

From Private Surveillance to Public Protection: The Pervasive Interplay. The Case of NEOM*

Malik Bozzo-Rey

(Research Professor – ETHICS (EA 7446), Université Catholique de Lille)

Mehdi Ghassemi

(Head of Research at ISTC – Fellow at ETHICS (EA 7446), Université Catholique de Lille)

ABSTRACT This article examines the role of facial-recognition technology (FRT) in Saudi Arabia's NEOM megaproject to show how the megacity's "cognitive" infrastructure normalizes totalizing surveillance and reconfigures the political status of urban subjects. Combining a close reading of corporate and vendor material with critical surveillance studies, the first section maps the hardware–software assemblage that converts the human face into a continuously monitored, algorithmically actionable data point. We argue that NEOM's promise of frictionless security and efficiency collapses the distinction between private and public sphere and erodes privacy as a meaningful category. The second section develops a philosophical critique grounded in an ethics of anonymity. We contend that anonymity can function as a normative counter-strategy: by reinstating zones of deliberate indeterminacy, it challenges the automation ideology that seeks to erase subjectivity itself.

KEYWORDS: Facial recognition - Automation - Surveillance - Privacy - Ethics of anonymity - Responsibility - Security

TABLE OF CONTENTS: 1. Introduction. – 2. NEOM, FRT and the negation of privacy. – 2.1. NEOM and FRT. – 2.2. Negation of privacy. – 3. Ethics of anonymity as a form of resistance. – 3.1. NEOM as a model for society. – 3.2. For an ethics of anonymity. – 3.2.1. Elaborating a concept of anonymity. – 3.2.2. Anonymity and the concept of society. – 3.3. Could anonymity resist NEOM?. – 3.4. Is anonymity a threat to public safety?. – 3.4.1. Gyges' ring. – 3.4.2. The question of responsibility: does anonymity necessarily lead to a crime without a perpetrator... but not without a victim?. – 4. Conclusion.

1. Introduction

Facial Recognition Technology (FRT) has evolved into a cornerstone of modern surveillance, seamlessly integrating with Closed-Circuit Television (CCTV) and other monitoring systems. Once an exceptional tool for security and law enforcement, surveillance technologies have become ubiquitous, transforming the cultural and social significance of the human face as a key identifier in surveillant assemblages.¹ Unlike human observers, machines equipped with FRT can identify, analyze, and recall individuals on a scale that was previously unimaginable, effectively transforming public spaces into zones of systematic surveillance.² This intersection of public and private spheres raises critical ethical questions. The face, an inherently personal attribute, becomes a tool for systematic visibility and control.

Framed as a trade-off for security and

efficiency, this enforced visibility introduces tensions between privacy, anonymity, and collective accountability.

Rethinking anonymity - not as a barrier to security but as a safeguard for personal freedom - is essential in an era of pervasive surveillance, especially and when the conventional relationship between freedom and security is inverted: instead of security measures serving to uphold and reinforce inherent personal freedoms, the pervasive surveillance paradigm posits that freedom itself becomes a conditional state that is 'allowed' or granted only by the establishment of comprehensive security.

This article seeks to explore these tensions through the emblematic example of NEOM,³ Saudi Arabia's futuristic urban project first officially announced in 2017, and still under construction. Promoted as a "city of the future," "city of dreams" and a cornerstone of the Kingdom's Vision 2030 initiative, NEOM aspires to be a global model of technological innovation and sustainability. It is framed as a

* Article submitted to double-blind peer review.

¹ M. Andrejevic and N. Selwyn, *Facial Recognition*, Cambridge, Polity, 2022.

² M. Andrejevic and N. Selwyn, *Facial Recognition*, cit., 122-123.

³ www.neom.com.

blueprint for the future of urbanism worldwide, embodying a technosolutionist ideology and a vision that is explicitly international: NEOM's infrastructure, technologies, and workforce are predominantly sourced from global partnerships, while its funding relies heavily on foreign private and state investment. Moreover, NEOM's branding as a "model for the future" has garnered significant global media attention, reflecting its aspiration to set the standard for post-AI cities. At the same time, it is a site where facial recognition, integrated with other AI-powered surveillance technologies, will be deployed on an unprecedented scale. As such, NEOM is not merely a regional project but a testing ground for the integration of AI in urban planning and governance at a global scale. The first part of this article will therefore detail the ways in which facial recognition is conceived, utilized, marketed and justified within the NEOM project, highlighting the technological, social, and political dimensions of its implementation. The second part, adopting an ethical and philosophical perspective, will build on the NEOM case to argue that anonymity can serve as a critical response to these surveillance practices. By connecting these two arguments, this article aims to provide a framework for understanding how technologies could and should be used, and to emphasize the critical need to build an ethics of anonymity to resist surveillance societies.

