Every Breath You Take, I'll Be Watching You. Explicit Surveillance and Algorithmic Countersurveillance in Healthcare

Every breath you take, I'll be watching you.
Explicit surveillance and algorithmic countersurveillance in the health care

INTRODUCTION

In this chapter we explore resistance practices applied to algorithmic surveillance in the health domain, with a specific focus on the Italian contact tracing app 'Immuni' specifically developed to contrast the COVID-10 pandemic. Algorithmic resistance is indeed a specific reaction against power of algorithms as largely described in the literature (Velkova and Kaun 2021). Although localised within the Italian context, we believe that the Immuni app is a good case to reflect on some interesting aspects since it entails some key features of algorithmic resistance in general and introduces it an up-to-date case study for health control. First, Immuni could represent an apt starting point for observing a very peculiar form of algorithmic surveillance – typical of governmental contact tracing apps – that we can label as *explicit*. In fact, contrary to most systems of algorithmic surveillance – which are by definition opaque and invisible[1] (Schellewald, 2022) – the surveillance purposes of contact tracing apps are crystal clear to everyone. Therefore, it becomes very interesting to reflect on how resistance functions in such an 'open system' of surveillance. Second, as several contact tracing apps launched during the pandemic emergency, Immuni was a 'fiasco' (White & Van Basshuysen, 2021); since not enough users downloaded it as well as it was harshly criticised by the public opinion since the beginning (Bosa et al., 2021). Another reason often associated with Immuni's failure is the low penetration of smartphones; as shown in a paper by Shahroz and colleagues (2021) the success of digital contact tracing depends largely on user adaptability and older devices (or smartphones running out-of-support versions of mobile operating systems) are unable to use these apps.Immuni represents a good starting point to observe the specific role played by users' practices of resistance in determining these kinds of 'surveillance failures and resistance activities to algorithmic surveillance that, in other words, brought to its failure.

Boyd et al. (2014) describe algorithmic surveillance as "along with information about who you know, technical mechanisms that underlie the "big data" phenomenon – like predictive analytics and recommendation systems – make imputations about who you are like, based on your practices and preferences" (p. 54). Additionally, the rapid growth of algorithmic surveillance has left many important questions unasked. Therefore, it becomes of great import to better understand how people react to such ubiquitous systems of health monitoring and if, and to what extent, put in motion measures of *countersurveillance* to contrast them – and to what purposes.

Countersurveillance is the task of making surveillance difficult or to avoid it, and can be employed by individuals and communities to protect privacy, civil rights, and against abuses regarding personal information and sensitive data in public spaces, online and offline (Wood & Thompson 2018). Additionally,

[1] See for example those algorithmic systems delivering targeted advertising or suggesting the consumption of specific cultural contents (Airoldi, 2021).

countersurveillance may be engaged to put pressure on the public and private surveillance systems by identifying potential vulnerabilities and errors (Monahan, 2006). In the contemporary digital society most of countersurveillance activities are directed towards algorithmic systems of surveillance (Ettlinger, 2018), such as: cookies, bots, traced payments, recommendations filtering, and (of course) tracking health apps (O'Donnel, 2014). One of the main practices through which algorithmic countersurveillance manifests is *resistance* (Wood & Thompson, 2018), consisting in sabotaging specific digital devices of monitoring by manipulating them, spreading negative word-of-mouth about them, or (simply) avoiding using them (Marx, 2003). Anyhow, despite being central to the dynamics of surveillance, the concept of resistance remains underdeveloped within the surveillance studies corpus (Treré, 2018); and especially so regarding the emerging phenomena of health contact tracing apps – which started popping-up all over the world soon after the COVID-19 pandemic – as well as explicit surveillance.

To this purpose, in the present contribution, we explore the practises of resistance users develop around the Immuni app. To do that we implemented an explorative qualitative analysis of Reddit conversations, aimed at: a) mapping the online discourses emerging around Immuni, and b) identifying possible strategies of resistance towards the app. Specifically, our analysis was aimed at answering the following research questions: *What kind of discourse users articulate around the Immuni app? Which are the main sources of concern? Which are the main narratives emerging from such discourse? Which kinds of practices of resistance are possible to derive from such narratives? What is the role of digital media in shaping the practices of resistance?* These questions contribute to the analysis of resistance as a specific feature of those processes connected to algorithmic care (see Chapter 1) and more in general to analyse current developments in the contemporary health management.

The case of Immuni is a particularly relevant entry point to tackle those processes: indeed, it is an "explicit" device of surveillance although is less invasive compared to other apps (Di Salvo & Milan 2020) the public debate around it expressed several criticisms re-igniting the issue of privacy in a datafied society increasingly depending on algorithms and platforms (Id). For our case, this engaged in forms of resistance. Moreover, it seems that it is the very digital public sphere (Schäfer, 2015) that enables individuals to monitor and countersurveil top-down health measures. We address this point by discussing what we call the *paradoxes* of explicit algorithmic surveillance. The chapter is structured as follows: in the first paragraph we discuss the aims and logics of functioning of contact tracking apps in the health domain (with a specific focus on COVID-19), and connect this to relevant literature on algorithmic surveillance and countersurveillance. In the second paragraph we present the Immuni app case. The third paragraph describes the methodology of our digital analysis. Fourth and fifth paragraphs are dedicated to the description and discussion of results. The chapter closes with a review of the outcomes of our research and proposes future paths of research overcoming the limits of our explorative study.

