volume will be ready before CPDP 2027.

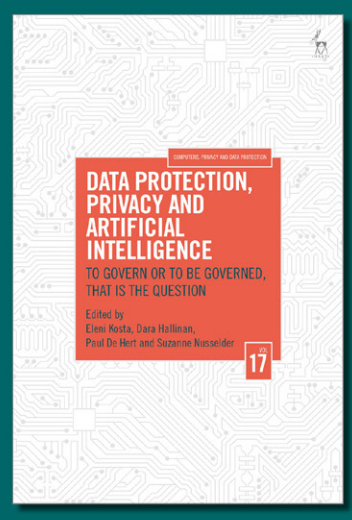
COMPUTERS, PRIVACY AND DATA PROTECTION

Series Editor: Paul De Hert

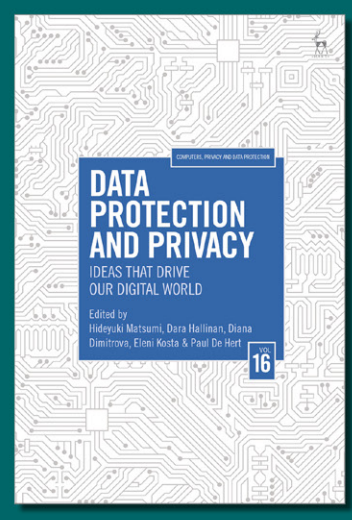
Cutting-edge research from the world-leading Computers, Privacy and Data Protection conference.



Apr 2026 | RRP: £55

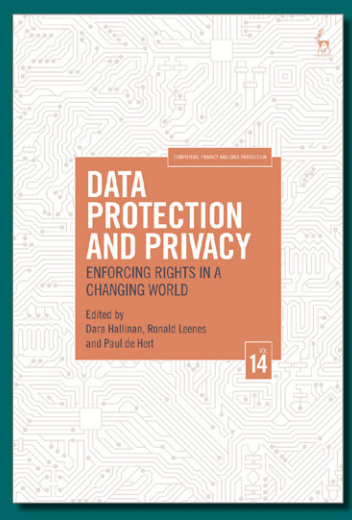


May 2025 | RRP: £55

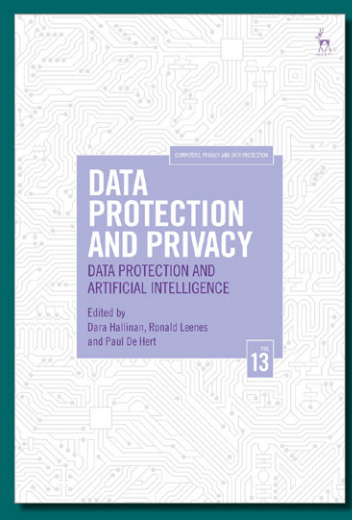


May 2024 | RRP: £60

May 2023 | RRP: £60



Dec 2021 | RRP: £65



Jan 2021 | RRP: £70

Interested in contributing a chapter to **Volume 19**?
Contact **Jonas Breuer** at **jonas@privacysalon.org**

Discover the full series at **bloomsbury.com/cpdp**

HART

Organisation of CPDP

Directors

- Paul De Hert (LSTS, VUB, Tilburg University TILT))
- Barbara Lazarotto (CPDP - Belgium)
- Thierry Vandenbussche (Privacy Salon) Interim Director
- Jonas Breuer (CPDP - Belgium) Interim Director

Core Programming Committee

- Jonas Breuer (CPDP - Belgium)
- Barbara Lazarotto (CPDP - Belgium)
- Dara Hallinan (FIZ Karlsruhe GmbH - Leibniz Institute for Information Infrastructure)
- Rebeca Bacci (Privacy Salon)

Extended Programming Committee

- Luca Belli (Center for Technology and Society at FGV Law School)
- Ronald Leenes (TILT, Tilburg University)
- Dennis Hirsch (Ohio State University Moritz College of Law)
- Malavika Jayaram (Digital Asia Hub)