2. NEOM, FRT and the negation of privacy

Crown Prince Mohammed bin Salman (MBS), the de facto ruler of the Kingdom of Saudi Arabia, has emphasized that artificial intelligence will be integral to every aspect of NEOM, from optimizing daily operations to ensuring security. The mega-city's design promises seamless surveillance, real-time optimization, and hyper-efficient service essentially via the large-scale integration of AI.⁴ One area AI-driven will be extensively applied is FRT. NEOM's deployment of FRT is intricately woven into the infrastructure of its major zones, such as The Line,⁵ NEOM Bay Airport, and Oxagon.⁶ Designed as an integral component of NEOM's AI-driven

operational framework, FRT underpins key functionalities, from urban security to personalized services. By leveraging advanced hardware and software solutions, NEOM establishes a data-rich environment that serves its ambitious vision of becoming a "cognitive city."⁷

2.1. NEOM and FRT

In terms of hardware, NEOM employs high-resolution cameras strategically placed across key locations such as transportation hubs, residential areas, and commercial spaces.⁸ These cameras, equipped with infrared imaging capabilities, ensure accurate facial detection even in low-light conditions, providing uninterrupted monitoring throughout the city. Complementing these are edge computing devices⁹ that facilitate localized data processing. By performing real-time image analysis at the source, these devices minimize latency and reduce dependency on centralized data centers, thus enhancing both speed and efficiency. Drones integrated with biometric scanning capabilities add another layer of versatility, patrolling urban and industrial zones to monitor activity and respond swiftly to "anomalies" or emergencies.¹⁰ The software infrastructure driving NEOM's FRT is equally sophisticated, with the Neos operating platform serving as the central hub for data aggregation and analysis.¹¹ This AI-powered system integrates inputs from multiple data streams, including facial recognition feeds, and is designed to handle 90% of available data from residents and infrastructure. At the core of this platform is the VDG SENSE Video Management System (VMS), a cutting-edge tool that enables continuous video monitoring, event-driven analytics, and automated responses to

⁷ www.neom.com/en-us/newsroom/neom-cognitive-cities.

⁸ *NEOM demonstrates cutting-edge airport technologies to Jawazat chief*, in *Saudi Gazette*, 2 May 2024, www.saudigazette.com.sa/article/642589/SAUDI-ARABIA/NEOM-demonstrates-cutting-edge-airport-technologies-to-Jawazat-chief.

⁹ <https://tonomus.neom.com/en-us/insights/the-convergence-of-edge-computing-and-cloud-strategies>.

¹⁰ <https://terra-drone.com.sa/the-transformative-power-of-f-drone-services-in-saudi-arabia>.

¹¹ B. Bostock, *Saudi Arabia's \$500 million mega-city Neom is creating plans to harvest an unprecedented amount of data from future residents. Experts say it's either dystopian or genius*, in *Business Insider*, 24 March 2021, www.businessinsider.com/neom-saudi-smart-city-data-surveillance-plans-experts-2021-3.

⁴ O. Hassan, *Artificial Intelligence, Neom and Saudi Arabia's Economic Diversification from Oil and Gas*, in *The Political Quarterly*, vol. 91, n. 1, 2020.

⁵ www.neom.com/en-us/regions/theline.

⁶ www.neom.com/en-us/regions/oxagon.

security threats.¹² The VMS seamlessly interfaces with other systems, such as Automated Number Plate Recognition (ANPR), to provide a unified security framework. Furthermore, NEOM leverages advanced AI algorithms, specifically convolutional neural networks (CNNs), for facial analysis. These algorithms extend beyond mere identification, incorporating capabilities like emotion detection, age estimation, and behavioral prediction. By integrating these tools into its FRT framework, NEOM ensures a comprehensive approach to monitoring and governance.

In terms of application, for instance, at NEOM Bay Airport, FRT is integral to contactless travel experiences. High-resolution cameras embedded in biometric eGates capture and process travelers' facial features, matching them with immigration and travel documents in real-time.¹³ This system eliminates the need for manual document checks, aimed at reducing wait times and ensuring seamless passenger movement. Beyond airports, FRT is employed in hotels, where automated check-ins replace traditional reception desks. Guests' identities are verified through facial scans, granting them access to their rooms without physical keys or additional verification steps. Public safety is another critical domain where FRT plays a pivotal role. Cameras equipped with FRT will be (and are being) deployed across NEOM's public spaces, continuously monitoring for potential threats and ensuring rapid response to incidents.¹⁴ These systems are integrated with advanced analytics platforms capable of identifying suspicious behavior or detecting individuals flagged on security watchlists. In emergencies, biometric data collected through FRT is paired with health-monitoring systems to provide targeted assistance. For example, if a resident remains immobile for an extended period, drones equipped with FRT and health-

monitoring tools can be deployed to assess the situation and alert emergency services.