COVID, ALGORITHMS AND COUNTERSURVEILLANCE PRACTICES

Besides security, health is one of the areas that most applies to surveillance. The relationship between surveillance and medicine is often thought of in terms of monitoring risk factors that could compromise the health status of a population. Efforts are made to control various aspects of life, with the aim of developing prevention programs to keep people from getting sick, from epidemiology to classification manual, it is possible to notify how procedures, methods, sophisticated imaging, robotics and other technologies are applied to understand and control certain conditions. This whole set of knowledge and technologies is extremely important to governments for the elaboration of health policies, disease prevention and the general wellbeing of the population. Algorithmic surveillance is surveillance performed by technology with the use of algorithms and it has the potential to drastically improve patient outcomes. Such technological interventions seemed promising to many governments that started developing different protocols for implementing digital health solutions on mobile devices (Vaudenay, 2020). At the same time, the plethora of digital and technological tools for information gathering purposes makes surveillance activities constantly more complex and difficult to detect.

These features are imbricated in the attempts to manage COVID-19 pandemic. The pandemic has placed a huge strain on the health care system globally. From the very beginning, the ongoing COVID-19 has shown an "epidemiological turn in digital surveillance" (Taylor et al., 2020, p. 11), marked by corporate and national initiatives to contain the pandemic. This strategy became increasingly important in order to avoid the collapse of the hospital system and to preserve a high level of care for most critical COVID-19 cases (e.g., oncological cases).

Among the many non-pharmaceutical interventions (Murtas et al., 2021), several governments invested in the development of digital contact tracing tools; they consist of a set of procedures and digital technologies which rely on smartphone apps to track and notify contacts of positive people in a more efficient way.

If contact tracing is one of the predominant methods for containing the virus, algorithms can be used to analyse the data collected (Collado-Borrell et al., 2020). This data can be captured using personal smartphones, which can be nowadays understood as a comprehensive and systematic way of collecting contact information. Therefore, algorithms can process data from contact tracing in order to provide users with risk assessment, referring to the risk that an individual may be infectious and, therefore, must quarantine, on the same digital device. Automated real-time digital distribution via algorithms means contact tracking and risk assessment in COVID-19 are closely linked, and the same device will allow the input data and the output risk status (Liu & Graham, 2021). Despite its promises, contact traces application opened up a large debate, since many scholars critiqued the process of particular country risk assessment and the consequential violations for civil liberties (Kitchin, 2020). We mention, *inter alia*, different examples, such as China (Liu & Graham, 2021), the United Kingdom (Edwards et al., 2020), Poland (Nielsen, 2020), and Russia (Ilyushina, 2020).

Public health programs related to surveillance initiatives rely on what Amstrong theorised as a "fundamental remapping of the spaces of illness" (1995, p. 400). This change has broadened the boundaries of medicine and painted a new picture of the relation between health and disease, so as to promote (through control over the

population) a widespread welfare system. COVID-19 has revealed how everyone is directly or indirectly affected by a consistent surveillance regime (Lyon, 2022).

A general criticism to algorithms for risk assessment consists in smartphones to be representative of the general population. Prediction models for predictive performance failed in several cases, sometimes because of the overwhelming number of people infected or detected as potentially infected, sometimes because some individuals started to "sabotage" the inherent surveillance sense of this process.

Following the assumptions above, the present research proposes a reflection on practices of countersurveillance in the healthcare field taking stock of experience of 'Immuni' case. Countersurveillance is the practice of making surveillance activities of institutions difficult or implementing technologies to evade surveillance altogether. Monahan (2006, p. 515) defines countersurveillance as "intentional, tactical uses, or disruptions of surveillance technologies to challenge institutional power asymmetries". It follows a rationale of surveilling those doing the surveillance (Marx, 2003), promoting accountability, and rendering more transparent instances of state agents' brutality and misconduct (Wilson & Serisier, 2010).

Countersurveillance achieves its goal by subverting various components of the surveillance process (Wood & Thompson, 2018) and it has many practices and applications. It can be used to protect privacy, civil liberties, and against abuses of surveillance. Additionally, it may be employed to push surveillance systems beyond their breaking point and in doing so it identifies potential vulnerabilities and points of error. Many countersurveillance techniques use human methods rather than electronic. Monahan stated (2011, p. 515) that countersurveillance can include different practices, such as "disabling or destroying surveillance cameras, mapping paths of least surveillance and disseminating that information over the Internet, employing video cameras to monitor sanctioned surveillance systems and their personnel, or staging public plays to draw attention to the prevalence of surveillance in society."

Most of countersurveillance practices can be performed online, where individuals resist to algorithmic systems in different ways, in order to "expose wrongdoing, express opinions, mobilise protest, monitor elections, scrutinise government, deepen participation, and expand the horizons of freedom" (Diamond, 2010, p. 70). Penny and Dadas (2014) stressed how social media dynamics, and particularly those spaces away from the mainstream media structures, bring different possibilities to subvert the traditional order, including e-mobilization, citizen journalism, second-hand circulation, online deliberation or e-tactics.

Digital networks are acquiring a more prominent role as a political and social change instrument, since mobile communication is a recurring tool in protests and demonstrations. For instance, Hermida and Hernández-Santaolalla (2018) show through their research on Twitter and video activism how the citizen media and participatory journalism converge on the concept of countersurveillance. Finally, it is worth mentioning that countersurveillance can be also enacted *with* and *within* algorithmic systems themselves. As several data activism initiatives have shown, by manipulating algorithms' inputs and outputs, it is possible to expose their embedded social biases and power relations (Velkova & Kaun, 2021).

Similarly, countersurveillance practices and discourses within the healthcare system show how people can resist algorithms by interacting with them or avoiding its use. For instance, recent research published by Liu

and Graham (2021) probed how Chinese make sense of Health Code – the national contact tracing and risk assessment algorithmic assemblage – showing a consistent and active interaction with it.

THE ITALIAN CONTACT TRACING APP…A STORY OF FIASCO?

