

Onopticon and Homovictimus: The Ontological Regime of the Digital Leviathan and the Operationalization of Algorithmic Governmentality

1. Introduction: The Transition from the Panopticon to the Onopticon

Section Summary: The classical surveillance model, the Panopticon, is no longer sufficient to explain the contemporary digital ecosystem. Power has constructed a new ontological regime—the "Onopticon"—which, rather than merely "observing" subjects, reconstructs them through data and preemptively forecloses their futures.

The governance architecture of contemporary societies has undergone a profound ontological rupture that cannot be explained by mere technological evolution. The classical Panopticon^[1], a prison architecture conceived by Jeremy Bentham and later analyzed by Michel Foucault, functioned as a disciplinary mechanism in which the mere possibility of being observed compelled the subject to internalize control. However, the digital ecosystem of the 21st century has propelled surveillance far beyond the limits of physical or visual visibility.

To conceptualize this new structure, the term *Onopticon*^[2] (derived from the Greek *on* for "being" and *optikon* for "seeing/observing") is proposed. The Onopticon does not merely observe the subject; it reconstructs the subject's very existence as data. Power no longer contents itself with recording the past or the present; it transforms into an algorithmic regime of execution that preempts and forecloses the future. This operationalization occurs through *Algorithmic Governmentality*—the governance of the social world based on the automated processing of big data rather than on politics, law, or social norms. The illusion that complex social and political dilemmas can be neatly resolved through algorithms—a fallacy Evgeny Morozov critiques as "technological solutionism"^[3] (Morozov, 2013)—provides the legitimizing ideological foundation for this regime.

2. The Onopticon: Algorithmic Recognition and the Foreclosure of the Future

Section Summary: The Onopticon views human unpredictability as a flaw. Through predictive modeling, it categorizes individuals based on data sets before they even act, confining them to statistical profiles and eliminating alternative future possibilities.

The Onopticon aims to eradicate uncertainty by trapping the future within the present. This institutional structure operates through two primary mechanisms:

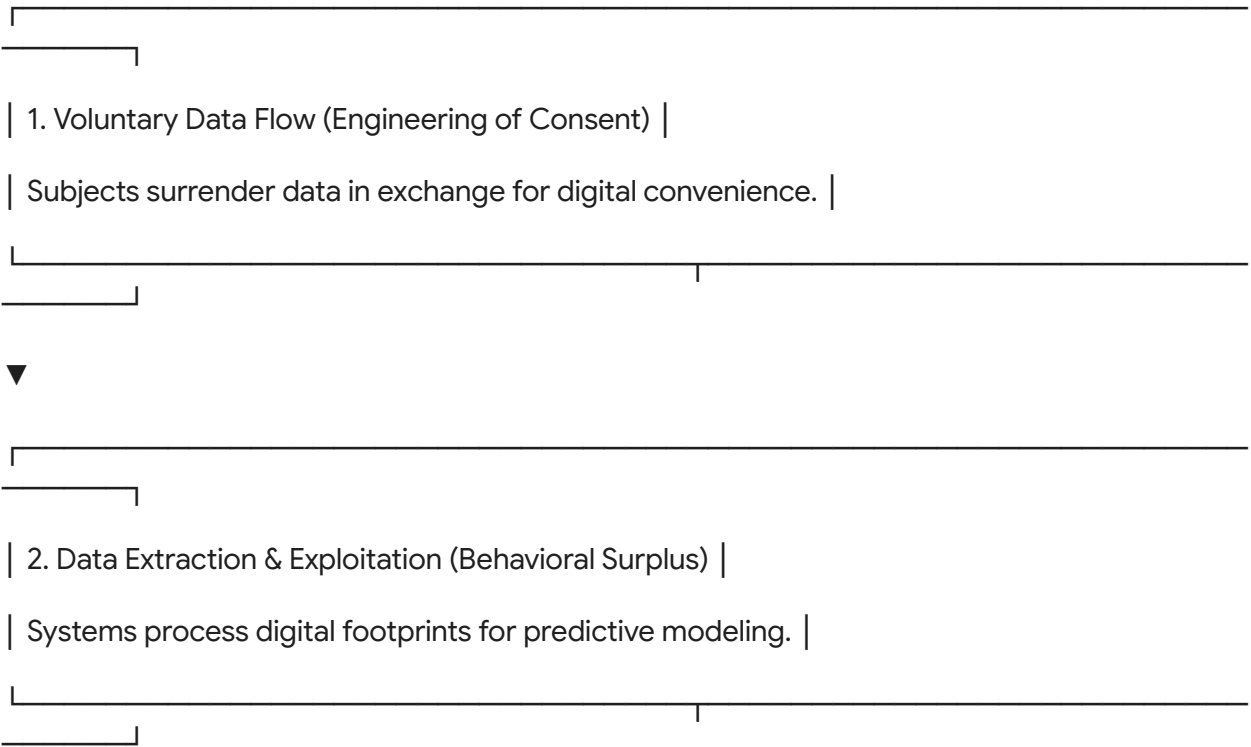
The Pre-recognition Regime: The Onopticon is no longer an "observing eye" but a

