

Privacy Camp 26

Programme

Streamed

Salle des Arches

Boudoir

Salon

Le Grenier

08:30 - 09:30

Registration & coffee

09:30 - 10:10

Opening & Keynote

10:10 - 11:10

Tech sovereignty for whom? Power, war & resistance in Europe (panel)

Resisting Europol & the new age of digital policing in Europe (panel)

Community infrastructure clinic: diagnosing dependencies & designing digital self-determination (workshop)

11:10 - 11:25

Coffee break

11:25 - 12:30

Decentering 'Tech Sovereignty': algorithmic warfare, civilian harm documentation, & digital self-determination in the Global South (panel)

Mobilising across struggles - resisting border infrastructures, militarism & surveillance (workshop)

Encryption in practice: feminist strategies of self-resistance (workshop)

AlgoDance session 1 (workshop)

12:30 - 13:45

Lunch

13:45 - 15:00

EDPS - Civil society summit: safe by design, not by exclusion: reclaiming our digital futures (fishbowl)

From cobalt to code: community self-determination in the AI supply chain (screening & panel)

Building power through strategic litigation: defending LGBTIQ+ rights in digital spaces (workshop)

15:00 - 15:15

Coffee break

15:15 - 16:15

From posts to power: how digital platforms are reshaping domestic work & labour rights in Africa (panel)

After the abyss (screening & panel)

From surveillance to ecosystems of care: How to challenge narratives on the use of technology in alternatives to detention & center agency & rights (workshop)

AlgoDance session 2 (workshop)

16:15 - 17:00

Closing

17:00 - 18:30

Apero & snack

Privacy Camp 26

Tech sovereignty for whom? Power, war & resistance in Europe

10:10 - 11:10

Streamed

Salle des Arches

Panel

Organiser:

- European Digital Rights (EDRi)

Moderator:

- Jan Penfrat, EDRi

Speakers:

- Dr. Corinne Cath, Head of Digital, Article 19
- Alex Lutz, Advocacy Manager, Data for Good
- Sarah Chander, Director, Equinox
- Cyrielle Chatelain, Member of the French national Parliament, President of the group 'Écologiste et Social' & Rapporteur for the French National Assembly's Committee of Inquiry on Structural Dependencies & Systemic Vulnerabilities in the Digital Sector & the Risks to France's Independence

In June 2026, the European Commission released its Tech Sovereignty package, aiming to increase EU's independence from foreign technology providers, mostly US Big Tech companies, throughout the supply chain (chips, cloud infrastructures & AI).

This proposal showcases the EU's political ambition to become an "AI continent", imposing an "AI first" principle & embedding AI in key economic sectors as well as in public services. This agenda translates into an aggressive industrial policy promising to pump hundreds of billions of euros into data center infrastructures, cloud service providers, AI systems & Gigafactories, as well as tearing down the remaining barriers to access data for AI development.

Europe is turning a highly speculative forecast of future AI demand into a political justification for a large-scale build-out of computational, energy & digital infrastructure, while simultaneously reorganising public spending around defence, border control & security. All the while, the sovereignty package falls short in challenging incumbent technology actors over the European market & Member States.

Local communities & social movements are increasingly mobilising, across Europe, to resist a data centre build-out driven by geopolitical & military imperatives, corporate investment strategies & state security agendas.

Who gets to benefit from the tech "sovereignty" discourse, when more compute capacity is treated as an unquestionable public necessity & when its allocation is left to big tech alone? How can we challenge & reframe the narrative from 'sovereignty' without democratic control to 'digital self-determination' for all?

The first part of this panel will explore how Europe's current industrial strategy threatens the livability of our environment & biodiversity, undermines hard-won rights & freedoms protections, reinforces the wealth & power of US Big Tech & shareholders, deepens social & racial inequalities, enables militarisation & warfare, & worsens geopolitical tensions in the Global South, where raw materials are extracted. In the second part, we will look to identify the building blocks of a rights-centered, care-based vision for digital self-determination.