Related to the pandemic, one of the earliest examples of surveillance initiatives proposed by numerous governments are contract-tracing proximity apps, which imply the potential to alert users and authorities when a user's phone had come into proximity with a COVID-19-positive person (Morley et al., 2020). In the fight against the COVID-19 epidemic, Italy was one of the first countries adopting many measures including digital contact tracing and risk assessment algorithms. Starting in spring 2020, the Italian government has begun a media campaign encouraging people to download the country's COVID-19 track and trace app as infection rate rises again.

The national operations of Immuni began, thanks to the implementation made by Apple and Google, on June 15, 2020. Once the app was compatible with the two main operating systems for mobile devices (Android and Ios) it was ready to be activated in order to show whether the user has come into contact with an infected person as a main function. The app uses Bluetooth Low Energy (BLE) technology, when two or more subjects are physically close, their smartphones send their pseudorandom ID (derived from the current UUID and renewed every 15 min) to each other via BLE. The app assesses the risk of the encounter based on its duration and the distance between the two smartphones. Immuni also sends to the server some analytical data. These include epidemiological (i.e., details of encounters) and operational information and are sent for the purpose of helping the Italian National Healthcare Service to provide effective assistance to users (Martin et al., 2020). Through Immuni, and if all users collaborate by reporting information, it is possible: a) identifying individuals who has been clinically confirmed as having COVID-19; b) classifying epidemiologically main contacts of that individuals; c) communicating with that list of contacts to advise them of potential exposure, d) linking them to public health officials, diagnostic services, or self-isolation information.

However, as stated in the app commercial description, Immuni does not (and cannot) collect any data that would identify the user, such as their name, date of birth, address, telephone number, email address or GPS data – (it only accesses specific smartphone's functions: connection to wifi networks, stand-by, Bluetooth, boot execution)[2]. Since June 2021, the App is one of the access points to get the EU Digital COVID Certificate, a digital document implemented at EU level to facilitate safe free movement of the European citizens during the pandemic. More than 21 million people downloaded Immuni and roughly 194.000 notifications have been sent[3].

As health authorities have pointed out, the more people download the contact-tracing app, the better it will become at notifying users of whether they may have been in contact with an infected person. Some research shows a generally positive attitude towards digital contact tracing (DCT) apps, as highlighted by Altmann and colleagues (2020). However, issues of cyber security, variable risk perception, and poor awareness of benefits

[2] https://www.immuni.italia.it/funzionamento.html.

[3] https://www.immuni.italia.it/dashboard.html.

have been indicated as barriers to their use (Walrave et al., 2020; Chen & Thio, 2021). In their provocative article *What went wrong with the Immuni contact-tracing app in Italy?*, Isonne and colleagues (2022) presented their results of a cross-sectional study administered to students enrolled in the healthcare area, showing that use of the DCT app was relatively limited. As shown by the research, the main problem is that contact tracing requires a strict and unambiguous organisation, while Immuni has shown confusion, scarce information and often worsened the already complicated scenario. Additionally, many devices currently in use are running older versions of iOS and Android software, while others are not able to run the app. More specifically users have argued that the app had low download rates because of privacy reasons. This aspect is more relevant when the data is related to very sensitive issues, such as health conditions. People questioned whether their health data would be in safe hands once transferred to the Immuni platform. Second, users shows a kind of *a priori* distrust towards the Italian State that leads them to harshly criticise the app as well as not using it. As a third level of criticism, people's trust and mistrust in the App Immuni services is not only about how it detects risk but also how its function is implemented. Although Immuni raises the alarm when people meet a potential positive, it gives such inadequate and often late data that it is difficult to trace contacts. All these concerns lead users to enact different (but yet quite passive and micro) practices of resistance, namely: a) not to download the app; b) uninstall the app; c) to have the app on the smartphone but not to use it; d) to use the app in a different way than required; e) to engage in negative online word-of-mouth.

METHODOLOGY

The goal of the research is to explore how Italian citizens adopted countersurveillance tactics towards the Immuni contact tracing app. Many authors frequently investigate countersurveillance in the context of avoiding and disrupting surveillance (Marx 2003; Monahan, 2006) or increasing the visibility of police misconduct (Bradshaw, 2013). Indeed we can hypothesis that users might not have downloaded the app because of privacy reasons. People might have questioned whether their health data would be in safe hands once transferred to the Immuni platform (Shahroz et al 2021). Second, especially during the pandemic, a widespread feeling of *a priori* distrust towards the Italian State emerged and this may have led to a refusal of the app (Bainotti 2021). Besides these two levels of criticism, people's trust and mistrust in the App Immuni services might be related to how its function is implemented (. Taking stock of these hypothesis in this chapter, we examine how users engage online about the Immuni, by questioning it and discussing (possible) practices to resist it. Particularly we addressed the following research questions:

- *What kind of discourse users articulate around the Immuni app?*
- *Which are the main sources of concern?*
- *Which are the main narratives emerging from such discourse?*
- *Which kinds of practices of resistance are possible to derive from such narratives?*
- *What is the role of digital media in shaping the practices of resistance?*

To answer them we carried out an analysis of Reddit. Reddit can be considered as an 'alternative platform', where users engage in a more liberal debate, compared to the leading social media platforms like Facebook or Twitter, which often suspended and removed a variety of individuals and groups (Rama, 2021). To develop our study on Reddit's conversations, we implemented a content analysis based on digital methods (Niederer, 2016), which consists in a hybrid approach that blends "computational and manual methods throughout the content analysis process" (Lewis et al., 2013 p. 39). We took advantage of computational techniques to: a) automatically extract posts from Reddit; b) organise such data in a structured data set; c) perform operations of data management (Caliandro & Gandini, 2017 p. 194). While we submitted the posts we retrieved from Reddit to a qualitative analysis, in order to better identify and interpret discourses and narratives embedded in them (Caliandro et al., 2021).