"recognizing and calculating apparatus." Before a subject even initiates an action, the system has already categorized them across vast data sets as a consumer, a potential criminal, or a high-risk borrower. This is the institutionalized manifestation of what Shoshana Zuboff terms "behavioral surplus" (Zuboff, 2019), where human experience is unilaterally claimed as raw material for translation into behavioral data.

The Foreclosure of the Future: The regime intervenes in the present based on statistical probabilities without waiting for an event to transpire. By doing so, it strips the individual of their agency. The individual experiences an epistemological closure, surrendering the right to author their own life to algorithmic black boxes.

The most destructive manifestation of this closure is predictive policing. While purportedly forecasting where crime will occur, these algorithms often encode historical biases, thereby initiating an era of "Digital Jim Crow" (Rodriguez, 2025).¹ As Virginia Eubanks (2018) has demonstrated, such tools automate inequality by criminalizing poverty and marginalizing minority communities. Furthermore, empirical evidence demonstrates the catastrophic inaccuracy of these systems: an analysis of over 23,000 predictions made by the Geolitica (formerly PredPol) software in Plainfield revealed a success rate of only 0.6% for robberies and aggravated assaults, and a staggering 0.1% for burglaries (Rodriguez, 2025).¹ These systems do not deliver justice; they merely automate and launder systemic prejudice.

Figure 1: The Operational Flow of Algorithmic Governmentality





3. Algorithmic Profiling (Pre-recognition)	
Subjects are confined to risk profiles prior to any action.	



4. Foreclosure of the Future (Algorithmic Execution)	
Automated decisions preemptively eliminate life possibilities.	



5. The New Subject: Homovictimus (The Data Victim)	
A hyper-visible, agency-stripped subject enslaved by its data.	

3. Homovictimus: The New Subject as a Data Victim

Section Summary: At the core of this regime lies *Homovictimus*, a subject crushed beneath the weight of its own digital shadow. Stripped of political agency, the individual is reduced from an autonomous citizen to a continuously harvested data carcass.

At the center of this paradigm is a new typology conceptualized as *Homovictimus*^[4], extensively detailed in the 2026 preprint *The Manifesto of Homovictimus* (Tan, 2026).² In stark contrast to the Enlightenment ideal of the rational, autonomous agent, Homovictimus is

depicted as a "phantom built of ciphers," whose will is shackled within a cold digital womb (Tan, 2026).²

Cognitive Proletarianization: Data produced in everyday life flows into the system via engineered consent. Byung-Chul Han identifies this voluntary submission as *psychopolitics* (Han, 2017), a neoliberal technique of self-exploitation. When individuals delegate memory, orientation, and decision-making capacities to AI, they undergo what Bernard Stiegler terms "cognitive proletarianization"—a systemic loss of the critical knowledge of how to live and act autonomously (Stiegler & Rouvroy, 2016).

Ontological Violence and Algorithmic Guilt: Homovictim is deemed "guilty" or "risky" purely based on statistical inferences drawn from digital traces, resulting in a state of "administrative suspension" or "digital civil death" where the subject is exiled from the system without a trial (Tan, 2026).³ This translates into direct *ontological violence*, particularly manifesting as technology-facilitated gender-based violence (TFGBV). Recent data confirms the industrial scale of this violence: deepfake videos surged by 550% between 2019 and 2023, with 98% of these being non-consensual pornography and 99% explicitly targeting women (Maiberg & Cole, 2025; UN Women, 2025).⁴ The generation of millions of sexualized images by AI tools like Grok in mere days underscores how women's bodily integrity is being algorithmically violated (CSO Hate, 2026).⁵

4. The Operational Models of the Digital Leviathan

Section Summary: The Onopticon manifests globally through "Digital Leviathan" infrastructures. While states utilize these systems to enforce social compliance and digital colonialism, market-driven models reduce individuals to behavioral commodities.