FRT is also promised to underpin NEOM's governance and resource allocation. According to James Bradley, NEOM's Head of Tech, "each resident would have a unique ID number, and Neos would process data from heart-rate monitors, phones, facial-recognition cameras, bank details and thousands of IoT devices."¹⁵ These IDs are linked to NEOM's Neos operating platform, allowing the city to offer personalized services based on real-time data. For instance, facial recognition integrated with smart transportation systems can optimize mobility by predicting and responding to passenger demand. In governance, automated identity verification expedites administrative processes like voter registration and public resource allocation, ensuring efficiency and reducing bureaucratic delays.¹⁶

The deployment of FRT in NEOM is intricately tied to the city's broader operational goals, which are centered around enhancing security, optimizing efficiency, and personalizing urban experiences. One of the primary objectives is to establish NEOM as a benchmark for urban safety through a comprehensive, AI-driven surveillance infrastructure. FRT, integrated with video analytics systems like the VDG SENSE Video Management System (VMS), enables 24/7 monitoring of public spaces, critical entry points, and key transit routes.¹⁷ By detecting anomalies in real time – such as unauthorized access, abnormal crowd behavior, or the presence of individuals on security watchlists – this system ensures rapid responses to potential threats. The use of Automated Number Plate Recognition (ANPR) further complements this goal, streamlining traffic management and enhancing checkpoint efficiency, crucial in a city aiming for seamless transportation flows.

Another key operational goal is the optimization of resource allocation and city management through data-driven governance. FRT functions as a cornerstone of NEOM's

¹² *Ensuring a technologically advanced environment in Neom, Saudi Arabia*, 15 November 2023, <https://tkhsecurity.com/collaborating-with-oxagon-for-community-expansion-project-in-neom-saudi-arabia>.

¹³ *NEOM Bay Airport will use cutting edge tech for smoother travel experiences*, in *List Magazine*, 6 May 2024, www.listmag.com/en/travel-stay/neom-bay-airport-will-use-cutting-edge-tech-for-smoother-travel-experiences-1752.

¹⁴ *Ensuring a technologically advanced environment in Neom, Saudi Arabia*, 15 November 2023, <https://tkhsecurity.com/collaborating-with-oxagon-for-community-expansion-project-in-neom-saudi-arabia>.

¹⁵ B. Bostock, *Saudi Arabia's \$500 million mega-city Neom is creating plans to harvest an unprecedented amount of data from future residents*.

¹⁶ *Saudi Neom: The first cognitive city in the world is coming*, in *Leaders Magazine*, 5 May 2021, www.leaders-mena.com/saudi-neom-the-first-cognitive-city-in-the-world-is-coming.

¹⁷ *Ensuring a technologically advanced environment in Neom, Saudi Arabia*, cit.

Neos operating platform, which is designed to collect and analyze up to 90% of available data from residents and urban infrastructure. Biometric data obtained through FRT is utilized to enable real-time decision-making in resource distribution, emergency response, and public service provision.¹⁸ For example, by monitoring population density in different zones, the system can dynamically adjust the allocation of public transportation vehicles or manage energy consumption more efficiently. This capability extends to healthcare, where FRT-integrated biometric systems can detect medical emergencies, such as a resident exhibiting signs of distress, and trigger immediate interventions from drones or paramedics.

Finally, NEOM's FRT deployment aligns with its ambition to position itself as a global leader in AI-driven personalization. By assigning each resident a unique biometric ID linked to their preferences and behavior patterns, NEOM leverages FRT to deliver tailored services. This includes personalized mobility solutions, where transportation schedules adapt to user needs, and targeted entertainment offerings, such as recommending events or venues based on past attendance.

2.2. Negation of privacy

In addition to the adoption of the IDA The embedded, systemic integration of facial recognition technology into the foundational design and operation of space in NEOM crystallizes a radical shift in how privacy is conceptualized and undermined by the project's designers. As already demonstrated by surveillance scholars, even during its earlier developments, FRT "renders the face a token in an automated regime of classification."¹⁹ Combined with current and future automation capabilities, NEOM plans to turn the human face – a deeply personal identifier – into a continuously monitored facial infrastructure that operates not merely to identify but to preemptively evaluate,

categorize, and predict behaviors. In this context, privacy is not simply infringed upon; it is systematically rendered obsolete, redefined as a controlled commodity within NEOM's operational framework. It is another example of how surveillance ceases to be an exceptional measure and becomes the default condition,²⁰ supported by a complex network of AI-powered systems that blur the boundaries between private and public spheres.²¹ The promise of efficiency and security, central to NEOM's technosolutionist narrative, enforces a regime of hyper-visibility, where the autonomous subject dissolves into a matrix of algorithmic governance.

Mark Andrejevic's concept of the "bias of automation,"²² that is, the systemic tendencies and assumptions that underlie automated systems, elucidates the broader implications of this shift, particularly through the interconnected logics of preemption, operationalism, and framelessness. NEOM's FRT architecture does not merely observe; it preempts. By leveraging predictive analytics, it forecloses on the unpredictable dimensions of human agency, constructing a data-driven environment that emphasizes certainty and control over spontaneity and individuality. This operational bias reframes governance as an automated process, where decisions are made in real-time by systems optimized for efficiency rather than human deliberation. Such systems, as seen in NEOM's AI-integrated governance platforms, act without the need for narrative or explanation, creating a space where human judgment and subjectivity are increasingly evacuated. The result is an "operational city" where

¹⁸ T. Porter, *The Saudi crown prince wants to build a trillion-dollar utopia in the desert. His deals with China reveal a darker vision*, in *Business Insider*, 23 April 2023, www.businessinsider.com/saudi-crown-princes-china-deals-hint-city-darker-neom-mbs-2023-3.