Panel Coordinators

- Achim Klabunde (Deutsche Vereinigung für Datenschutz DVD)
- Adriana Schnyder (Digitus Legal)
- Alessandra Calvi (EUTOPIA PhD Fellow)
- Anastasiia Adeeva (Apogado)
- Andrés Chomczyk Penedo (ICAI-ICADE)
- Camilla Silvestri (KU Leuven)
- Carissa Anderson (5Rights Foundation)
- Francesca Tassinari (Universidad del País Vasco)
- Guillermo Lazcoz Moratinos (CIBERER)
- Ine van Zeeland (imec-SMIT, Vrije Universiteit Brussel)
- Isabel Sola Sanchez (NTT DATA, Inc.)
- Isabela Xavier Gonçalves (Vrije Universiteit Brussel (VUB) - Belgium)
- Josipa Špoljarić (Privacy for All)
- Laura Centeno Casado (CSIC)
- Liubomir Nikiforov (EDHEC Business School)
- Naira López Cañellas (Technological University of Dublin)
- Nonso Anyasi (Open Universiteit Nederland)
- Oğuzhan Yeşiltuna (Vrije Universiteit Brussel (VUB) - Belgium)
- Virginia Marinelli (European Union Agency for Asylum – EUAA)
- Wenkai Li (LSTS (VUB))

Scientific Advisory Board

- Gloria González Fuster (LSTS/VUB - Belgium)
- Rocco Saverino (ALTEP DP - Belgium)
- Franziska Boehm (FIZ Karlsruhe GmbH - Leibniz Institute for Information Infrastructure - Germany)
- Eleni Kosta (Tilburg University - Tilburg Institute for Law, Technology and Society (TILT) - Netherlands)
- Ian Brown (Fundação Getulio Vargas Law School, Visiting Prof - Spain)
- Willem Debeuckelaere (Former President, Belgium Privacy Commission)
- Ronald Leenes (TILT, Tilburg University)
- Paul De Hert (LSTS, VUB)
- Dave Lewis (ADAPT Centre, Trinity College Dublin - Ireland)
- Claudia Diaz (Nym Technologies SA)
- Jo Pierson (VUB)
- Michael Friedewald (Fraunhofer ISI - Germany)
- Kristina Irion (Institute for Information Law (IViR) - Europe)
- Charles Raab (University of Edinburgh - United Kingdom)
- Marit Hansen (State Data Protection Commissioner of Land Schleswig-Holstein)
- Marc Rotenberg (Center for AI and Digital Policy (CAIDP) - International)
- Mireille Hildebrandt (LSTS (VUB))
- Ivan Szekely (Central European University/ Blinken OSA Archivum - Hungary)
- Dennis Hirsch (Ohio State University Moritz College of Law)
- Gus Hosein (Privacy International - United Kingdom)
- Frederik Zuiderveen Borgesius (Radboud University - Netherlands)
- Els Kindt (CiTiP)

Former Members Scientific Advisory Board

- Eva Lievens (Ghent University - Belgium)
- José Luis Piñar (Ada Lovelace Institute - International)
- Serge Gutwirth (Lstst – VUB)
- Marc Langheinrich (Università della Svizzera italiana)
- Bert-Jaap Koops - Tilburg University
- Caspar Bowden (1961 – 2015)

Oversight Committee

- Marc Rotenberg (Center for AI and Digital Policy (CAIDP) - International)
- Thibaut D'hulst (Keystone Law)
- Christel Simons (Privacy Salon)

Privacy Salon

- Thierry Vandenbussche
- Jonas Breuer
- Barbara Lazarotto
- Karin Neukermans
- Christel Simons
- Ferre Vander Elst
- Birte Vingerhoets
- Raquel Nogal Santamaria
- Rebeca Bacci
- Melis Gurses
- Tammo De Vries

Logistics and Registration

Medicongress Services

Noorwegenstraat 49
9940 Evergem, Belgium

Phone: +32 (09) 218 85 85
www.medicongress.com

Auvicom

Suikerkaai 40d
Zone 3a, 1500 Halle, Belgium

Phone: +32 2 2 380 10 44
www.auvicom.be

Studio Pompelmoes

hello@bartvandersanden.be
www.studiopompelmoes.be

Josworld

Rue de Laeken 99
1000 Brussels, Belgium

jos@josworld.org
Phone: +32 2 411 20 54
www.josworld.org

Thank you

This conference would not be possible without the industrious support of Els Vertriest, Sofie Philips, Ariëlle Desmet, Astrid Dedrie and all Medicongress staff, as well as the technical support of the wonderful people at Auvicom, in particular Cedriek Stoffels and Mats Laermans . Also, for the mastery of our caterer ARTFOOD (represented by Steven Jacobs), a big thank you to their team for providing such delicious food! A big thank you to Jean Vandamme and Natasha Rosar for the great partnership between CPDP and Maison de la Poste. A big thank you to Marine Renwart and her colleagues from Le Baixu, and Danai Vafiadis and the staff from Brasserie de la Senne who are hosting the Mozilla Party on Thursday.