Inspired by Thomas Hobbes's concept of absolute sovereignty, the *Digital Leviathan* represents the concentration of power through technological infrastructure and machine learning, exercising what Luciano Floridi discusses in the context of "digital sovereignty" (Floridi, 2025). This Leviathan primarily operates through two models:

4.1. The State-Centric Model In this model, the citizen's ontological status is reduced to a biometric code or a social score. India's *Aadhaar* system pioneered this by linking fundamental rights to biometric databases (Drèze & Sen, 2019). A highly controversial parallel is Kenya's \$15 billion *Maisha Namba* digital ID project; implemented in a nation where 91% of the population already possessed valid identification, it has been heavily criticized as an exercise in "digital colonialism" driven by external donor interests and political rent-seeking (Zollmann & Sambuli, 2026; KICTANet, 2023). Meanwhile, China's Social Credit System continues to enforce behavioral compliance through regional databases, culminating in the formalization of the "Credit Repair Management Measures" implemented in April 2026 to manage the penalties imposed on "dishonest" entities (NDRC, 2026; Liang et al., 2018).⁶ These systems operationalize

Giorgio Agamben's concept of *Homo Sacer*^[5] (Agamben, 1998), condemning those outside the digital registry to "bare life."

4.2. The Market-Centric Model Under surveillance capitalism, the market-centric Leviathan converts the illusion of freedom into continuous data extraction. Tech monopolies provide intelligence agencies with predictive "risk scores" (e.g., Palantir), effectively privatizing state surveillance (Taplin, 2017). Simultaneously, social media algorithms (such as Meta's intent prediction models) trap users in hyper-personalized echo chambers, leveraging their psychological vulnerabilities to modify behavior and maximize engagement (Sprinklr, 2025).⁷

5. Ontological Mutiny: Legal and Negentropic Resistance

Section Summary: Resistance to the Digital Leviathan is mounting through stringent legal frameworks—such as the EU AI Act and landmark court rulings demanding algorithmic transparency—and "negentropic" technological sabotage that poisons AI training data.

Escaping the Onopticon requires approaching technology as a *pharmakon* (both poison and cure). Resistance is currently crystallizing across legal and technological fronts:

5.1. The EU AI Act and Normative Safeguards The European Union's AI Act establishes a rigorous timeline to dismantle the most egregious aspects of algorithmic governmentality. As of **February 2, 2025**, the deployment of social scoring, manipulative AI techniques, and purely profiling-based predictive policing became strictly prohibited within the EU (European Parliament, 2024).⁸ Most critically, the mandate for "Human Oversight" (Article 14), which ensures that high-risk AI decisions can be overridden by a human via a "stop button" or the "two-person rule," will be fully enforced by **August 2, 2026**, legally safeguarding human agency against machine autonomy (European Union, 2024).⁹

5.2. Landmark Jurisprudence: BOSCO and Dun & Bradstreet The judicial branch has begun to shatter algorithmic black boxes. On **September 11, 2025**, Spain's Supreme Court delivered a historic ruling against the government's refusal to disclose the source code of *BOSCO* (an algorithm used for allocating energy subsidies) (Civio, 2025).¹⁰ The Court established that algorithmic transparency overrides intellectual property claims, cementing it as a constitutional right essential for digital democracy (Civio, 2025).¹⁰ Similarly, on **February 27, 2025**, the Court of Justice of the European Union (CJEU) ruled in *CK v Dun & Bradstreet* (Case C-203/22) that trade secrets cannot negate a data subject's right under the GDPR to receive "meaningful information about the logic involved" in automated credit scoring, effectively legally validating the "right to explanation" (CJEU, 2025).

5.3. Technological Sabotage and Decentralized Justice

Where the law lags, *negentropic*^[^6] (friction-inducing) resistance disrupts the automation of the Leviathan.