¹⁹ L. Introna and D. Wood, *Picturing algorithmic surveillance: The politics of facial-recognition systems in Surveillance & Society*, vol. 2, Issue 2/3, 2004, 177-198.

²⁰ K. Gates convincingly traces the shift from episodic identification to "continuous biometric addressability." See K. Gates, *Our biometric future: Facial-recognition technology and the culture of surveillance*, New York, NYU Press, 2011.

²¹ Traditionally, the distinction between public and private spheres has been based on the difference between political and family spaces. The latter is understood to be beyond the state's control, i.e. beyond the state's influence and that of other social institutions. The public sphere is a space for political deliberation that allows people to express themselves. Although these spheres appear to be clearly delineated, their boundaries are clearly fluid and dynamic. For a detailed analysis, see J. Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, Cambridge, Polity Press, 1989.

²² M. Andrejevic, *Automated Media*, New York, Routledge, 2020, 32-36.

individuals are not participants in governance but data points within a seamless computational framework. Moreover, drawing on Andrejevic's conception of "environmentality,"²³ privacy is no longer about safeguarding personal information but is reframed as a transactional element within an environment designed for continuous monitoring and predictive control. NEOM's systems commodify data, seamlessly extracting it through integrated surveillance networks while promoting this as a benefit by offering residents compensation for their data.²⁴ However, this commodification obscures the pervasive surveillance and preemptive mechanisms that underpin its operation, actively reconstructing privacy to align with technosolutionist objectives. This transformation is further intensified by NEOM's integration of FRT into daily life – extending from airports, hotels, and residential areas, to healthcare provision and governance processes – effectively collapsing traditional boundaries between public and private spaces. By enforcing visibility and making anonymity virtually unattainable, NEOM not only diminishes public space as a realm for freedom of expression but also encroaches on private life, turning every interaction into a surveilled transaction.

This trajectory arguably reflects a deeper ideological commitment to the eradication of subjectivity itself – a core tenet of automation ideology that is based not just on the loss of privacy but as a negation of the individual as a political and social subject.²⁵ Andrejevic's notion of "framelessness"²⁶ helps us see how NEOM's interconnected surveillance systems aspire to a view from "everywhere," encompassing all aspects of urban life without the limitations (frames) of human perception. Building on Agre's "capture model"²⁷ of surveillance and Andrejevic's concept of "framelessness," we argue that NEOM's quest

for total information capture – realized through a dense sensor mesh – seeks to supplant the interpretive, situated dimensions of human experience with what Kitchin and Dodge describe as a "code/space" of computational objectivity,²⁸ thereby compressing the contingencies of social life into algorithmically derived patterns, correlations, and predictive probabilities.²⁹ In attempting to automate subjectivity – to render the human condition legible and actionable within an AI-driven framework – NEOM negates the very qualities that define the autonomous human subject. By aligning governance, security, and urban functionality with the logic of automation, NEOM envisions a future for the post-AI world where subjectivity, with all its unpredictability and resistance, is not merely managed but fundamentally erased.

3. Ethics of anonymity as a form of resistance

3.1. NEOM as a model for society

Even if the NEOM project is not yet a fully-fledged reality, we should not underestimate the imaginary it conveys and the future society it proposes. NEOM is, in a sense, the beginning of a process of generalised and globalised surveillance that Bernard E. Harcourt calls the 'expository society'.³⁰ The term is important because it underlines the fact, highlighted by the NEOM project, that this is indeed a project for society. In light of what we have said above, what characteristics can we retain of such a project? The first point is probably the most important, in the sense that the other features are merely the modalities of this essential point: NEOM aims to abolish the distinction between the private and public spheres through a comprehensive strategy of transparency and disclosure. By reducing individuals' lives to sets of data that can be analysed, NEOM is proposing to 'datafy' people, meaning all aspects of their lives can be accessed and used to influence and predict their behaviour. This involves merging the public and private spheres into a new 'data-

²³ M. Andrejevic, *Automated Media*, cit., 37.

²⁴ M.A. Farouk, *Saudi 'surveillance city': Would you sell your data to The Line?*, in *Reuters News*, 23 August 2022.

²⁵ This line of thought has been demonstrated by several surveillance and legal scholars. See for instance M. Hildebrandt, *Smart Technologies and the End(s) of Law*, Cheltenham, Edward Elgar, 2015; L. Amoore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*, Durham, Duke UP, 2020.

²⁶ M. Andrejevic, *Automated Media*, cit., 36.

²⁷ P.E. Agre, *Surveillance and Capture: Two Models of Privacy*, in *The Information Society*, vol. 10, n. 2, 1994, 101-127.