Specifically, to collect our data, we employed an hoc Python script programmed to interrogate Reddit's API and retrieve specific threads of conversation from the platform (submissions in the Reddit jargon), along with the related comments[4] (Rama, 2021). First, we searched the subreddit 'r/italy' by means of the query 'app + immuni', from the 1st of March 2020 up until the end of December 2021. In this way, we have been sure to run into relevant submissions, that is, threads of conversation: a) written by Italian users discussing about the Italian situation; b) mentioning the App independently from the spelling form used, 'app immuni' or 'immuni app'; c) posted in a period of time that was consisted with the 'rise and fall' of Immuni App. Once launched the script within subreddit 'r/italy', we retrieved 65 submissions dealing with the Immuni App. After that, we sorted the submissions by the number of comments, discarding 57 threads which hit 1 or 0 comments. We left with 8 relevant submissions, which are listed in Table 1.

Tab. 1 – Thread App Immuni

Submission	Score	Comment	Time
Il MIT sta tracciando e valutando tutte le app Covid19	673	521	2020
L'app di tracking "Immuni" per gestire i contagi da coronavirus è closed source, e perché questo è un importante problema	1k	375	2020
Cosa ne pensate di questa ignoranza generale dell'utente medio sui social riguardo la privacy	251	152	2021
Scaricherete l'app Immuni? Perché sì e perché no?	43	126	2020
Chi ha ucciso l'app Immuni e perché	16	93	2021
App Immuni: come si usa e come funziona - Guida dettagliata	5	5	2020
Flop app Immuni!	12	4	2021
Immuni e consumo energetico	23	2	2021

Then, we launched again the script to collect all the comments contained in the list of submissions - obtaining a total of 1,446 of single comments. Finally, we manually coded a sample of 500 comments, taken from each

[4] We are very grateful to Dr Ilir Rama (ilir.rama@unimi.it), who built the script and gave us access to it.

of the 8 submissions. We reached this number by saturation. This sample was analysed through a qualitative and manual content analysis (Altheide, 1987). The construction of the coding categories followed an iterative process, insofar as the categories were not defined *a priori* but instead gradually emerged during the observation of the texts through a constant and collaborative examination by the two authors (Caliandro & Anselmi, 2021). Specifically, we identified four categories: *privacy and data protection*, *ideological reflections*, *technical issues*, *other* (see Table 1 for the coding book). The data analysis was carried out by the two authors (without relying on external coders), who organised regular and collective sessions of discussion and coding – where disagreement was addressed and, eventually, resolved (Lacy et al., 2015).

Tab. 2 – Coding book. The table describes the category we used to analyse our data

Category	Description	Example
Privacy and data protection	Affecting the individual perception of data-surveillance. Feeling at risk of being monitored, Surveillance, and the process of algorithmic control are visible to all.	*This app is a free pass to Google and all the companies that steal our data* *the purpose is to track people not stop the disease*
Ideological reflections	It includes person's impression of the national response to COVID (from the mediatic campaign to the implementation of the digital contact tracing)	*Our government claims higher than actual number of downloads* *I don't trust Conte and the five stars movement*
Technical issues	Technical failures and external barriers	*My device is too old and can't handle the battery consumption* *Older people are the ones who would need it most but do not know how to use smartphones. What's the point of that?*
Other	Residual category	😕 😕*Immuni*

Beyond counting the categories, and thus focusing on the *manifest* content of the posts, we paid attention to their *latent* content as well (Sjøvaag et al., 2012), trying to identify the narratives users articulate around each topic of discussion (Georgakopoulou, 2021). This approach was conducive to identify the main forms of resistance towards Immuni that users describe, discuss, imagine, plan and/or enact.

Discussing countersurveillance tactics and algorithmic resistance

As mentioned above, most of the comments tend to cluster into three main thematic categories, which are evenly distributed in our dataset: *privacy and data protection* (29%), *ideological reflections* (36%), and *technical issues* (31%); plus *other*, 4%). In the following paragraphs, we describe the narratives emerging around each topic of conversation, from which it is possible to derive the main concerns users express about Immuni, and, in turn the practices they develop to resist it.

Privacy and Data Protection

Most of the reactions showed aversion and criticism, mainly due to the risk that these apps may not fully guarantee users' privacy.

> I'm concerned about my privacy, I'm concerned about how my data will be handled (furthermore since it is data about my health). The fact that the data is deleted on December 31st [2020] seems ridiculous to me, what if the pandemic continues? They will make a law to extend the validity of data retention. And then who guarantees me that data will be deleted for sure?[5]

> Privacy-wise, I'd rather not use a private company app. Your data that you consider so unimportant goes to enrich American capitalists. Who do you think controls Amazon, Google, Visa, Mastercard, Apple, Facebook, the ministry servers? Do you think they care about your privacy?

Despite the app clearly stating that the location privacy of users is protected by not collecting location data, many people were still concerned about downloading Immuni, because they are not used to being explicitly traced. They fear that such (purported) systematic extraction of location data will pave the way for a future Orwellian-like dystopia.

> I don't like being watched every step I take. I believe it is another step that normalises the surveillance state that Snowden, Assange, Manning and others have been trying to warn us about for a long time.

> Do you really want to have your movements tracked at any time? No thank you. Seriously speaking, this app will also be open source and whatever you want, but it's still the first step towards [Orwell's] 1984.

The ongoing pandemic has shown a tangible and quick application of different surveillance measurements. In a short period of time, large amounts of research, studies for vaccines, tests for detection, forms for identification of patients, and applications from geolocation to indicate areas of higher incidence of the virus for prevention have been applied. According to some users, sharing some personal details might lead to a surveillance as 'social sorting' (Gandy, 1993), where the State categories and evaluates citizens by assigning them an individual score.