- **Data Poisoning:** Tools like *Nightshade* and *Glaze* empower artists to launch "ontological attacks" against unauthorized AI scraping. The release of *Glaze* v2.1 in 2026 successfully countered "noisy upscaling" attacks by embedding imperceptible perturbations that drastically degrade the output quality of generative models attempting to bypass the protection (Zhao et al., 2026).¹¹
- **Decentralized Justice:** Blockchain-based arbitration platforms like *Kleros* (specifically the *Kleros 2.0 Beta* launched on *Arbitrum One*) bypass algorithmic monopolies by crowdsourcing dispute resolution to randomly selected, economically incentivized human jurors, returning the power of judgment to human conscience (Lesaegre, 2019; Kleros, 2025).¹²

6. The Architectural Rights Doctrine: A Hardwired Constitution

Section Summary: To ensure permanent protection, human rights must transcend legal texts and software policies; they must be physically embedded into the hardware of computing systems.

Software and legal frameworks are perpetually vulnerable to backdoors, corporate lobbying, and state security exemptions. A definitive resolution demands the implementation of the *Architectural Rights Doctrine*, which posits that human dignity must be engineered into the physical architecture of technology. It rests on three pillars:

1. **The Right to Opacity:** As articulated by Éric Sadin, this is the fundamental right to resist being rendered completely transparent, quantifiable, and computable^[^7] (Sadin, 2020).¹³ It guarantees the individual a zone of darkness impervious to algorithmic extraction.
2. **Human-in-the-Loop:** The unyielding principle that decisions bearing significant legal, economic, or existential consequences must never be entirely ceded to autonomous systems.
3. **Hardwired Rights:** Because software protections are inherently flawed, memory safety and compartmentalization must be enforced at the Instruction Set Architecture (ISA) level. The *CHERI* (Capability Hardware Enhanced RISC Instructions) project and its IoT variant, *CHERI*IoT, achieve precisely this. By enforcing referential integrity and fine-grained compartmentalization directly in the silicon, *CHERI*IoT eradicates up to 70% of memory safety vulnerabilities (Watson et al., 2015; Norton, 2025).¹⁴ Implemented in *SiC* Semiconductor's *lCeni* microcontrollers, currently in test production as of late 2025 for a 2026 commercial launch, this technology proves that constitutional rights can indeed be hardwired into silicon (Norton, 2025).¹⁴

7. Conclusion: The Courage to Become a "Glitch"

The Onopticon is an absolute, hyper-historical project of sovereignty that intertwines the state, capital, and technology to reduce humanity to a predictable, exploitable data entity. The resulting Homovictimus is trapped in a seamless automation of the future, robbed of its political and existential agency.

Yet, this digital subservience is not inevitable. In *The Spirit of Hope* (2024), Byung-Chul Han posits that despair is merely hope's evil twin; against a trajectory of pure crisis management and survival, we must adopt a posture of "hopeful pessimism"—recognizing the bleakness of the algorithmic enclosure while acting radically to dismantle it (Han, 2024).¹⁵

The Onopticon's greatest vulnerability is its insatiable dependence on flawless data and frictionless computation. The legislative boundaries established by the EU AI Act, the dismantling of trade secret defenses by the CJEU and the Spanish Supreme Court, the negentropic sabotage enabled by Glaze, and the hardware-level security of CHERIoT all form the vanguard of an ontological mutiny. The spontaneity and unpredictability inherent in human nature remain the ultimate anomalies that algorithms cannot compute. Rather than yielding to the tyranny of perfect prediction, humanity must summon the courage to become an uncorrectable "Glitch" within the system.

Footnotes

[^1]: **Panopticon:** An institutional building and system of control designed by the English philosopher Jeremy Bentham in the 18th century. It serves as a metaphor in Michel Foucault's work for modern disciplinary societies where subjects self-regulate due to the constant possibility of surveillance.

[^2]: **Onopticon:** A neologism derived from the Greek *on* (being) and *optikon* (seeing/observing). It denotes the contemporary digital regime that moves beyond visual surveillance to fully reconstruct and pre-empt human existence as calculable data.

[^3]: **Technological Solutionism:** A critical concept coined by Evgeny Morozov describing the dangerous fallacy that complex social, political, and moral problems can be neatly solved via simple algorithmic applications.

[^4]: **Homovictimus:** A portmanteau of *homo* (human) and *victima* (victim), signifying the modern data-subject who is entirely integrated into digital ecosystems but utterly stripped of political agency and autonomy.

[^5]: **Homo Sacer:** A figure from Roman law adopted by philosopher Giorgio Agamben, representing a person stripped of all civil rights—reduced to "bare life"—who can be killed

without it being considered murder.

[^6]: **Negentropy (Negative Entropy):** The measure of a system's resistance to disorder and decay. In digital resistance (influenced by Bernard Stiegler), it refers to the deliberate introduction of human unpredictability to sabotage the flawless, deterministic automation of algorithms.