²⁸ R. Kitchin and M. Dodge, *Code/Space: Software and Everyday Life*, Cambridge, MIT Press, 2011.

²⁹ L. Amoore, *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*, in *Contemporary Political Theory*, 21 (Suppl 3), 2022, 118-121.

³⁰ See B.E. Harcourt, *Exposed: Desire and Disobedience in the Digital Age*, Harvard, Harvard University Press, 2015.

sphere', where the distinction between them becomes meaningless.³¹ Such an approach is reminiscent of the instruments envisaged by Jeremy Bentham in his text on 'Indirect legislation':³² tattoos, etc., should make it possible, on the one hand, to govern individuals – i.e. to influence their behaviour – without having to resort to criminal sanctions, and, on the other hand, to devise a mode of government based on the reduction of alarm in society – i.e. to ensure security. This presupposes a generalised strategy of transparency on the part of individuals towards themselves and others, as well as a predictive conception of law.

On the other hand, the difference between Bentham's view and the NEOM project is that indirect legislation is part of a reflection on criminal law, and its end is the principle of utility, i.e. maximising the greatest happiness for the greatest number. But the important thing to remember about this comparison is that any dynamic - or strategy - of individualised transparency aims to ensure global surveillance, which in turn aims to influence or even shape the behaviour of individuals in the name of their own security. In other words, NEOM moves from private surveillance to public surveillance in the name of security, which takes the form of protecting the public - even if, and this is probably a particularly ingenious and pernicious trick, this security and surveillance strategy is submerged in the midst of other objectives (making life easier for tourists, enabling faster traffic, automating tasks and purchases, etc.). This abolition of the private and public

spheres is based on the reduction of the individual to the desire to satisfy all his or her desires immediately (whether they are invented or not, whether they are conscious or not):³³ immediacy and desire become the cardinal values of society, and technological solutionism the means by which they are expressed. This first reduction is linked to a second: the individual and the reality that surrounds him or her are reduced to data that can be interpreted by the surveillance system. The way in which the world and individuals are conceived through datafication is the basis for the technology that will be used to organize and put them under surveillance. This relationship with technology is then turned into voluntary submission, since the question of freedom is no longer an issue: as a value, it is annexed and secondary. By concealing the real purpose of technological devices, NEOM orchestrates an implicit acceptance of surveillance for unknown, uncontrolled and undemocratic purposes. In other words, NEOM makes surveillance a *way of life*.

It proposes a society in which surveillance is widespread but targeted and individualised; the purposes of such surveillance are multiple and respond to different logics: economic, political, authoritarian, security or practical. Surveillance is total and all-encompassing: it reduces the individual to the object of surveillance, and private and public spaces merge into one surveillance space. In this respect, we should remember these few words by Julian Assange - which should have alerted us already:

That people determined to be in a democracy, to be their own governments, must have the power that knowledge will bring – because knowledge will always rule ignorance. You can either be informed and your own rulers, or you can be ignorant and have someone else, who is not ignorant, rule over you.³⁴

Such a vision of society is (and should be) a call for resistance.

³¹ For a detailed analysis, see B.C. Han, *Infocracy*, Cambridge, Polity Press, 2022; see also H. Arne, L. Dencik and K. Wahl-Jorgensen, *Digital Citizenship in a Datafied Society*, Cambridge, Polity Press, 2019 and S. Newell and M. Marabelli, *Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification'* in *Journal of Strategic Information Systems*, vol. 24, n. 1, 2015, 3-14.

³² In *Surveillance Studies*, Bentham is best known for his writings on the Panopticon, but it would be interesting to take a closer look at this concept of 'indirect legislation'. It is designed to enable states to govern individuals without resorting to criminal sanctions. Although it is rooted in penal law, Bentham intended to apply this type of indirect legislation to other areas of law. We also have to keep in mind that reducing alarm in society is part of utilitarian views. See M. Bozzo-Rey, A. Brunon-Ernst and M. Quinn (eds.), *Indirect Legislation: Jeremy Bentham's Regulatory Revolution*, in *History of European Ideas*, vol. 43, Issue 1, London, Taylor and Francis, 2017 and M. Quinn, *Bentham*, Cambridge, Polity Press, 2022.

³³ See B. Brecher, *Getting What You Want?: A Critique of Liberal Morality*, London, Routledge, 2012. The economic and moral dimensions of NEOM should not be underestimated.

³⁴ J. Assange quoted in M. Hastings, *Julian Assange: The Rolling Stone Interview*, in *Rolling Stone*, 18 January 2012, www.rollingstone.com/politics/politics-news/julian-assange-the-rolling-stone-interview-234403

An ethics of anonymity intends and proposes to provide the theoretical framework for such resistance, articulated around a critique of the processes of surveillance at work in societies, democratic or otherwise. In this way, anonymity marks a reversal of the process at work in the NEOM project. NEOM aims to abolish the private and public spheres in favour of a sphere of surveillance. Anonymity, on the other hand, proposes to reaffirm this distinction in a dialectical movement that aims to reintroduce a private dimension into the public sphere in order to limit and evaluate the processes of surveillance, or more precisely, to constantly question their legitimacy.