[5] All the comments displayed in this chapter have been translated from Italian by the two authors. We deem this necessary procedure also more respectful for users' privacy, since, in this way, their original statements are more difficult to retrieve by means of web search engines (Bainotti et al., 2021).

> Ok but in the future somewhere keys and names will meet right? What prevents the state from matching codes and people? The less the state records me, the happier I am. Do you feel secure about your privacy? Then download it ... I won't

In general, all these concerns about privacy, data management and the purported Orwellian State brought about Immuni's invasion of privacy, that to a specific countermeasure as reported below.

> I didn't install Immuni on my smartphone! No way!

> My girlfriend doesn't download it because she says it's useless...how can I blame her?

> Yup, removed it the next day.

Users enacted drastic although simple practices of resistance, that is, not to download the app or uninstall it if they already downloaded.

Ideological Reflections

As briefly anticipated, many users have been resistant to downloading the app, citing concerns about privacy. However, the use of Immuni can also be influenced by negative attitudes towards the government that reverberate on individual opinions about the app. In this sense, we below is possible to note how users are not prone to give Immuni a chance precisely because of distrust to the Italian government. Here some users' comments:

> No, I don't trust what ends up in the hands of the Italian state; and the less information they have the better it is.

> I don't trust the IT security of the Italian state.

> In general I don't like police state, and especially so if enforced by the Italian state.

Another aspect of distrstrut towards the government is well represented in those comments in which users explicitly admit not to follow the institutional recommendations – showing an individual response to the recommended measurements:

> I prefer to keep my distance and take my precautions, I am not a person in contact with other people, I will not go to aperitifs, I do not go to the gym.

> I am not in contact with masses of people, indeed apart from shopping, with very few people.

To conclude, the general sentiment of distrust toward the Italian government brings people to resist Immuni by not downloading it (*When they announced it* [Immuni] *I laughed. I hope anyone with any sense of sanity didn't download it*). Anyway, differently from what we saw in the previous paragraph, the motivations here are more 'individualistic': users are not so much concerned about privacy (which, although personal, is a fundamental civil right), they simply refuse to do what the State tells them to do. In this sense, their practices of resistance are a little bit more articulate, since, beyond not downloading the app, they also develop alternative and 'homemade' strategies for contrasting the virus (e.g., not going shopping or out for a drink).

Technical Issues

This third category shows how people's resistance builds upon the fact that notifications are followed by a non-linear process. Most of the time the app does not report a potential contact until the user launches the app, so it is counterintuitive. On the other hand, even when Immuni works properly (e.g. notifying a contact) might lead to false positives or false negatives alerts. The notification is sent when a "dangerous contact" happens on a specific day for at least 15 minutes. But the app does not specify neither where the contact happened nor the exact time, making it almost impossible for some categories (health care workers) to assess the situation with this data.

> There may be false positives in fact the app collects data to "calibrate" the distances on the BLE. I don't feel like quarantining myself "by mistake".

Additionally, the epidemiological and operational analytics in Immuni backend, is not sufficiently protected. According to online comments, it is necessary to avoid any possible reidentification of data subjects, informing users about the specific types of data processing with such analytics and which data are collected for different categories of data subjects.

> The BLE is not a reliable system to steal precise distances, the same creators of Bluetooth said so.

> I was going to take a test and whilequeuing I received the notification that I had been in contact with a positive ... what useless.

Additionally, a mobile contact tracing app needs to be widely adopted by a population for it to be of benefit; this is challenging to achieve. Many devices currently in use are running older versions of iOS and Android software, which remain incompatible with Immuni and its BLE (Bluetooth Low Energy) technology.

> I have an old version of android that doesn't support it, it doesn't even appear in the playstore. My smartphone, even if it is 4 years old, works well and I have no intention of changing it

My phone is too old :(

The widespread adoption of contact tracing apps requires that people would have access to a smartphone and, in most cases, access to a reliable internet connection. Some users suggested making the privacy information notice and the alert more legible, considering that also older people must use the app. Proximity by itself is not enough to determine the risk of someone being exposed to the virus. There are several other parameters involved, such as being indoors or outdoors, being in a room with good air circulation or not, etc. The exposure alert may not correspond to real risks because some exposures happened in contexts with adequate health safeguards. Healthcare operators recommend different approaches when their patients receive an alert by Immuni, also considering that another weakness in the notification system is data upload. Only at the end of 2020 healthcare operators and public officials uploaded codes of infected people in the national database (Ussai et al., 2022).

I work as a nurse and I was working when I got the alert…My doctor told me to ignore it!!

The narrative emerging from the comments clustering around the topic *technical issues* depicts a very interesting scenario. It seems that among those citizens willing to download the app on their smartphones and actively use it, the major technical glitches and flaws of Immuni failed them – along with the National Health Systems that seems 'uncoordinated' with the app. In response to this situation, probably imbued with frustration, users started engaging in three main practices of resistance against Immuni: a) to have it on their smartphone but not to use it (*I downloaded it but I'd rather disinfect my house and stay away from people than use it*); b) to use it in a 'different' way than required (*I downloaded it but I keep bluetooth always off so I don't get notifications*); c) spreading negative word-of-mouth (*I told my parents not to download it*).

From a privacy perspective, the resistance demonstrated thus appears to be related to the improper functioning of the app itself rather than a generalized distrust for the control system. The Immuni app has been criticized by users primarily for lack of support and material difficulties in its use. Backward compatibility is a significant negative aspect as the technology does not fulfill the subject's expectations and thus disregards the promises of reducing the effective reproductive number, or the number of infected individuals. In decentralized digital contact tracking systems (Cohen et al., 2020), the user is in fact in control of the data and decides whether or not to upload it to a central server. Although this approach is less privacy intrusive (Barrat et al., 2020; Currie et al., 2020; Ferretti et al., 2020) than a centralized system, in which with a top-down architecture the data is collected from the smartphone through an app and is stored in a remote central server. it struggles to ensure that sufficient data is collected for contact tracing (Gasser et al., 2020).

