The Ambivalence of Platforms: Between Surveillance and Resistance in the Management of Vulnerable Populations

Lorenzo Olivieri
Università di Bologna

Annalisa Pelizza
Università di Bologna

Abstract: This contribution aims to summarize and highlight the main themes emerged during the panel "Surveillance infrastructures or open platforms? Aid and control of vulnerable populations through digital data" that took place at the 8th STS Italia Conference. The panel invited to reflect upon the ambivalence and ambiguity of digital platforms and data infrastructures for population management as well as on the highly diversified functions and users they support and attract. More precisely, presenters were encouraged to enquire how platforms and data infrastructures affect vulnerable populations and reconfigure the boundaries between the private~~public~~ and public domains: how do they allow empowering and innovative communication and resistance strategies? How, on the contrary, do they produce novel or exacerbate already existing vulnerabilities? How is the modern distinction between government, business, and civil society de facto reshuffled as a consequence? Although panel's presentations discussed remarkably different types of platforms – from online maps and social networks to public health databases and migration technologies – they overall emphasized that only a careful, situated analysis of the multiple socio-technical factors shaping users' engagement might help to understand how – and why – those technologies become tools for control and surveillance or empowerment resources.

Keywords: Platforms; surveillance, resistance, vulnerable populations, data infrastructures.

Submitted: November 22, 2021 – **Accepted:** January 31, 2022

Corresponding author: Lorenzo Olivieri, Università di Bologna, Dipartimento di Filosofia e Comunicazione, Via Azzo Gardino 23, Bologna, Italy. Email: lorenzo.olivieri3@unibo.it.

1. Introduction

In his seminal article, Gillespie (2010) stressed how the semantic richness and ambiguity of the term "platform" allowed firms to attract users, clients and advertisers by promising an open, neutral and egalitarian space. The term, he suggested, could be connected to four semantic territories – computational, architecture, figurative and political – which overall "point to a common set of connotations: a 'raised level surface' designed to facilitate some activity that will subsequently take place" (Gillespie 2010, 350). Through this semantic and discursive escamotage, firms attempt to obscure and alleviate the tensions between "user-generated and commercially-produced content, between cultivating community and serving up advertising, between intervening in the delivery of content and remaining neutral" (Gillespie 2010, 348).

One decade later, digital platforms have become even more ubiquitous and increasingly able to attract multiple, heterogenous types of users, who gather around their services in order to accomplish a continuously expanding set of actions. In this respect, our panel "Surveillance infrastructures or open platforms? Aid and control of vulnerable populations through digital data" aimed to shed light on some of the tensions which were not addressed by Gillespie's analysis. First, we decided to focus on a specific typology of users – vulnerable people and vulnerable populations – and on a specific type of data – sensitive and personal data. Second, but strongly connected to the previous point, we asked to reflect upon the dialectic between power and resistance, between aid and surveillance, which shapes the use of online platforms.

In proposing a discussion about this two-fold tension crossing the multiple uses and appropriations of platforms, we suggested to broaden the scope of the analysis in order to include data infrastructures which are not usually considered in the ranks of platforms, such as those for migration management. This move, we think, is needed in order to question and problematize what is usually perceived as a 'division of labor' between the biopolitical traits and purposes associated to institutional data infrastructures and the emancipatory, self-empowering features usually connected to digital platforms. This rigid distinction does not seem satisfactory: on the one hand, data infrastructures for population management provide access to healthcare and shelter; on the other hand, digital platforms and their data have increasingly become new sources of surveillance and control (Manokha 2018; Wood and Monahan 2019).