3.2. For an ethics of anonymity³⁵

3.2.1. Elaborating a concept of anonymity

However, such a project is not self-evident, since it has to be said that there are few attempts to philosophically conceptualise anonymity. But if we are to use anonymity as a framework for critical analysis of NEOM, we need a definition that allows us to conceptualise it. This is Wallace's project in his article 'Anonymity'. The interest of her analysis lies in highlighting the eminently social *and* communicative nature of anonymity, but also in emphasising that anonymity structures society and allows a demarcation between the public and private spheres.

Anonymity presupposes social relations. In other words, it is relative to social contexts in which one has the capacity to act, affect or be affected by others, or in which the knowledge or lack of knowledge of who a person is is relevant to their acting, affecting or being affected by others.³⁶

For Wallace, anonymity can be defined as the inability to link features (such as facial features) or characteristics that define a person in order to identify them as such.³⁷ Anonymity is relational and contextual, which makes it possible to define degrees of anonymity, multiple spheres of anonymity that are graded and non-exclusive. The advantage of this

definition is that it is highly dynamic and can take account of many situations, while insisting on the *a priori* axiological neutrality of anonymity. It also incorporates a form of temporality: anonymity may be ephemeral, but it presupposes a certain permanence. It is interesting to note that Wallace insists on the possible inter-contextuality of anonymity: it can persist in different contexts, to different degrees, but without disappearing altogether. The non-identifiability inherent in anonymity can therefore depend on both internal and external elements. This relationship between interiority and exteriority also allows us to add two other possible characteristics to anonymity: it can be deliberate or the result of complex social arrangements. The definition of anonymity is therefore cumulative: it is possible to define it in terms of several characteristics that reinforce it. Anonymity does not mean social isolation or being invisible in society. Anonymity presupposes the epistemic condition of a person's existence (we know they exist), but we are unable to define who they are, to identify them. To be anonymous, then, is not to know nothing about a particular person, but rather to have information that characterises a person and makes it possible to know their existence, without being able to link this characteristic information in such a way as to individualise the person, i.e. to identify them.

3.2.2. Anonymity and the concept of society

This concept of anonymity is linked to a concept of the individual and society. Anonymity (within a society) is never and can never be total, because the impossibility of linking the traits that characterise an individual – without denying the possibility of identification – is ultimately only possible if these different traits relate to different social spheres. In other words, in order to identify a person, it is necessary to establish a link between different characteristics that are present in different spheres. The underlying concept of society is therefore as follows: at the macro level, a society is a set of places that can either belong to other places or integrate different spheres. At the micro level, each place is a social sphere in which an individual can be located. It is therefore possible to conclude that:

Each person is a combination of interrelated traits; each trait is a position in a network of

³⁵ For a full development, see M. Bozzo-Rey, *Pour une éthique de l'anonymat*, in *Raison-publique.fr : arts, politique, société*, 2024, <https://raison-publique.fr/3432>.

³⁶ K.A. Wallace, *Anonymity*, in *Ethics and Information Technology*, 1, 1999, 24.

³⁷ K.A. Wallace, *Anonymity*, cit., 24.

relations or equivalently, the location of the person in an order. Every person *is* a combination of traits, *is* located in multiple orders.³⁸

A good example is anonymous medical testing: a person is randomly assigned a number that allows him or her to be identified or, more precisely, to be linked to a blood sample, for example. As a result, this number can only be linked to this sample and not to other characteristics of the person. This means that the person is identifiable in one particular sphere (the one involving blood samples, which we could call the 'hospital' location), but cannot be linked to other characteristics in other locations or spheres. The person is therefore anonymous, but their existence is known and they are identifiable by just one of their characteristics. We can consider the person to be anonymous precisely because there is no relational coordination between the different characteristics that would make it possible to identify exactly which person it is. The process of individualisation cannot be completed. What can we learn from this example? In a way, anonymity can be understood as questioning the consent of the relationship with the other and the place of the will in the relationship of recognition. From this point of view, anonymity refers to a fundamental freedom, that of showing oneself in relation to others. With such an understanding of anonymity, the totalising dimension of NEOM, which aims to remove the boundary between the private and the public and authoritarian spheres, becomes even clearer: society is reduced to individualised and individualising data whose sole function is to enable surveillance and influence behaviour. The relationship is no longer conceived as a relationship with the other, but as a mediation between a surveillance technology (whatever it may be) and a purpose external to the individual, whose consent is postulated without any real meaning being attached to it. The freedom to expose oneself in a relationship with another - this other is not necessarily an individual, but a social, political or economic institution - is denied and at the same time automated.