Privacy Camp 26

Resisting Europol & the new age of digital policing in Europe

10:10 - 11:10

Boudoir

Panel

Organiser:

- Front-LEX/Statewatch UK

Moderator:

- Romain Lanneau, Front-LEX/Statewatch UK

Speakers:

- Chloé Berthélémy, EDRI
- Coline Schupfer, Surveillance Resistance Lab
- Juraj Sajfert, VUB, Postoc Researcher

The most impacted by digital policing have the least access to digital rights. Law enforcement & migration authorities run technological experiments with little oversight & with few to no penalties when they are found to violate the law. EU rules have crafted large exemptions in the field of data protection for law enforcement. The exceptions for prohibition & oversight on high-risk AI technologies in the AI Act are a good illustration. Police are self-monitoring while Data Protection Authorities have been averse to political backlash & timid in using their corrective powers against law enforcement.

Europol is the best illustration of this tendency in Europe. The agency built, for years, parallel systems & ran automated profiling technologies without control. It processes data on people not suspected of any crimes, including migrants, asylum seekers & human rights defenders. The third reform of the agency in four years proposes to reward the EU police agency by doubling its budget & workforce. The Commission wants to make it the indispensable cog in every police investigation across Europe by betting on AI & on the mandatory exchange of information between national authorities & the EU agency. The reformed regulation aims to deregulate & eliminate "administrative burden" while serving as the preferred gateway for private parties to develop & experiment with digital policing.

In the United States of America, the Immigration & Customs Enforcement agency is polarising attention after deporting mass numbers of people using violence & technologies. This is not happening in a vacuum & comes from years of collaboration between the tech industry & the Department of Homeland Security on national security & terrorism.

Individuals have been asked to walk a long & tightrope to access their rights to privacy & data protection against law enforcement authorities. Big data policing has worsened this delicate balance & the overall secrecy. Front-LEX launched an innovative litigation to compel the EDPS to act & to ban parallel processing systems at Europol, asking what individuals & impacted communities can do to resist mass surveillance & digital policing through the court. In the USA, inspiring local resistance with communities seeks to challenge the collaboration between tech oligarchs & the state. Today's discussion needs to be not only about resisting deregulation but also about what future alternatives to propose to digital policing.

Privacy Camp 26

Community infrastructure clinic: diagnosing dependencies & designing digital self-determination

10:10 - 11:10

Salon

Workshop

Organiser:

- Free Software Foundation Europe

Facilitators:

- Marta Andreoli, FSFE
- Sofía Aritz, FSFE

Community Infrastructure Clinic is a participatory workshop that invites participants to become "digital infrastructure doctors." Rather than focusing on technology as an abstract concept, the workshop explores how everyday community practices: from preserving local knowledge to coordinating volunteers or accessing essential services, depend on digital infrastructures that are often invisible until they fail. It asks how communities can build & govern digital infrastructures that support collective care & participation without creating new forms of dependency, surveillance or exclusion.

Working in small groups, participants receive a fictional "patient file" describing a community, such as a botanical club preserving local ecological knowledge, a rural village coordinating emergency support, or a migrant association helping newcomers access financial services. Each community faces a different "symptom": a cloud archive locked into a proprietary ecosystem, a communication network dependent on a single messaging platform, or access to essential services restricted to specific operating systems. These scenarios illustrate how decisions about software, platforms & infrastructures shape communities' ability to retain control over their technology, data & participation.

Participants first bring their community to life by mapping the knowledge, relationships & digital practices that sustain it, drawing on their own lived experiences & place-based understanding. They then diagnose the hidden dependencies embedded in these infrastructures & examine how proprietary platforms, closed ecosystems & vendor-controlled services can undermine communities' autonomy & ability to make collective technological choices.

Building on the principles of the Free Software Foundation Europe's Device Neutrality campaign, participants collaboratively develop a "treatment plan" for healthier digital infrastructures. Rather than promoting specific technologies, the workshop explores how communities can build infrastructures where people are free to choose the devices & software they use, where different services can work together instead of locking users into a single provider, & where communities (not platform vendors) can collectively decide how their data & infrastructures are governed... using Device Neutrality, interoperability, self-hosting & community governance as design principles to shape technologies according to their own needs.