DISCUSSION AND CONCLUSION

The analysis we provided here informs the broader reflection about algorithmic care from a different entry point. Although explorative, our digital analysis allows us to articulate some interesting reflections on resistance towards explicit systems of algorithmic surveillance.

Our data show that users, through the online discourse they articulate on Reddit, express three main concerns about Immuni: privacy, distrust toward the Italian State, and technical functioning. In turn, these concerns trigger users to enact a variegate set of resistance practices (although admittedly quite passive and micro, namely: a) not to download the app; b) uninstall the app; c) to have the app on the smartphone but not to use it; d) to use the app in a different way than required; e) to engage in negative online word-of-mouth. Many scholars disagree over the idea of intent, the extent to which resistant individuals must see themselves as resisting. The relevance of public recognition is also unclear. Scholars have differing opinions on whether or not resistant acts that go unnoticed still count as resistance (Hollander & Einwohner 2004). Anyway, there exists a conspicuous stream of literature, mostly related to political and consumer culture research (based on qualitative methods), which frames invisible and micro practices such not voting, not following a particular influencer, not clicking on a given website, etc., as 'resistance' (Christensen, 2011; Casemajor et al., 2015; Audy Martínek et al., 2022). This is mainly because the very actors playing out such practices consider them as resistance acts. Moreover, the narratives emerging from the different users' comments, permit to draw some general conclusions on Immuni, intended as an 'explicit' system of algorithmic surveillance and its related practices of resistance. Specifically, we argue that it is possible to identify two 'surveillance paradoxes' that doomed the destiny of Immuni from the start. On the one hand, since Immui is a 'governamental app', the Italian State had to necessarily disclose and make clear its surveillance purposes. La maggior parte dei commenti in questa direzione solleva problemi etici e di privacy legati ai dati personali. Secondo gli utenti, ed in linea con alcuni studi (Ferretti et al., 2020; Nguyen et al., 2020), la necessità di informazioni epidemiologiche non dovrebbe portare alla violazione della privacy dei dati personali. I governi dovrebbero creare un quadro giuridico che garantisca la privacy dei dati personali per ottenere la fiducia dei cittadini. As a result, many citizens immediately started to be critical towards the app, expressing their criticism mostly on social media – (which in many cases amplified their voices). To put it simply: *if one knows of being surveilled she will very likely resist it*. On the other hand, we saw that many users were willing to download Immuni (and being surveilled, so to speak), but the app failed them, due to the many technical glitches and flaws.

Digital tracing, when tied to smartphones alone, must take into account socio-demographic variables (who has such tools) and the devices themselves in their technical conformation (how those tools work). In addition to problems of a technical nature, whereby, for example, some older smartphones were unable to support app updates, it is also interesting to note the digital literacy of some users, particularly with relation to age group. Indeed, remarkably low usage was noted among the elderly, the group most affected by COVID-19 (López et al., 2021).

Again, we can observe that such technical issues seem to depend on the 'public' nature of the app. Differently from commercial apps (e.g., Facebook or Google), Immuni couldn't take full control of users' smartphones, but instead had to respect specific privacy protocols, having limited access to users' data. Thus, the very

technical capabilities of Immuni impaired its proper functioning from the beginning. At any rate, as a result, the once enthusiastic Immuni users stopped using it, and started voicing their discontent on social media. Furthermore, as we observed in users' comments – independently from the reasons why they averse Immuni –, social media are not mere megaphones for users' criticism, but become 'virtual repositories' of concrete practices of resistance, through which users can actively sabotage contact tracking apps. To put it simply: *if one wants to be surveilled but no one surveilles him/her, s/he will stop being compliant with surveillance*.

Therefore, we can conclude that one of the main reasons why Immuni failed is the very digital public sphere (Schäfer, 2015) for which it has been designed. In fact, on the one hand, the digital public sphere set too strict technical constrains for the app to function properly; on the other hand, it offers users the very tools (particularly social media) to criticise and resist the app.

While the ideologies and intentions of those who engage in counter-surveillance are many and disparate, in this chapter we have focused on the creation of conversational and communicative spaces in which specific forms of resistance come to life. And in fact, the users participating in conversations about Immuni on Reddit seem to be part of a specific category ones. The comments we analysed appear to be posted by users with a high interest towards Immuni (for example, as an excuse to criticise the Italian government) as well as endowed with a notable digital literacy (since they discuss proficiently about digital privacy, data protection, and specific technical features of the app). Hence, it can't be safely said that their critical opinions and related practices of resistance represent those of the ordinary citizens who downloaded Immuni or heard talking about it. Anyhow, it is important to stress that, being an explorative qualitative analysis, our research was not meant to generate representative results, but to observe specific cultural processes. In this case, meaningful participation in counter-surveillance is linked to certain social, technological, and political conditions of user experience. It has been observed that counter-surveillance agents may have immediate practical goals, such as not downloading the app or otherwise misusing it, as well as symbolic acts of resistance with the intention of raising awareness of modern surveillance regimes and challenging institutional power asymmetries... Obviously, the technical and social dimensions of all technologies are deeply intertwined, (Bijker, Hughes, and Pinch Citation1987; Bijker and Law Citation1992) and constitute the sites of intervention where counter-surveillance tactics take shape.,

LIMITS AND FURTHER RESEARCH

Although we deem our digital exploration provided some interesting insights, it presents, of course, some limitations too. We decided to analyse the conversations around the Immuni app because we deemed it an 'emblematic' case to start reflecting on explicit algorithmic surveillance and the related forms of resistance. Anyway, even though it is based on an emblematic case, the results of our analysis can't be considered representative. This is mainly because of our source of empirical data: Reddit. Reddit can't be considered representative for the entire Internet population: only 7.6% of Italian internet users use Reddit – a fair good share, but nothing compared to the percentage of Facebook (78.6%) or Instagram (71.4%) (WeAreSocial, 2022).

