The Vitreous Refugee

Lintner, C.ᵃ

(a) Researcher of Sociology of Cultural and Communicative Processes, Freie Universität Bozen, mail claudia.lintner2@unibz.it, ORCID: 0000-0002-8705-767X

ABSTRACT

Taking the example of smartphones, the article discusses the impact of digital technologies on refugee trajectories considering the ambivalent potential of technologies to generate simultaneously new opportunities for refugees' agency and new structural constraints regarding their mobility and actions due to control capacities. It therefore aims to offer a deeper discussion of the empowerment-control nexus and promote a better understanding of the various intersections that are developing between digitalization and migration/mobility patterns. The article is based on a qualitative research approach. Linking the individual level (the need of refugees to use smartphones for communication, information and orientation) to the political level is an emerging international market of surveillance and security technologies that has developed in recent years. Technology firms have contributed to develop and to promote the digital turn in surveillance and security-focused practices based not exclusively on the physical body, but on the digital devices as 'extended bodies'.

Claudia Lintner[1]
The vitreous refugee[2]

1. Theoretical Introduction

This article critically examines the practice of smartphone surveillance and thus the extraction of personal data as a common control practice in different European countries by addressing issues of digital agency, privacy and data protection in the context of refugees and asylum seekers. The primary aim is to put forward the idea that the understanding of the impact of digital technologies on refugee trajectories has to consider the ambivalent potential of technologies to generate simultaneously new opportunities for refugees' agency and new structural constraints regarding their mobility and actions due to control capacities. Following this research focus, the article is part of an emerging interdisciplinary strand of research, that of digital migration studies, which focuses on studying migration in, through and from the digital lens (Leurs and Prabhakar, 2018). By drawing on Candidatu *et al.* (2018), Leurs and Prabhakar (2018) define three possible research focuses that investigate the migration-digitalization nexus: first, migrants in cyberspace; second, the everyday experiences of digital migrants; third, migrants as data. In line with this definition, the present paper brings together agency- and structure-oriented research approaches that allow for deeper insights into the interplay of migration and digitalization patterns. The paper refers to several empirical research studies that focus on the enabling aspects that new communication technologies provide to people on the move. They do this by opening up new perceptions and imaginations, and possibilities of proximity independent of space and time (Diminescu, 2008) as well as new information channels along their mobility experiences (Latonero and Klift, 2018; Gillespie *et al.*, 2016). In line with recent digital sociological approaches (Lupton, 2012, 2013; Orton-Johnson and Prior, 2013), social and other digital media are understood as inherent parts of everyday life and thus inherent features that constitute and configure social life-patterns of human behaviour, social relationships and concepts of the self (Lupton, 2012). Linked to this, it can be argued that virtual spaces have lost their 'exotic edge' and have transformed into an 'embedded, embodied and everyday part of social life' (Hine, 2015, p. 164). Therefore, more than ever before, new mobile technologies are rooted in everyday life activities and are used in very different ways depending on the needs and specific life contexts (Madianou and Miller, 2012). As a result, virtual spaces do not exist as 'a single cultural artefact' (Hine, 2015, p. 36), but as 'multiple and variable cultural objects' (Hine, 2015, p. 164).

The present paper also refers to recent literature, in particular from critical migration studies (Nedelcu and Soysüren, 2018) and critical border studies (Horst and Taylor, 2014), that focuses less on individual experiences and more on surveillance and control practices that increasingly make use of digital technologies and datafication (Leurs, 2013). In the context of forced migration, the development of technologies has led to new forms of governmentality with new protagonists (governments, traffickers and [private] corporations) following the attempt to shape and control subjects, as well as organizing smuggling. Hence, whereas from the bottom-up, migrants use smartphones and apps to access information, maintain transnational relations, establish local connections and send remittances, different scholars point to an ever-increasing digital infrastructure which institutes new forms of governmentality and makes people on the move highly vulnerable to surveillance by others (Leung, 2011; Nedelcu and Soysüren, 2020). Following Lyon's (2001, p. 2) definition, surveillance is defined as 'any collection and processing of personal data, whether

identifiable or not, for the purposes of influencing or managing those whose data have been garnered'. Ball and Webster (2004, p.134) underlines that 'surveillance is the practice of gathering and sorting data with the explicit purpose of influencing and managing the data target'. The new mobile and interactive media embodied in Web 2.0 platforms and devices are dispersed and multimodal; a web of nodes that incorporates presumption but also constant surveillance and information-gathering on users (Beer, 2013; Beer and Burrows, 2013; Lash, 2007). Lyon (2004) points out, innovations in technological surveillance and control practices have become more and more integrated into daily lives. They penetrate into areas of life that were previously only marginally monitored or not monitored at all.