2. The Role of Digital Infrastructures in the Control and Empowerment of Vulnerable Subjects

The contributions to our panel addressed these issues along three main topics. First, the hybrid and open nature of online maps and social media was analyzed in terms of resistance and surveillance (Montanari and Olivieri). Second, presenters highlighted the blurred boundaries between digital, private platforms and public services during the Covid pandemic (Varvara Boboch) and between health data stored in medical platforms and the possible risk of co-optation of those data for control and surveillance purposes (Della Torre). A third set of presentations explicitly addressed data infrastructures for migration management by analyzing the 'scripts of alterity' through which migrants are enacted by the European information systems (Pelizza), by showing how the principle of non-refoulment is jeopardized by the datafication and digitalization of European borders (Fill), and by focusing on the issues of data quality and data frictions between migrants' identities and the standards and interfaces available in information systems (Van Rossem).

Montanari's talk addressed the ambivalent nature of online platforms by focusing on maps and mapping. As a matter of fact, maps, and especially online maps, add a further level of complexity, as they are simultaneously interfaces, representations, and tools. As pointed out by authors like Mitchell (2002), Latour (1990) and Farinelli (2009), maps have historically been vectors of cognitive, perceptive and social transformation. It is thus their highly hybrid nature that makes maps powerful tools allowing for both surveillance and control, and for solidarity, aid and cooperation. Today, maps and mapping constitute the basic elements of infrastructures and social media, and, as a consequence, they have also emerged as pillars of contemporary surveillance capitalism. Drawing on these insights, Montanari's contribution enquired how the polymorphous nature of maps allowed to provide and support aid, solidarity and resistance. More specifically, his work has investigated how maps allow the representation of the so-called 'Balkan route' as a site in which multiple types of solidarity and struggle have stratified over the years.

Olivieri's presentation discussed how border-crossers' smartphones, and the data stored in them, have become new means of surveillance. His work drew upon interviews collected at Greek Hotpsots as well as on a recent body of literature (Latonero and Kift 2018; Bolhuis and van Wijk 2020) which have shown how the vetting of smartphones and social media is an increasingly common practice during both registration and identification procedures conducted at the Hotspots, and the asylum process. These security checks allow extracting different types of data from smartphones and laptops in order to assess migrants' stories and identities through content that is generated in non-securitarian and non-institutional contexts. The

novelty represented by this modality of surveillance is that it seems to contrast with 'the epistemic suspicion towards the story' which characterizes biometric technology (Ajana 2013). By taking into account content produced by migrants in non-institutional contexts, smartphone and social media surveillance seem, at first glance, to be able to recover and foreground their stories and narrations. Yet, the vetting of smartphone and social media ends up reproducing and enhancing power relations: the content extracted and analyzed is always partial, deleted content can be retrieved without consent, the interpretation of data is done by officers. As a consequence, rather than filling the gap between identity and identification, social media surveillance and digital forensic technologies ultimately produce a proliferation of spokespersons (Pelizza 2021) which enact border-crossers in different, contrasting and unjust ways.

In Varvara Boboch's contribution, the implementation of apps and services for digital contact tracing during the COVID-19 pandemic represented a precious opportunity to explore the relational frictions and the co-productive processes at stake in the collaboration of private and public services. In April 2020, Google and Apple joined their forces to develop an Exposure Notification System (GAEN) which replaced the EU's previously developed options and enabled interoperability between Android and iOS devices using apps from public health authorities. These circumstances made particularly visible the co-production of power-relations. On the one hand, private platforms are considered reliable and invisible, provide public services on their own and, unlike public institutions, have the ability to transform a risk or crisis situation in a commercial opportunity. On the other hand, public institutions are both regulators and users of those platforms, while simultaneously being concerned with the organization of trust. The reciprocal dependency of public and private sectors became even more relevant during the COVID-19 pandemic, when digital, private platforms emerged as the main resilient actors, to the extent that essential public services became dependent on them. Yet, private companies still need to operate within a set of rules stipulated by institutional actors: privacy, interoperability, data management and lawful implementation then become the core issues to be clarified and implemented within a coherent regulatory structure. In this regard, one of the main obstacles highlighted by the contact-tracing case was policy-makers' struggle to produce consistent guidelines and propose feasible alternatives to private companies. However, Boboch argues, public and private bodies' need to access a large volume~~number~~ of high-quality data, as well as the urgency to determine the governance of data collection, make difficult to achieve a balance between individual rights and public health. Overall, the experience with apps for digital contact-tracing leaves with more questions than answers: how can public and private actors earn citizens' trust? Is the private going public or, vice versa, is the public going private? Can secondary usage such as surveillance be prevented?