By moving from community practices to technological dependencies & finally to collective redesign, the workshop explores how digital self-determination can emerge through community innovation. It contributes to the conference theme by inviting participants to imagine community-led infrastructures that strengthen privacy, collective agency & democratic participation while reducing dependence on dominant platforms & extractive digital ecosystems.

Privacy Camp 26

Decentering 'Tech Sovereignty': algorithmic warfare, civilian harm documentation, & digital self-determination in the Global South

11:25 - 12:30

Streamed

Salle des Arches

Panel

Organiser:

- Ali Shehab, independent

Moderator:

- Ali Shehab, civil society/lived experience with hands-on data collection & archiving of civilian harm

Speakers:

- Dina Abi Saab, president of the Guild of Journalists accredited at the UN, Geneva
- Ayman Sorour, founding executive director of Protection Against Armaments & Consequences (PAC), working on humanitarian disarmament across the Middle East & North Africa
- Alyna Smith, Equinox

The current European public debate on "Tech Sovereignty" frequently treats technology as a sanitised geopolitical asset. However, as the 2026 Privacy Camp call notes, digital technologies are actively used to experiment, target, & kill people in contemporary conflicts like the war in Lebanon. This panel directly challenges the EU's deregulatory push (such as the AI Omnibus) by centering a grounded, lived experience of algorithmic warfare from the Global South. The session centers on the case of Ali's brother Mohamad Shehab (journalist & drone operator) & his brother's four-year-old daughter Taline, who were killed on March 12, 2026, in an Israeli airstrike in Aramoun, Lebanon. Military statements confirmed they were not the intended targets—they were the "outcome" of an automated, AI-assisted targeting system designed to accelerate lethal decision-making at scale.

This tragedy highlights a profound systemic failure: while AI marketing promises "precision," in practice, it yields "cognitive offloading" & efficient civilian slaughter. When European institutions consider stripping away human rights safeguards under the guise of geopolitical competitiveness, they isolate themselves from the deadly testing grounds where these technologies are deployed. Led by Ali Shehab, an organisational psychologist, OSINT strategist, & the brother of the victim, this panel will unpack the reality of "trauma as an archivist". It will explore how victims from the Global South are forced to become the digital historians of their own tragedies to preserve evidence according to international standards.

The panel will address critical intersections of Privacy Camp 2026's political vision: Military Use & Deregulation: How the normalisation of military AI & automated targeting undermines data protection frameworks & accountability mechanisms. Transnational Solidarity: How grassroots open-source intelligence (OSINT) networks & civil society bridge institutional weaknesses to preserve evidence. Challenging "Sovereignty": Redefining digital self-determination not as state-level market dominance, but as the community's collective power to refuse, audit, & prosecute algorithmic harm. By connecting lived experience with forensic data collection & strategic litigation, this session moves beyond abstract policy speak to demand a regulatory framework that treats human rights not as barriers to competitiveness but as non-negotiable boundaries against digitized violence.

Privacy Camp 26

Mobilising across struggles - resisting border infrastructures, militarism & surveillance

11:25 - 12:30

Boudoir

Workshop

Organiser:

- Border Violence Monitoring Network

Facilitators:

- Pauline Fritz, Research & Advocacy Coordinator, Border Violence Monitoring Network
- Tristan Solf, Researcher, Border Violence Monitoring Network

Drawing from the insights of the Infrastructuring Nature research project, conducted by the Border Violence Monitoring Network, alongside Border Forensics & many other organisations, this workshop explores how research & movement knowledge can contribute to building connections between struggles that are often addressed separately: environmental destruction, anti-militarism, border violence, digital surveillance, & community organising. The workshop starts from the recognition that through recent decisions in EU migration & security policy border regimes, military infrastructures, & digital technologies are increasingly interconnected. At the Turkish-Iranian border, BVMN research shows how EU funding drives a destruction of local livelihoods & criminalisation of movement & deaths & disappearances as a result of border infrastructures. Moreover, EU border infrastructures frequently fragment protected wildlife & habitats in Croatia & Hungary. The intensification of border violence, surveillance, ecological destruction & the impact on local communities as a result of the EU border regime are rendered increasingly invisible through increased secrecy around border surveillance & the construction of the image of a "seamless" EU border.