Given these limits, we believe that, in order to have a more complete understanding of explicit algorithmic surveillance and resistance, further research should take into consideration a broader spectrum of social media platforms, to be studied with a systematic integration of quantitative (e.g., topic modelling) and qualitative techniques (e.g., ethnographic observations) – necessary to get a more comprehensive mapping of online critical discourses and resistance activities.

Ackowledgement

This work was supported by Fondazione Cariplo (Bando 2020, Ricerca Sociale: Scienza Tecnologia e Società. Project name: "The value of digital data: enhancing citizens' awareness and voice about surveillance capitalism (V-DATA)"– https://vdataresearch.com/).

REFERENCES

Airoldi, M. (2021). *Machine habitus: Toward a sociology of algorithms*. John Wiley & Sons.

Altheide, D. L. (1987). Reflections: Ethnographic content analysis. *Qualitative Sociology*, *10*(1), 65-77.

Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S., & Abeler, J. (2020). Acceptability of app-based contact tracing for COVID-19: Cross-country survey study. *JMIR mHealth uHealth*, *8*(8), e19857.

Amstrong, D. (1995). The rise of surveillance medicine. *Sociology of Health and Illness*, *17*(3), 393-404

Audy Martínek, P., Caliandro, A., & Denegri-Knott, J. (2022). Digital practices tracing: studying consumer lurking in digital environments. *Journal of Marketing Management*, 1-31. https://doi.org/10.1080/0267257X.2022.2105385.

Bainotti, L., Caliandro, A., & Gandini, A. (2021). From archive cultures to ephemeral content, and back: Studying Instagram Stories with digital methods. *New Media & Society*, *23*(12), 3656-3676.

Boyd, d., Levy, K., & Marwick, A. (2014). The networked nature of algorithmic discrimination. In S. Gangadharan (Ed.), *Data and discrimination: Collected essays* (pp. 53-57). Open Technology Institute – New America Foundation.

Bosa, I., Castelli, A., Castelli, M., Ciani, O., Compagni, A., Galizzi, M. M., ... & Vainieri, M. (2022). Response to COVID-19: was Italy (un)prepared?. *Health Economics, Policy and Law*, *17*(1), 1-13.

Bradshaw, E.A. (2013). This is What a Police State Looks Like: Sousveillance, Direct Action and the Anti-Corporate Globalization Movement. *Critical Criminology*, *21*(4), 447-461.

Caliandro, A., & Gandini, A. (2017). *Qualitative Research in Digital Environments: A Research Toolkit*. Routledge.

Caliandro, A., & Anselmi, G. (2021). Affordances-based brand relations: An inquire on memetic brands on Instagram. *Social Media+ Society*, *7*(2), https://doi.org/10.1177/20563051211021367.

Caliandro, A., Garavaglia, E., & Anselmi, G. (2021). Studying ageism on social media. An exploration of ageing discourses related to Covid-19 in the Italian Twittersphere. *Rassegna Italiana di Sociologia*, *62*(2), 343-375.

Casemajor, N., Couture, S., Delfin, M., Goerzen, M., & Delfanti, A. (2015). Non-participation in digital media: toward a framework of mediated political action, *Media, Culture & Society*, *37*(6), 850-866.

Chen, A. T. Y., & Thio, K. W. (2021). Exploring the drivers and barriers to uptake for digital contact tracing. *Social Sciences & Humanities Open*, *4*(1), 100212.

Christensen, H. S. (2011). Political activities on the Internet: Slacktivism or political participation by other means?. *First Monday*. https://journals.uic.edu/ojs/index.php/fm/article/view/3336.

Collado-Borrell, R., Escudero-Vilaplana, V., Villanueva-Bueno, C., Herranz-Alonso, A., & Sanjurjo-Saez, M. (2020). Features and functionalities of smartphone apps related to COVID-19: systematic search in app stores and content analysis. *Journal of Medical Internet Research*, *22*(8), e20334.

Diamond L. (2010). Liberation Technology. *Journal of Democracy*, *21*(3), 69-83.

Di Salvo, P. & Milan, S. (2020). The Four Invisible Enemies in the First Pandemic of the "Datafied Society", Open Democracy, 8 June, https://www.opendemocracy.net/en/can-europe- make-it/four-invisible-enemies-in-the-first-pandemic-of-a-datafied-society/

Edwards, L., Veale, M., Lynskey, O., Coldicutt, R., Loideain, N. N., Kaltheuner, F., ... & Bietti, E. (2020). The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates. Preprint, 13 April. *LawArXiv*. https://osf.io/preprints/lawarxiv/yc6xu/.

Ettlinger, N. (2018). Algorithmic affordances for productive resistance. *Big Data & Society*, *5*(1), https://doi.org/10.1177/2053951718771399.

Gandy, O.H. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Westview Press.

Georgakopoulou, A. (2021). Small stories as curated formats on social media: The intersection of affordances, values & practices. *System*, 102, 102620.