The problems of health data – or, more precisely, of the access to such data – was also addressed by Della Torre's contribution. Her presentation focused on refugees' medical records and on the risks of instrumentalization and misuse of such data. It relied on interviews conducted with doctors and social workers working in French health structures~~hospital structures specialized in the case of precarious subjects~~, such as the Permanances d'access aux Soins de Santè (PASS), ~~health structures~~ providing access to care and medication to people living in the streets, people without social security and migrants. The research revealed, first of all, that the digitalization, data collection and exchange of patient medical records is significantly underdeveloped and poorly harmonized, leading to inefficient situations. However, most of the interviewees did not express any specific concerns about the possible misuse of medical records and felt to be in control over the data collected. This perception, according to Della Torre, might be due to the major role played by secrecy and confidentiality for professionals like doctors and social workers. A second element which might explain the perception of low risk is the logic of care associated to the PASS, which, despite not being an autonomous structure, is thought to work regardless any possible issues linked to migratory flows. However, these elements are not, per se, sufficient to exclude the possible, future misuse of medical data for purposes of migration management and control, especially in the light of the relationship between the Ministry of Interior and the Ministry of Health. To mitigate these risks, Della Torre suggested a few strategies, such as the minimization of data collection and the use of paper medical records, as they are generally perceived as more secure.

Pelizza's presentation discussed how the categories and modalities of classification utilized in European data systems for information management enact different typologies of people on the move. Crucial in her argument is the shift from a representational understanding of identity to one based on the performativity of practices, doings and actions. This shift suggests paying particular attention to the mediums, or chain of translations, through which identities are built, which are especially important when it comes to the technologically mediated management of populations. Drawing on empirical analysis of the data models implemented in information systems used at the European borders, Pelizza identified four typologies of intended border-crossers, four 'scripts of alterity' which show how intended people, with their own skills, goals, limitations and capabilities, are inscribed into databases for migration management. First, the several functions (administration, security, health care, family reunification, etc~~.~~) allowed by the data collected in the Greek register of foreigners are seeing a~~nd~~s ~~s~~ enacting people on the move as long term foreigners, eligible for integration. On the other hand, Eurodac – the European database storing asylum seekers' fingerprints ~~–~~ – contains significantly ~~fewer~~ less data. The scarcity of data collected suggests that Eurodac

tends to enact people on the move as irregulars migrants who are expected to cheat and to remain in Europe for a short period. Along similar lines, by collecting only information about possible aliases, physical features and episodes of violent conduct, SIS II (the European Schengen Information System) enacts people as potential criminals. Lastly, the categories contained in the European Visa Information System (VIS), the databases used to process third-country nationals' Visa applications, enact people simultaneously as a travelers and as a settled individuals. Yet, this paradox is only apparent: the type of intended individual inscribed in the VIS is in fact the settled non-Western traveler.