3.3. Could anonymity resist NEOM?

Unlike Saudi Arabia, European law offers

privacy protection through data protection legislation. This could explain why projects such as NEOM aim to eliminate the private sphere and merge the public and private spheres into a data-sphere that turns into a surveillance sphere. Anonymity could then be a grain of sand in the well-oiled machine of legitimation and social acceptance of a project like NEOM - assuming its designers attach any importance to it. An ethics of anonymity could then provide the essential elements to allow for the possibility of resistance to technological tools that promote particular forms of social - and political - organisation.

The first and probably most important difficulty facing an ethics of anonymity is the argument of security, which has been elevated to a cardinal value in the NEOM project. Security, both in the sense of physical security, but also in the sense of securing certain values: freedom, for example. In this respect, the discourse surrounding the use of video surveillance in the context of the Paris 2024 Olympic and Paralympic Games is striking: measures using mass surveillance technologies are presented in a positive light, as a guarantee of personal security while guaranteeing respect for fundamental freedoms. Let's take just one example from the mainstream media:

... QR codes, the key to free movement in Paris during the Olympic Games.³⁹

This kind of formulation is characteristic of the use of fiction, which aims to deconstruct reality to impose it more effectively, in particular by denying the question of temporality. While it is clear that not all actions - and especially contradictory actions - can be carried out simultaneously, fictional discourse seeks to free itself from any reference to the conditions under which they are possible.⁴⁰ It is therefore quite possible to promote a model of a 'free' society, but one in which surveillance is global and all-encompassing, a 'free' society in which freedom is attached to the possibility of constant surveillance. In a way, anything is

³⁸ K.A. Wallace, *Anonymity*, cit., 26.

³⁹ https://rnc.bfmtv.com/actualites/police-justice/jo-2024-ce-qu-il-faut-savoir-du-qr-code-pour-circuler-aux-abords-des-sites-olympiques-a-paris_AV-202405100094.html.

⁴⁰ This process is detailed and analyzed in M. Bozzo-Rey, *Influencer les comportements en organisation: fictions et discours managérial*, in *Le Portique. Revue de Philosophie et de Sciences Humaines*, 35, 2015.

possible: a society based on the individual, but without privacy; a society with unlimited access to data but based on freely consented provision.

3.4. Is anonymity a threat to public safety?

3.4.1. Gyges' ring

The relationship between anonymity and security therefore seems to be about the process of individual responsibility that would ensure security at a societal level – in other words, it is about the dynamic relationship between private and public, individual and society. The myth of the ring of Gyges presented by Platon is often used to illustrate the risks inherent in anonymity.

Gyges was a shepherd who found a ring that allowed him to become invisible through simple manipulation. What did he do with such a tool? He used it to seduce the queen and plot against the king, allowing him to murder her and seize power. Wallace refers to Plato's text to illustrate the idea that, thanks to the invisibility afforded by the ring, a bad person can commit reprehensible and unjust acts without being held accountable for them – because she cannot be identified as the person who committed these acts. Whatever the person's actions, it is impossible for the victims of injustice to hold the person responsible to account. In other words, invisibility is a way of evading responsibility for one's bad deeds and avoiding punishment. The shift from invisibility to responsibility was not Plato's aim: it is not so much to question individual responsibility as to examine the relationship between our actions and our conceptions of justice, in other words the sources of motivation for ethical action. Do we act ethically (or morally) only because of a disposition derived from an idea of morality, or because of laws that impose sanctions?

Wallace uses this myth as a paradigmatic example of the possible abuse of anonymity, establishing a causal relationship between anonymity (reduced to invisibility) and lack of responsibility, or more precisely, between anonymity and the impossibility of holding the perpetrator of the act to account – which could lead to increased insecurity and alarm in society.⁴¹ Security becomes a question linked only to individuals, without taking into

account some specific contexts. It is difficult to understand how, after all her definitional work, she could make such a claim. For to make it, she has to establish a strict equivalence between invisibility and anonymity, which is in contradiction – or at least a paradoxical relationship – with her own definition of anonymity. I believe that this equivalence does not apply *stricto sensu* and that a causal relationship cannot be inferred between the absence of liability and anonymity. Being invisible means that no one can see you, a *fortiori* recognise you, and therefore presupposes that no one knows that you are present in such and such a place. Being anonymous, on the other hand, implies that we know that a person is present in such and such a place, that he or she is performing such and such an action, or even that he or she possesses such and such a characteristic, but that it is not possible to trace this action directly back to its author. In a way, we can say that in the case of invisibility there is an action without a (visible) author, whereas in the case of anonymity there is an action with an author, but we have no coordinating characteristics that enable us to identify him.