Hermida, A., & Hernández-Santaolalla, V. (2018). Twitter and Video Activism as Tools for Counter-Surveillance: The Case of Social Protests in Spain. *Information, Communication & Society*, *21*(3), 416-433.
Hollander, J., & Einwohner, R. (2004). Conceptualizing Resistance. *Sociological Forum*, *19*(4), 533-554.
Ilyushina, M. (2020). How Russia is using authoritarian tech to curb coronavirus. *CNN*. https://edition.cnn.com/2020/03/29/europe/russia-coronavirus-authoritarian-tech-intl/index.html.
Isonne, C., De Blasiis, M. R., Turatto, F., Mazzalai, E., Marzuillo, C., De Vito, C., ... & Baccolini, V. (2022). What Went Wrong with the IMMUNI Contact-Tracing App in Italy? A Cross-Sectional Survey on the Attitudes and Experiences among Healthcare University Students. *Life*, *12*(6), 871.
Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society*, *20*(1), 14-29.
Lacy, S., Watson, B. R., Riffe, D., & Lovejoy, J. (2015). Issues and best practices in content analysis. *Journalism & Mass Communication Quarterly*, *92*(4), 791-811.
Lewis, S. C., Zamith, R., & Hermida, A. (2013). Content analysis in an era of big data: A hybrid approach to computational and manual methods. *Journal of Broadcasting & Electronic Media*, *57*(1), 34-52.
Liu, C., & Graham, R. (2021). Making sense of algorithms: Relational perception of contact tracing and risk assessment during COVID-19. *Big Data & Society*, *8*(1), https://doi.org/10.1177/2053951721995218.
Lyon, D. (2022), *Pandemic Surveillance*. Polity.
Martin, T., Karopoulos, G., Hernández-Ramos, J. L., Kambourakis, G., & Nai Fovino, I. (2020). Demystifying COVID-19 digital contact tracing: A survey on frameworks and mobile apps. *Wireless Communications and Mobile Computing*, *2020*, 1-29.
Marx, G. T. (2003). A tack in the shoe: Neutralizing and resisting the new surveillance. *Journal of Social Issues*, *59*(2), 369-390.
Monahan, T. (2006). Counter-surveillance as political intervention?. *Social Semiotics*, *16*(4), 515-534.
Monahan, T. (2011). Surveillance as Cultural Practice. *The Sociological Quarterly*, *52*(4), 495-508
Morley, J., Cowls, J., Taddeo, M., & Floridi, L. (2020). Ethical guidelines for COVID-19 tracing apps. *Nature*. https://www.nature.com/articles/d41586-020-01578-0.
Murtas, R., Morici, N., Cogliati, C., Puoti, M., Omazzi, B., Bergamaschi, W., ... & Russo, A. G. (2021). Algorithm for individual prediction of COVID-19–related hospitalization based on symptoms: development and implementation study. *JMIR Public Health and Surveillance*, 7(11), e29504.
Niederer, S. (2016). *Networked content analysis: The case of climate change*. Amsterdam University Press.
Nielsen, N. (2020). Privacy issues arise as governments track virus. *Euobserver*. https://euobserver.com/health-and-society/147828.
O'Donnell, C. (2014). Getting Played: Gamification, Bullshit, and the Rise of Algorithmic Surveillance. *Surveillance & Society*, 12(3), 349-59.
Penney, J., & Dadas, C. (2014). (Re) Tweeting in the service of protest: Digital composition and circulation in the Occupy Wall Street movement. *New Media & Society*, *16*(1), 74-90.
Rama, I. (2021). The Coronavirus Conversation on Reddit: A Mixed Methods Approach. *Culture e Studi del Sociale*, *6*(1), 175-192.
Schäfer, M. T. (2015). Digital Public Sphere. In G. Mazzoleni et al. (Eds.), *The International Encyclopedia of Political Communication* (pp. 322-328). Wiley Blackwell.
Schellewald, A. (2022). Theorizing "Stories About Algorithms" as a Mechanism in the Formation and Maintenance of Algorithmic Imaginaries. *Social Media+ Society*, *8*(1), https://doi.org/10.1177/20563051221077.
Sjøvaag, H., Moe, H., & Stavelin, E. (2012). Public service news on the Web: A large-scale content analysis of the Norwegian Broadcasting Corporation's online news. *Journalism Studies*, *13*(1), 90-106.
Taylor, S., Landry, C. A., Paluszek, M. M., Groenewoud, R., Rachor, G. S., & Asmundson, G. J. (2020). A proactive approach for managing COVID-19: the importance of understanding the motivational roots of vaccination hesitancy for SARS-CoV2. *Frontiers in Psychology*, *11*, 575950.
Treré, E. (2018). From digital activism to algorithmic resistance. In Meikle, G. (Ed.), *The Routledge Companion to Media and Activism* (pp. 367-375). Routledge.
Ussai, S., Pistis, M., Missoni, E., Formenti, B., Armocida, B., Pedrazzi, T., & Mariani, I. (2022). "Immuni" and the National Health System: Lessons Learnt from the COVID-19 Digital Contact Tracing in Italy. *International Journal of Environmental Research and Public Health*, *19*(12), 7529.

Vaudenay, S (2020) Centralized or decentralized? The contact tracing dilemma. Cryptology ePrint Archive 2020: 1–31.
Velkova, J., & Kaun, A. (2021). Algorithmic resistance: Media practices and the politics of repair. *Information, Communication & Society*, *24*(4), 523-540.
Walrave, M., Waeterloos, C., & Ponnet, K. (2020). Adoption of a contact tracing app for containing COVID-19: A health belief model approach. *JMIR Public Health and Surveillance*, *6*(3), e20572.
WeAreSocial (2022). Digital in 2021. *WeAreSocial.com*. https://wearesocial.com/it/blog/2022/02/digital-2022-i-dati-italiani/.

White, L., & Van Basshuysen, P. (2021). Without a trace: Why did corona apps fail?. *Journal of Medical Ethics*, *47*(12), e83-e83.
Wilson, D., & Serisier T. (2010). Video Activism and the Ambiguities of Counter-Surveillance. *Surveillance & Society*, *8*(2), 166-180.
Wood, M. A., & Thompson, C. (2018). Crowdsourced Countersurveillance: A Countersurveillant Assemblage?. *Surveillance & Society*, *16*(1), 20-38.