The workshop asks: How can we connect the findings of research such as Infrastructuring Nature to broader movements & collective action? How can we move from documenting harms towards building shared strategies of resistance & mobilisation? What narratives, relationships, & forms of solidarity are needed to connect struggles across different movements & contexts?

Following a short introduction to the research, facilitators will present a small number of concrete cases illustrating how border infrastructures, militarisation, digital technologies, & environmental destruction intersect at EU external & externalised borders. Participants will first be invited to reflect individually on these cases, considering what forms of harm, power, resistance, or inequality they recognise from their own work or personal experiences. They will then work in small, mixed groups to map connections between the concrete cases presented as well as participants' own knowledge on personal experiences on digital policy & anti-militarisation, border justice, & resistance to environmental destruction & capitalist exploitation. The groups will then move from identifying connections to exploring possibilities for collective mobilisation. What lessons can be shared between environmental justice, migrant justice, anti-militarist, labour, & digital rights movements? What challenges are shared across these struggles? What strategies or forms of resistance might be transferable? Where do existing alliances or forms of cooperation already exist? What opportunities exist for stronger alliances & collective mobilisation?

The session will conclude with groups collectively producing a visual map of the connections they have identified & a small number of concrete ideas for future cooperation. Through participatory mapping & small-group discussions the workshop aims to create a space for exchange, stronger alliances & collective mobilisation.

Privacy Camp 26

Encryption in practice: feminist strategies of self-resistance

11:25 - 12:30

Salon

Workshop

Organiser:

- Féministes contre le cyberharcèlement, France

Facilitators:

- Imène El Kadouri
- Laure Salmona

Encryption is often framed as a technical issue reserved for cybersecurity experts &, in recent legislations, reduced to politically motivated debates about online child safety. But for those facing harassment, surveillance, repression or other forms of digital violence, encryption is neither just a technical matter nor an option : it is essential to safely exist, communicate & organise online. At a time when policymakers, including the EU, increasingly instrumentalise debates around online anonymity & encryption, it is more important than ever to recognize these as feminist issues. Beyond technical expertise & political debates, encryption is deeply tied to privacy, autonomy & self-determination. It creates the conditions for people to freely communicate, organise, seek support, & build collective power with control over who can access their conversations & private information.

For feminist organising, encryption is a tool of collective safety & solidarity, enabling young girls, women, LGBTQ+ communities & individuals facing systemic oppression to access information, express their opinions & their identities, share their experiences & amplify voices too often silenced. That is precisely why encryption is to be considered when reflecting on "the future of communities of digital self-determination" : how can we address technology-facilitated gender-based violence (TFGBV) without weakening the privacy & safety of those most affected by it?

Through this workshop, we will explore concrete examples in which encryption helps feminism & identify actionable strategies that integrate privacy into feminist & empowering movements. No coding, cryptography or hacking skills required!

Privacy Camp 26

AlgoDance session 1

11:25 - 12:30

Le Grenier

Workshop

Facilitators:

- Marit Hoefsloot
- Julie van Essen

Algodance is a speculative installation that offers dance as an alternative communication form to undermine the censorship of Meta's algorithms. Meta platforms are highly controlled digital spaces, where people can come together and interact, but only under strict surveillance and censorship. We desire digital public spaces where marginalised groups can freely convene and communicate, outside of Big Tech's restrictive policies and content formats. By using Algodance, words that are often banned or shadowbanned can be communicated through the language of dance. These words are created for and by queer marginalised communities, and the visitors are encouraged to add their own encoded dance moves to the dictionary during the showcase.

Algodance is a speculative interactive installation, developed during the CODE programme at IMPAKT, that turns dance into an encoded language, built by and for queer and marginalised communities to communicate past the censorship of Meta's algorithms. It offers a case study for this year's question: what does digital self-determination look like when the infrastructures we depend on are neither neutral nor accountable to the communities they claim to serve?