Following this line of argument, Lyon (2004) introduces the concept of social sorting; more precisely, the attention to individual and personal data and details involved in surveillance practices that produces new vulnerabilities, particularly in the context of forced migration. In line with this, new developments in ICT via large information systems give governments new possibilities not only to control external borders (Broeders, 2009; Karandidou, Kasparek, 2018), but also to trace, control and identify so-called 'unwanted' (unauthorized) migrants. New technological possibilities in combination with politically motivated events of terrorism, like 9/11, have undoubtedly accelerated this development in surveillance trends and (digital) control practices of refugees on a global scale (Huysmans, 2006).

Now, looking to surveillance practices from a complete and totalizing Foucauldian perspective—as the panoptic ideal type would have us believe—would be too short-sighted. This refers in particular to electronic surveillance practices and the question of how individuals connect to and use digital devices. By using social media platforms, other communication channels and different apps to gather information, refugees not only rely on an ever-increasing digital infrastructure to facilitate their flight experience, but also supply digital systems with intimate and personal information, leaving behind digital footprints that make them traceable.

Against this background, the present article aims to offer a deeper discussion of the empowerment-control nexus and promote a better understanding of the various intersections that are developing between digitalization and migration/mobility patterns. The article thus joins the broader research strand of a digital sociology, which focuses on digital practices that change social relations and provide both new inclusions and spaces of action, and new exclusions and vulnerabilities.

2. Methodology

The paper is part of the project DIBO (Digital Border Experiences of Refugees and Asylum Seekers), which has been carried out by the [name of institution]. It investigates and critically evaluates the role that ICT (in particular mobile phones) plays for refugees in places of forced immobility around the border area of the Brenner Pass.

The article focuses on the smartphone as both an enabling and constraining digital device in the refugee context. It discusses new possibilities that facilitate refugees' experiences and new vulnerabilities and exclusion mechanisms that can be identified by the increasing practice of smartphone surveillance, following the attempt to shape and control subjects entering the European Union (EU).

The research adopted a qualitative approach to understand the complex settings, using semi-structured interviews and document analysis. The results build on a data set which is composed of 17 semi-structured and narrative interviews conducted with refugees and asylum seekers who are currently in the Italian northern border zone, from December 2019 to May 2020. The majority of the results presented are, however, based on an additional data set composed of 10 expert interviews in different European member states (UK, Germany, Denmark, Belgium, Netherlands, Greece). These interviews were carried out from September 2020 to December 2020. Additionally, a document data

set has been collected that includes newspaper articles, documents on different legal situations and case reports, etc.

Data collection and analysis were intertwined and interdependent. Document analysis followed a three-step process that comprised skimming/reading, interpretation and the organization of information into categories (Bowen, 2009). Similarly, the analysis of the interviews was based on the open coding process described by Strauss and Corbin (1994). In this process, the analysis concentrated on the conceptualization and categorization of the research data. The smaller parts of the transcripts were first analysed deeply to grasp the core idea, which was described within a code. These analysed parts were then compared, appropriated and summarized under the same code and/or related to other codes/concepts of higher order (categories). The coding process was supplemented by using maps as per the research strategy developed by Clarke (2003).

3. Results: the importance of smartphones in everyday life

Drawing on the analysis of the interviews on the personal use of smartphones, conducted with asylum seekers and representatives of non-governmental organizations (NGOs) at the Italian border with Austria and in southern Germany, it was highlighted that smartphones are among the most important tools that refugees and asylum seekers carry with them. One representative of an NGO in Germany outlined: «One of their biggest concerns is often where to charge their smartphones. They are often their only connection to friends and family in their countries of origin. They are at the same time a translation aid, a means of communication and a repository of digital memories'». This was confirmed by the interviews with refugees and asylum seekers in northern Italy who are currently stuck at the Italian border with Austria. Bilar, a young man from Guinea, outlined: «I always have my phone in my jacket. I always take it with me. I do everything with it». Smartphones have become a vital tool for refugees and asylum seekers in two respects: first, as a means of communication to keep in touch with their country of origin, especially with family and friends; second, as a tool to orient themselves quickly in new environments. Fahir an asylum seeker from Senegal, outlined: «Facebook, WhatsApp, all this stuff allows me to get in contact with my family, my life left behind. I am here but I am also there, through [the] Internet». This constructed co-presence via the digital world allows refugees and asylum seekers to remain part of a life that they have left behind. Similarly, another asylum seeker, currently forced to stay in the northern Italian border zone, gave some personal insight into what this co-presence really means in everyday life: «When my mother died, they shared the picture through Facebook because I have to see her. There is no other way. You understand».