[^7]: **Right to Opacity:** A concept articulated by philosopher Éric Sadin, advocating for the individual's legal and existential right to maintain a "zone of darkness," resisting the algorithmic imperative of absolute transparency and calculability.

Bibliography

- Agamben, G. (1998). *Homo Sacer: Sovereign Power and Bare Life*. Stanford University Press.
- Civio. (2025). *Civio pulls back the curtain on public algorithms: Spain's Supreme Court orders the government to release BOSCO's source code*. Civio Foundation.¹⁰
- CJEU. (2025). *Judgment of the Court (First Chamber) of 27 February 2025: CK v Magistrat der Stadt Wien (Case C-203/22)*. Court of Justice of the European Union.
- CSO Hate. (2026). *Algorithmic Design & Gendered Violence: The Grok Case*. Center for the Study of Online Hate.⁵
- Drèze, J., & Sen, A. (2019). *An Uncertain Glory: India and its Contradictions*. Princeton University Press.
- Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.
- European Parliament. (2024). *Artificial Intelligence Act: Regulation (EU) 2024/1689*. Official Journal of the European Union.⁸
- Floridi, L. (2025). *Agentic AI Optimisation (AAIO): What it is, How it Works, Why it Matters, and How to Deal With It*. SSRN.
- Foucault, M. (1975). *Discipline and Punish: The Birth of the Prison*. Gallimard.
- Han, B.-C. (2017). *Psychopolitics: Neoliberalism and New Technologies of Power*. Verso.
- Han, B.-C. (2024). *The Spirit of Hope*. (D. Steuer, Trans.). Polity.¹⁶
- KICTANet. (2023). *Understanding Maisha Namba: Kenya's New Digital Identity System*. Kenya ICT Action Network.
- Kleros. (2025). *Kleros Project Update 2026: Kleros 2.0 Beta on Arbitrum One*. Kleros Blog.¹²
- Lesaege, C. (2019). *Kleros: A Decentralized Dispute Resolution Platform*. White Paper.
- Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy & Internet*, 10(4), 415–453.
- Maiberg, E., & Cole, S. (2025). *The Rise of Deepfake Pornography*. 404 Media / IGP.
- Mbembe, A. (2019). *Necropolitics*. Duke University Press.
- Morozov, E. (2013). *To Save Everything, Click Here: The Folly of Technological Solutionism*.

PublicAffairs.

- NDRC. (2026). *Credit Repair Management Measures*. National Development and Reform Commission, China. ⁶
- Norton, R. (2025). *Hardware-software co-design for security with CHERIoT*. HS3 2025 Workshop, European Symposium on Research in Computer Security. ¹⁴
- Rodriguez, F. S. (2025). *Predictive Policing: How AI is Setting the Stage for a Digital Jim Crow Era*. CHCI-Law Postgraduate Report. ¹
- Sadin, É. (2020). *L'Intelligence artificielle ou l'enjeu du siècle*. L'Échappée. ¹³
- Sprinklr. (2025). *The Algorithm Shift: What Social Platforms Are Prioritizing in 2025*. Sprinklr Insights. ⁷
- Stiegler, B., & Rouvroy, A. (2016). The digital regime of truth: from the algorithmic governmentality to a new rule of law. *La Deleuziana*, (3), 6-29.
- Tan, H. (2026). *The Manifesto of Homovictimus (An Ontological Tragedy)*. (Unpublished Preprint), SSRN/ResearchGate. ²
- Taplin, J. (2017). *Move Fast and Break Things: How Facebook, Google, and Amazon Cornered Culture and Undermined Democracy*. Little, Brown and Company.
- UN Women. (2025). *Tipping Point: The Chilling Escalation of Violence Against Women in the Public Sphere in the Age of AI*. UN Women / UNESCO. ⁴
- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law*, 7(2), 76-99.
- Watson, R. N. M., et al. (2015). CHERI: A Research Platform for Hardware-Software Co-Design. *IEEE Micro*, 35(2), 44-53. ¹⁷
- Zhao, B. Y., et al. (2026). *Glaze v2.1 and Nightshade Updates*. SAND Lab, University of Chicago. ¹¹
- Zollmann, J., & Sambuli, N. (2026). *Citizen Experiences with DPI: Kenya's Digital ID Transition*. Center for Financial Inclusion.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism*. PublicAffairs.