Meta's platforms function as de facto public squares, yet moderation on them is opaque, biased, and effectively unaccountable. This is not speculation: a Dutch class-action lawsuit, filed in May by Bureau Brandeis and Bits of Freedom on behalf of organisations including The Queer Agenda, COC Netherlands, and several queer nightlife and art collectives, alleges that Meta's down-ranking and censoring of LGBTQIA+ content breaches European fundamental rights law, the DSA, the GDPR, and Dutch anti-discrimination law. Algodance responds to this not by demanding better access to existing platforms, but by building an alternative: a living, community-authored "Dance Dictionary" that lets people encode and decode meaning through movement, expanding with every new contributor. These movements can be used to communicate (shadow)banned content on Meta platforms, while subverting its biased moderation practices.

This workshop proposal asks what happens when we treat the body, rather than a server, as infrastructure. It also extends the conversation beyond the digital: physical public space is undergoing its own tightening of control, as seen when Palestine flags and keffiyehs were banned from the end of Amsterdam's 2026 Pride march. Encoded, embodied communication becomes a tool of digital self-determination that works in both spaces at once.

Rather than presenting Algodance as a finished artwork, the session frames it as one prototype among many possible community-led, self-hosted alternatives to dominant platform models, inviting participants to interrogate its assumptions, limits, and transferability. Where does an encoded language like this hold up, and where does it break down? What would it take for a community to sustain, govern, and evolve its own communication system without recreating the extraction and gatekeeping it was built to escape? And how might this kind of tactic connect to other grassroots and cross-solidarity movements that face similar surveillance and suppression?

The topic sits at the intersection of art, protest, and infrastructure: using a real legal and political struggle as grounding, and a speculative, participatory method as the means of collectively imagining what self-determined communication could look like.

Privacy Camp 26

EDPS - Civil Society Summit : safe by design, not by
exclusion: reclaiming our digital futures

13:45 - 15:00

Streamed

Salle des Arches

Fishbowl

Organiser:

- European Digital Rights (EDRi)
- European Data Protection Supervisor (EDPS)

Facilitator:

- Simeon de Brouwer, EDRi

On September 18, the Commission published the KIDS Act ('Keeping Internet Digital Spaces Accountable & Trustworthy'), a legislative proposal to age-gate access to digital services that risks kicking out many young & older people of online spaces.

In a 'fishbowl' conversation with the European Data Protection Supervisor Wojciech Wiewiórowski, we will explore the limits of measures focused on exclusion or invasion of privacy, & analyse the underlying structures & business models that expose all users to harm & vulnerability.

The conversation will then aim to unpack what the EU should be doing to build an ecosystem of solutions that includes privacy & safety by design & by default, increases media & digital literacy for all, prioritises systemic platform regulation over content regulation, & guarantees effective enforcement.

Privacy Camp 26

From cobalt to code: community self-determination in the AI supply chain

13:45 - 15:00

Boudoir

Screening & Panel

Organiser:

- One More Percent, Kenya

Moderator:

- Brian Malika - One More Percent / Digital Democracy Initiative

Speakers:

- Maurice Carney, Friends of the Congo
- Victor Ndeda - Amnesty International Kenya
- Binyamana Iki - DRC community & lived-experience perspective
- Diego Marin - EEB (TBC)

Artificial intelligence is often discussed in terms of algorithms, regulation & innovation, yet its story begins much earlier—in the extraction of the critical minerals that power AI infrastructure, batteries, cloud computing & advanced digital technologies. This panel asks a simple but important question: can there be digital self-determination if the communities supplying the resources that make AI possible remain excluded from its benefits?

Using the Democratic Republic of the Congo (DRC) & Kenya as case studies, the panel will explore a growing AI inequality across the global value chain. The DRC produces approximately 70% of the world's cobalt, a critical mineral powering AI & the global clean technology transition. Yet mining communities, particularly in the provinces of Lualaba & Haut-Katanga, continue to experience armed conflict, displacement & environmental degradation linked to competition over these strategic resources, while benefiting little from the AI economy they help make possible.