Fill's contribution addressed the tensions and contradictions of the European system of international protection by focusing on the principle of non-refoulment. According to it, Member States are forbidden from returning asylum seekers to countries in which they might be in danger or subjected to persecution. Yet, as Fill showed, this principle is systematically violated by European countries through three different modalities of rejections: pushback, pullback and back-scattering. Pushbacks occur at the external borders of Europe and they are the most documented and violent violation of the principle of non-refoulment. Pullbacks depend on the increasing involvement of third-countries authorities which allow externalizing border control through strategies of non-arrival, remote control and deterrence. Lastly, the implementation of smart borders made possible what Fill defined as 'back-scatterings', a term used, in physics, to describe the reflection of waves, particles, or signals back to the direction from which they came. Through a network of interconnected biometric databases and through the aggregation of data which allows identifying who is suspect and to develop risk analysis, smart borders in fact operate a distinction between trusted and untrusted travelers, configuring a regime of 'border apartheid' which digitally exclude people from accessing the European territory. Smart borders then reproduce a systematic and discriminatory bias towards migrants, creating a 'data banned population' (Bigo 2014) based on categories and identification processes implemented in bureaucratic and algorithmic systems. Particularly interesting, in this regard, is the Eurosur project, a system of systems which supports European member States in the monitoring of the Mediterranean Sea and of the European external borders. By visualizing maps as operational areas and by expanding the capabilities to operate in those pre-frontier areas, Eurosur justifies preventive actions based on the analysis of potential migratory flows.

Whereas Fill's presentation foregrounded the functions of surveillance characterizing migration technologies, Van Rossem's contribution focused on issues of data quality in the infrastructures for migration management. Crucially, problems with data quality and data frictions might significantly hamper the respect of people's fundamental rights. As highlighted by the Fundamental Right Agency

(FRA 2018), European Information Systems often contain inaccurate alphanumeric, biographic and biometric data. This situation negatively affects people's possibilities to exert their rights and might eventually lead to accuse them of something they never did. This might occur, for instance, when an issue of low data quality is misrepresented, by authorities, as one of identity fraud. One of the major reasons for which the information might be incorrect or incomplete is that migrants' identities data do not always fit neatly in information systems' categories. Personal data, in fact, might be inputted in two different systems with slight but relevant differences, leading to what policy-makers define as 'blind-spots'. Such blind-spots could be solved through interoperability, which would allow to detect inconsistencies in the records. Van Rossem's presentation discussed the 'smart search and match' technology used in migration and border control in order to overcome data frictions and to match biographical data.

3. Conclusions

As this short summary demonstrates, despite the heterogeneity of platforms taken into considerations, the seven contributions to the panel have engaged with the ambiguity of platforms. An ambiguity that suggests the need to look for the sociotechnical conditions under which a platform can be used either for control purposes, or for empowering goals. When do mobile social networks stop supporting self-empowerment and become surveillance tools? What uses can turn institutional data infrastructures for population management into resources of care? As the STS tradition reminds us, only situated, performative and inclusive research can help to answer these questions.

References

Ajana, B. (2010) *Recombinant identities: Biometrics and narrative bioethics*, in "Bioethical Inquiry" 7, pp. 237–258

Bigo, D. (2014) *The (in)securitization practices of the three universes of EU border control: Military/Navy – border guards/police – database analysts*, in "Security Dialogue", 45 (3), pp. 209-225.

Farinelli, F. (2009) *La crisi della ragione cartografica*, Torino, Einaudi.

Gillespie, T. (2010) *The politics of 'platforms'*, in "New Media & Society", 12 (3), pp. 347-364

Latonero, M., and Kift, P. (2018) *On the digital passageways and borders: Refugees and the new infrastructure for movement and control*, in "Social Media + Society", Special Issue Forced Migration and Digital Connectivity, pp. 1-

11.

Latour, B. (1990) *Drawing things together*, in M. Lynch and S. Woolgar (eds), *Representation in scientific practice*, Cambridge, MIT Press, pp. 19-68.

Manokha, I. (2018) *Surveillance: The DNA of Platform Capital - The Case of Cambridge Analytica Put into Perspective*, in "Theory & Event", 21 (4), pp. 891-913.

Mitchell, T. (2002) *Rule of experts: Egypt, techno-politics, modernity*, Berkeley, University of California Press.

Pelizza, A. (2021) *Identification as translation: The art of choosing the right spokespersons at the securitized border*, in "Social Studies of Science", 51 (4), pp. 1-25

Wood, D. and Monahan, T. (2019) *Editorial: platform surveillance*, in "Surveillance & Society", 17 (1/2), pp. 1–6.