Moreover, Wallace ignores a fundamental question raised by Gyges' ring: what are the reasons that drive us to act morally, what are our fundamental motivations? In other words, while it is possible to avoid responsibility in the case of invisibility, this is not entirely the case with anonymity. The problem is that to draw an equivalence between anonymity and invisibility is to simplify every instance of anonymity and reduce it to invisibility. While invisibility may rhyme with impunity, anonymity does not. Under these conditions, it is easy to understand that NEOM's aim, through the multiplication of data recovery devices, is in fact to eliminate the very possibility of individual anonymity in the public sphere, while at the same time ensuring total transparency of the public space, preventing individuals from becoming invisible. On the other hand, it means reducing anonymity to a negative dimension, forgetting that it can have a protective dimension. The other interesting point in analysing this myth is that it insists on two key elements. The first is the question of identity: the ability of an individual to define his or her own identity and the possibility – or not – of other individuals to understand the identity of others. The second element that

⁴¹ K.A. Wallace, *Anonymity*, cit., 30-32.

seems important to us is that it also invites to question the ability of an individual to put himself in the place of others and to pose as an impartial spectator to ethically evaluate an action. These two points seem to us to be fundamental to the development of an ethics of anonymity. Indirectly, it also emphasises the voluntary and consensual dimension of relating to others: not being anonymous means agreeing to relate to others. NEOM seeks to remove this possibility by replacing relationships between individuals with relationships between technological tools.

3.4.2. The question of responsibility: does anonymity necessarily lead to a crime without a perpetrator... but not without a victim?

One of the criticisms of anonymity (on the Internet) is formulated by Dreyfus, who considers that it is not a question of enabling individuals to become impartial spectators capable of evaluating situations, but rather of individuals who are not situated and detached from the situation and the actions they might carry out.⁴² The direct consequence would therefore be that anonymity is at the root of the feeling of disempowerment of individuals, due in particular to the process of distancing themselves from their actions, which reduces their involvement. In other words, anonymity allows people to cut themselves off from the system of social relations that underpins responsibility. Does such an argument deal a fatal blow to the concept of anonymity and its use to critique a range of technologies? We can already point out that we have insisted on the eminently relational dimension of anonymity and its connection to the different social contexts in which individuals can develop. But let's look at what such a statement implies or expresses, which may help us to understand better why the main aim is to discredit anonymity in the public sphere and, in the case of NEOM, in the surveillance sphere, understood as encompassing private and public spheres, which no longer exist as such.

The idea is to legitimise surveillance through accountability: if individuals are to be identified and known, it is to ensure that they are accountable for their actions. Social space - which would then merge the public and

private spheres into one globalised space, erasing their distinction - is structured by processes of identification, which become processes of individualisation of responsibility. We can therefore better understand why NEOM is based on surveillance systems and places so much emphasis on identifying in real time the perpetrators of actions - criminal or not: individuals must be identified in order to define the perpetrator of the actions for which they are held responsible. If we follow this logic, there are at least two conclusions: firstly, that the author of a given action becomes the only dimension worthy of interest - which presupposes the removal of the context in which this action was carried out: we are therefore faced with a process of reducing the individual to his or her actions; and secondly, that anonymity necessarily becomes a means of evading responsibility. Nor should we underestimate the importance of this real-time surveillance: the elimination of temporality prevents any contextualisation or real understanding of the reasons for a given act. If they were to be taken into account - and assuming that this is what NEOM provides for - it could only be a posteriori, which leaves room for many security and authoritarian abuses.

This line of argument seems to us to be an oversimplification in several respects. First, because of the slippery slope that reduces the process of accountability to finding the perpetrator of an act in order to punish him or her. There is a temptation to say that it is all about being able to 'identify a perpetrator'. Next, we need to distinguish between 'responsibility' and 'accountability'. More precisely, it is a question of distinguishing between responsibility, which consists in merely attributing an action to a moral agent, and responsibility, which requires moral agents to give an account, i.e. to have the possibility of identifying the inadequacies between what is expected of a moral agent and the way in which the latter succeeds or fails in meeting these expectations. Anonymity does not eliminate this form of responsibility. Moreover, it removes any consideration of the need to identify a victim for an action to be morally blameworthy. Finally, it effectively eliminates the protective dimension of anonymity and the benefit it can represent for the proper functioning of society as a whole. Anonymity therefore remains a concept that

⁴² H.L. Dreyfus, *On the internet*, London, Routledge, 2008.

can be used to make a normative assessment of a project such as NEOM.

4. Conclusion

To date, we have very little information about how and if the NEOM project will take shape. The delays are considerable and it seems that the various initial announcements will not be realised, at least not in their current form. Nevertheless, it is undeniable that the socio-technical imaginary on which NEOM is based, and the general social trends of which it is the culmination, must be noted and taken into account. It should be pointed out here that it would be illusory to use it as a form of society from which we are protected because we are members of democratic states. The peculiarity of surveillance technologies lies precisely in the removal of the various boundaries that structure social space: the distinction between public and private, the distinction between authoritarian and democratic regimes, and so on.⁴³ NEOM should therefore remind us of the need to resist these security trends, which aim to transform individuals and the various spaces in which they move into data that can be interpreted by surveillance systems. This is why we believe it is essential to build an ethics of anonymity that can reintroduce the distinction between public and private space, and that does not reduce the protection of the public to a dynamic of globalised but individualised and pervasive surveillance.

⁴³ This is not to say, of course, that all regimes are equivalent and that there are no enduring differences. However, it should be noted that these differences are sometimes normative rather than descriptive.