Kenya presents a different side of this inequality. Around 97.5% of online adults use AI tools monthly, reflecting a youthful, digitally connected population & a vibrant innovation ecosystem. However, Kenya's leadership largely ends with AI software adoption. While software use has expanded rapidly, the Global North continues to lead the highest-value parts of the AI revolution, including advanced AI hardware, semiconductor manufacturing, cloud infrastructure, smart & connected vehicles, AI-powered medical diagnostics, robotics, assistive technologies for persons with disabilities & immersive technologies. This highlights an emerging AI divide where many Global South countries either supply the minerals or consume AI software while capturing only a small share of the industries, infrastructure & economic opportunities created by AI.

Bringing together panelists from the DRC & Kenya alongside experts in digital rights, technology governance & responsible mineral supply chains, the discussion will argue that digital self-determination must begin where AI begins—with the communities whose land, labour & natural resources make the technology possible. Without AI supply chain justice, the DRC risks remaining primarily a supplier of raw materials, Kenya risks being recognised mainly for AI software adoption, while the Global North continues to capture the greatest value from both AI software & AI hardware. The panel will explore how the EU AI Act, the EU Critical Raw Materials Act, the UN Guiding Principles on Business & Human Rights, the OECD Due Diligence Guidance for Responsible Mineral Supply Chains, & the Sustainable Development Goals—particularly SDGs 9, 10, 12 & 16—can help build AI ecosystems that promote resource justice, environmental stewardship, fair value sharing & meaningful participation by mineral-producing countries. In doing so, the panel directly responds to Privacy Camp 2026's call to rethink the origins of future technologies through communities of digital self-determination rather than systems of extraction & inequality.

This session will start with the screening of "Lwanzo (Cobalt)", brought to Privacy Camp with the help of Friends of the Congo. "In Kolwezi, where the earth bleeds cobalt & the future is forged in dust, a quiet war rages. Beneath the shadow of multinational giants, the artisanal miners of Mutoshi, Kakwama, & Kamilombe dig—not just for survival, but for dignity, for the right to remain on the land of their ancestors. They stand at the fault line of a world racing toward a green energy transition, where cobalt fuels high-tech dreams & global powers clash in a contest of greed."

After the screening, the discussions moderated by Brian Malika begins.

Privacy Camp 26

Building power through strategic litigation:
defending LGBTIQ+ rights in digital spaces

13:45 - 15:00

Salon

Workshop

Organiser:

- Digital Freedom Fund

Facilitators:

- Alexandra Giannopoulou, Digital Freedom Fund
- Deekshitha Ganeshan, TGEU

In Hungary in 2025, the Parliament banned Pride events & authorised facial recognition to identify attendees. In Uganda in 2024, the courts upheld the country's Anti-Homosexuality Act, imposing penalties of life imprisonment or death. In Argentina in 2025, President Javier Milei banned gender affirming care for people under the age of 18 & his administration explicitly rejected "the diversity of sexual identities that do not align with biology." Amid growing far-right efforts to dismantle democratic norms across the EU, LGBTI people are used as scapegoats to normalise the disregard for human rights. We are in the era of anti-rights.

As the anti-rights movement has grown with increasing momentum offline, it has followed LGBTI people online where it continues to amplify. Meeting the needs to counteract this shift will mean building power in order to protect & advance LGBTI rights. DFF has worked closely with its community to generate legal strategies & build power for LGBTI rights online. We have supported Trans Europe & Central Asia (TGEU) in their work to establish legal gender recognition for trans people in the EU, a general precursor to accessing digital rights. Háttér Society has completed research mapping the extent of discriminatory content filtering of LGBTI voices in Hungary. Following complaints filed against Grindr & five adtech companies written by our partners at the Norwegian Consumer Council (NCC), the Norwegian Data Protection Authority fined dating app Grindr for disclosing personal information about users to third parties for behaviour-based marketing without a legal basis.

We believe that by developing power in the LGBTI ecosystem individually & as community, we can advance digital justice. The reality is that opportunities for building this power are declining because of shifting priorities in the political space & the shrinking resources available to communities harmed by BigTech, tech-related policies, & government restrictions. The workshop aims to create a space that will explore actions to counter these practices & identify strategies that will make community-centered litigation impactful.