To the Privacy Salon team for all the great work behind the scenes of CPDP: directors Barbara Lazarotto, Thierry Vandenbussche and Jonas Breuer and the team: Karin Neukermans, Christel Simons, Ferre Vander Elst, Birte Vingerhoets, Raquel Nogal Santamaría, Melis Gürses , Tamo De Vries and Rebeca Bacci. Also, a big thank you to the Privacy Salon board members for their guidance: Paul De Hert, Ulrich Seldeslachts, Marleen Wynants and Ana Pop Stefania.

Many thanks also to all student volunteers of the interdisciplinary Research Group on Law, Science, Technology & Society (LSTS) of the Vrije Universiteit Brussel (VUB) and other student volunteers who have done a wonderful job, and a particular thanks to Alicja Joanna Kucharska from Tilburg University who very capably managed the call for papers and academic sessions.

Special thanks to all Workshop Organisers for enriching the programme with their dynamic, hands-on sessions.

A big thank you to Thierry Vandenbussche and Ferre Vander Elst, who commissioned the cover artwork by Simon Denny for CPDP 2026 and brought 'Competing Visions Shared Futures' into the CPDP sphere. Denny is not the only artist at the conference, the CPDP Culture Club is full of inspirational artists and creatives who we would like to thank for their time and generosity. The CODE project brings an interesting selection of artists and non-artists who are collaborating and presenting projects together at the conference. Thanks to the collaboration with Impakt, Werktank, Kunsthal Mechelen, Arjon Dunnewind, Pietro Ballero and everyone involved in CODE. As well as Project Sentiment represented by Joel Baumann, Laura Därr, Elko Braas from Kunsthochschule Kassel. With Avatar.fm we make live radio from the conference for the second time, this year with radio station GIMIC and the professional guidance by Robin Feron and Arthur Van Craen.

Thank you, Laura Drechsler, Aurélia Tamò-Larrieux, Irène Kamara, Anastasia Karagianni, project SENTIMENT, People vs. Big Tech for helping to organise the fourth edition of the CPDP Book Club. Thank you, Iris Stroep, from the local Antwerp bookshop De Groene Waterman for bringing an excellent selection of books to CPDP 2026.

Thank you to Gloria Gonzalez Fuster, Peter Dunne, Itxaso Dominguez de Olazabal, Sibel Top, Yin Harn Lee, Chloe Berthelemy and Andreea Belu for co-organising the pre-event The Digital Rights Lounge:LGBTIQ+ Rights in the Digital Age, which is also powered by the Privacy Camp.

A big thank you to Tanja Lange, Heloise Guarise Vieira, Mélissa Rossi, Thibauld Feneuil and Matthieu Rivain from the PQCSA consortium for co-organising the pre-event Workshop on post-quantum cryptography.

Thank you to Sophie Stalla-Bourdillon and the Brussels Privacy Hub for helping with making the CPDP Opening Night a strong and thought-provoking start to the week—and to the Brussels Privacy Hub and Privacy Salon for sponsoring the adjoining cocktail. We also warmly thank our partners for supporting the evening cocktails on Wednesday, Thursday, and Friday.

CPDP is grateful towards Jonas Breuer, Dara Hallinan, Paul De Hert,and Manos Roussos, the reviewers for their invaluable time as well as Roberta Bassi and the team at Hart Publishing for editing and publishing the conference book. Most of all, thank you to the authors for their high quality contributions, which are written proof of what CPDP is: an ambitious bet to knock down barriers among disciplines, think together, innovate, and leave a mark in the privacy and data protection world.