Privacy Camp 26

From posts to power: how digital platforms are reshaping domestic work & labour rights in Africa

15:15 - 16:15

Streamed

Salle des Arches

Panel

Organiser:

- Pollicy, Uganda

Moderator:

Bonaventure Saturday, Research Manager, Pollicy

Speakers:

- Elizabeth Gitau - Domestic Professionals Association of Kenya (DPAK)
- Prof. Salome R. A. Bukachi - Department of Anthropology, Gender & African Studies, University of Nairobi
- Agnieszka Marta Fal-Dutra Santos, University of Bern
- TBC

Digital platforms have become a primary gateway to employment for millions of domestic workers across Africa. Facebook, WhatsApp, X, LinkedIn & online recruitment platforms increasingly mediate how workers find jobs, negotiate employment conditions & access migration opportunities. Yet these platforms also shape labour markets in ways that often reinforce inequality through opaque recruitment practices, discriminatory hiring preferences, limited transparency, & weak accountability.

Drawing on research analysing thousands of online recruitment posts for domestic work in Kenya, this panel examines how digital platforms have evolved into critical labour market infrastructure. The findings reveal how employers & recruitment agencies use platform features to define expectations around gender, age, experience, wages, migration, accommodation & contractual arrangements, often without adequate worker protections or platform oversight.

The discussion will situate these findings within Privacy Camp's theme of digital self-determination by asking who governs digital labour markets, whose interests current platform designs serve, & how digital recruitment systems can better support workers' rights, dignity & agency. Beyond identifying challenges, the panel will explore practical pathways for developing more transparent, accountable & worker-centred digital recruitment ecosystems.

The session will bring together perspectives from research, domestic worker organisations, digital rights advocates & policymakers to discuss platform accountability, labour governance & community-led approaches to digital labour markets. Audience participation will be integrated through live polling, moderated questions from both in-person & online participants, & an interactive discussion inviting participants to identify priority actions for platforms, governments & worker organisations.

The expected outcome is a shared set of recommendations for fair digital recruitment practices & platform governance that better protect domestic workers while contributing to broader discussions on digital self-determination, labour rights & equitable digital futures.

Privacy Camp 26

After the abyss

15:15 - 16:15

Boudoir

Screening & Panel

Organiser:

• European Digital Rights (EDRi)

Speakers:

• TBC

Synopsis:

After The Abyss is a cinematic meditation on digital darkness, following former content moderators in Nairobi as they struggle to reclaim themselves after bearing the world's violence through their eyes. Meanwhile, a new kind of resistance is growing- unions are formed and the city's youth wield the internet as a source of hope in Nairobi, both connected and wounded by the screen.

Total Run Time: 28 mins

Key creative credits:

Director: Keiria Shishay

Producers: Ulrikke Xenia & Ane Vennize Andersen

Countries of production: Denmark, Kenya

Privacy Camp 26

From surveillance to ecosystems of care: how to challenge narratives on the use of technology in alternatives to detention & center agency & rights

15:15 - 16:15

Salon

Workshop

Organiser:

- International Detention Coalition

Facilitators:

- Antonella Napolitano, International Detention Coalition
- Hope Barker, StratComms Studio
- Amina Fahmy, Privacy International
- BID/AVID, TBD

Today, governments are using technology & data-intensive systems to turn borders into networks of surveillance that stretch across time & space, experienced by migrants as a continuous presence. Technologies used in immigration detention & on people released from detention are increasingly embedded within this infrastructure. In recent years, we have seen the growing use of tools such as [GPS ankle monitors or GPS-enabled watches](#) in the UK & in the US, where they even defined them as alternatives to detention (ATDs), appropriating a label that instead indicates community-based & human rights-centered solutions. Now, the European Union is poised to accelerate this trend. [The EU's Migration & Asylum Pact](#) & the rushed-through [EU Returns Regulation](#) create new openings for intrusive technologies to become further embedded in migration governance, particularly in the space of immigration detention & alternatives. Recent [reports point to Frontex developing](#) smartphone-based tracking apps with little transparency or public scrutiny.

On the other hand, people on the move & grassroots groups are using, repurposing & building technologies to create counter-networks of resistance, support & care. When designed with & for affected communities, technology can help people understand & exercise agency throughout their journeys, navigate systems, connect with essential services, access legal support & participate meaningfully in decisions affecting their lives.

This tension raises a broader question about digital self-determination: who gets to decide what technology is for, how it is used & whose interests it serves? Politicians & wealthy tech CEOs shape the stories that define the problems technology is supposed to 'solve' & make particular responses appear inevitable. We are told that tagging, surveillance & monitoring will make us 'safer', while private companies profit from lucrative contracts to build & deploy these systems, & politicians gain votes by presenting migrants as a threat to society - diverting attention from the underfunded public services & social infrastructure people actually rely on.

The debate around detention & migration technologies therefore offers lessons for digital self-determination more broadly. Resistance has challenged not only particular technologies, but the stories used to justify them. It has questioned whether "alternatives" that reproduce surveillance are really alternatives, & what systems might look like if they were built around agency rather than control. Who gets to define the problem, who benefits from the proposed solution, & whose voices are missing?

Privacy Camp 26

AlgoDance session 2

15:15 - 16:15

Le Grenier

Workshop

Facilitators:

- Marit Hoefsloot
- Julie van Essen

Algodance is a speculative installation that offers dance as an alternative communication form to undermine the censorship of Meta's algorithms. Meta platforms are highly controlled digital spaces, where people can come together and interact, but only under strict surveillance and censorship. We desire digital public spaces where marginalised groups can freely convene and communicate, outside of Big Tech's restrictive policies and content formats. By using Algodance, words that are often banned or shadowbanned can be communicated through the language of dance. These words are created for and by queer marginalised communities, and the visitors are encouraged to add their own encoded dance moves to the dictionary during the showcase.

Algodance is a speculative interactive installation, developed during the CODE programme at IMPAKT, that turns dance into an encoded language, built by and for queer and marginalised communities to communicate past the censorship of Meta's algorithms. It offers a case study for this year's question: what does digital self-determination look like when the infrastructures we depend on are neither neutral nor accountable to the communities they claim to serve?

Meta's platforms function as de facto public squares, yet moderation on them is opaque, biased, and effectively unaccountable. This is not speculation: a Dutch class-action lawsuit, filed in May by Bureau Brandeis and Bits of Freedom on behalf of organisations including The Queer Agenda, COC Netherlands, and several queer nightlife and art collectives, alleges that Meta's down-ranking and censoring of LGBTQIA+ content breaches European fundamental rights law, the DSA, the GDPR, and Dutch anti-discrimination law. Algodance responds to this not by demanding better access to existing platforms, but by building an alternative: a living, community-authored "Dance Dictionary" that lets people encode and decode meaning through movement, expanding with every new contributor. These movements can be used to communicate (shadow)banned content on Meta platforms, while subverting its biased moderation practices.

This workshop proposal asks what happens when we treat the body, rather than a server, as infrastructure. It also extends the conversation beyond the digital: physical public space is undergoing its own tightening of control, as seen when Palestine flags and keffiyehs were banned from the end of Amsterdam's 2026 Pride march. Encoded, embodied communication becomes a tool of digital self-determination that works in both spaces at once.

Rather than presenting Algodance as a finished artwork, the session frames it as one prototype among many possible community-led, self-hosted alternatives to dominant platform models, inviting participants to interrogate its assumptions, limits, and transferability. Where does an encoded language like this hold up, and where does it break down? What would it take for a community to sustain, govern, and evolve its own communication system without recreating the extraction and gatekeeping it was built to escape? And how might this kind of tactic connect to other grassroots and cross-solidarity movements that face similar surveillance and suppression?

The topic sits at the intersection of art, protest, and infrastructure: using a real legal and political struggle as grounding, and a speculative, participatory method as the means of collectively imagining what self-determined communication could look like.