Thank you also to our reviewers for the CPDP 2026 call for papers, all those involved in the process leading to the CPDP 2026 conference book, and the reviewers for the academic sessions: Hiroshi Miyashita, Simone van der Hof, Jacopo Piemonte,, Franziska Boehm, Charles Raab, Lina Jasmontaite, Mistale Taylor, Joseph Savirimuthu, Nicolo Zingales, Gabriela Zanfir Fortuna, Sascha van Schendel, Jef Ausloos, Mattis van'tSchip, Pawel Hajduk, Shweta Degalahal, Michael Czerniawski, Anastasia Karagianni, Ronald Leenes, Elena Petkovska, Pier Giorgio Chiara, Iris Xu, Sofia Santinello, Giorgio Monti, Henry Tari, Britta van Bussel, Marc van der Ham, Abdullah Elbi ,Stephan Mulders, Alice Palmieri, Vlada Druta, Ahlam Barnoussi, Maša Galič, Pratiksha Ashok, Andrés Chomczyk Penedo, Manos Roussos, Pratham Ajmera, Nathan Genicot, Michael Friedewald, Stephanie von Maltzan, Ine van Zeeland, Arnold Roosendaal, Gergely Biczok, Inge Graef, Raphael Gellert, Alessandro Mantelero, Max Van Iersel, Shakya Wickramanayake, Colette Cuijpers, Tal Zarsky, Diana Dimitrova, Alexandra Ziaka, Dennis Hirsch, Eleni Kosta, Jo Pierson, Bettina Berendt, Elisa Orru (S), Konrad Kollnig, Pia Groenewolt

We are grateful to our dedicated track curators of the Data Protection Officer (DPO), Digital Youth Futures, IT Security and Engineering Privacy and Data Protections tracks for their expert advice and availability throughout the year when completing the CPDP Tracks. Thank you, Peter Berghmans, Jolien Ghyselinck, Sophie Stalla-Bourdillon, Bárbara da Rosa Lazarotto, Franziska Boehm, Thilo Gottschalk, Stephanie Maltzan, Jaap-Henk Hoepman and Marit Hansen.

Additionally, we would like to thank all the panel liaisons for facilitating communication between the Programming Committee and the panel organizers. In particular Achim Klabunde, Adriana Schnyder, Alessandra Calvi, Anastasiia Adeeva, Andrés Chomczyk Penedo, Camilla Silvestri, Carissa Anderson,Francesca Tassinari,Guillermo Lazcoz Moratinos, Ine van Zeeland,Isabel Sola Sanchez, Isabela Xavier Gonçalves, Josipa Špoljarić, Laura Centeno Casado, Liubomir Nikiforov, Naira López Cañellas, Nonso Anyasi, Oğuzhan Yeşiltuna, Virginia Marinelli, Wenkai Li.

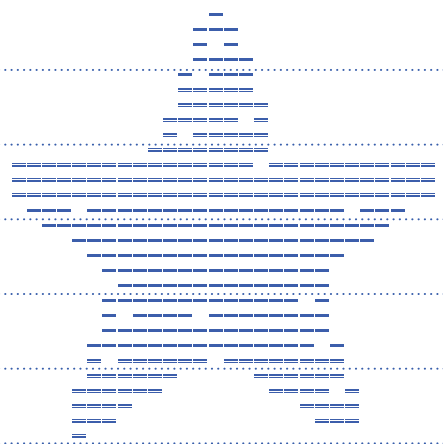
Furthermore, we would also like to thank Raquel Nogal Santamaría for her excellent coordination of the conference rapporteurs. We are also grateful to the rapporteurs themselves: Andrés Chomczyk Penedo, Jakub Misek, Mattéo Bard, Megan Hadasa Leal Causton, Pia Groenewolt, Sruthi Vanguri, Thiago Guimaraes Moraes, Kimmy Shah and Ting-Yu Yu.

A special word of gratitude goes out to Bart Vander Sanden, our web-master, whose quality work is evidence in itself, and who we have additionally gotten to know as a hands-on and energising addition to the CPDP team.

And of course, to the CPDP Scientific Advisory Board who steer and ensure the academic rigor of the conference programme. As well as the newly established Oversight Committee who is the new guardian of values and integrity and the complaint body of CPDP Brussels. Last but not least, CPDP 2026 would like to thank all sponsors, conference partners, event partners, moral supporters and media partners for their generous support and everyone who has approached us with new ideas and topics for panels. Without you, CPDP 2026 would not have been possible!

Notes

Notes



Notes

Sponsors 2026

Partners 2026

Panel Organisers

Media Partners

Moral Supporters

Conference Partners

CPDP.ai sponsors are organisations committed to dialogue around privacy, data protection and new digital technologies. Their contributions help to make CPDP into a trusted, quality conference that attracts participants from all over the globe. No more than 49% of the costs for the conference is covered by private enterprises, ensuring that commercial CPDP sponsors maintain an exclusive position in the privacy and data protection community.