As these findings show, in the refugee context, identity and relationship cultivation practices are now increasingly moving towards social networking and smartphone applications. Thus, co-presence is not only about exchanging news, information, etc., but also about sharing emotions via digital platforms. The digital space accessed mostly via smartphones is a personal space that give access to the most intimate information, but also gives insights into broader religious and political networks in which they are embedded: «This is a WhatsApp group for Mandinka people anywhere in the world. This is for [those] who are staying outside Gambia. They are in Europe or somewhere because of the work. Because they want to learn. Because the Mandinka is very deep. They want to learn their culture and to understand their language. Therefore, if you join this group, you can hear many, many words in Mandinka. So, you understand». The analysis also give insights into how refugees and asylum seekers use smartphones in daily life to orient themselves quickly in new environments: «I am learning English, I am leaning German and Italian and Arabic via YouTube, and here I watch these learning videos». However, smartphones also represent important tools for people to protect themselves in new environments. Farid, currently living on the streets at the border with Austria, stated: «When the police prevented us from sleeping under the bridge, my friend called me and told me not to return there. We usually communicate by phone. When the police are there, it is better not to return, so you are safe. Otherwise, you never know what might happen».

The use of smartphones can be seen as a prime example of the increasing interweaving of our everyday lives with digital technologies and the associated complexity of today's media environments. This was particularly evident in other interviews with undocumented refugees who tried to cross the Brenner border and continue their way to Austria and Germany: «I communicate with my friends who are already in Germany. They tell me about the situation at the border, then I will know. When there are fewer controls, I will go…I use Facebook and WhatsApp, yes. We are always in contact». Similarly, another interviewee stated: «Next time I will make the reservation online, as my friend told me, very quick then you pay and you travel to the border on the Flixbus. You do not come into contact with the police». These data show that by using the smartphone in different ways in everyday life, refugees and asylum seekers provide very personal, confidential information that may allow conclusions to be drawn about their networks, family, country of origin and experiences. In doing so, their smartphones open a door to their past, to their present and to their future. This is what digitalization means: every search query is a statement about their interests; every photo they post on a social network reveals where they are or were. Horst and Taylor (2014) emphasize that the digital agency of refugees and asylum seekers must thus be understood as partial and fragile, as their access to information is, most of the time, 'insecure, unstable and undependable' (Wall *et al*., 2015, p. 3). Thus, for the refugees interviewed, the smartphone becomes a universal tool that opens up new scope for decision-making and action, despite continuing dependencies and additional necessities, such as the supply of electricity and internet. The potential of smartphones as universal devices in exceptional situations emerges here with clarity. However, this micro sociological analysis based on enabling practices for a greater individual agency in the context of flight provided by the smartphone bumps up against an institutional surveillance apparatus and new possibilities in surveillance technology that, via smartphone data extraction, contributes heavily to criminalizing a necessity of a particular group of smartphone users and increasing existing inequalities.

4. Surveillance of smartphones A European trend with legal basis

It can be argued that, especially in the course of the so-called refugee crisis of 2015, refugees and asylum seekers have been increasingly seen as a threat to national security. In the following years, many European countries tightened entry regulations and restructured the rules for the asylum procedure. One focus in many European countries was the introduction of surveillance and the extraction of personal data of asylum seekers. In doing so, the law on Better Enforcement of the Obligation to Leave the Country (from 20th July 2017), for example, enabled the central German migration authority, the Federal Office for Migration and Refugees (BAMF), to access and analyse data from electronic devices in order to determine their owner's origin and identity. The legal regulations do not restrict the measure to smartphones, but allow for the evaluation of a large number of other devices, such as simpler models of mobile phone (referred to as feature phones), USB sticks, hard disks, laptops and even fitness wristbands. The decision whether or not to access digital devices is made by the migration authorities, as this quote explains: «if, for example, a person cannot produce a valid passport or if the passport is not recognized as valid by the Federal Republic of Germany, i.e., it doesn't have to be that the person doesn't have a passport at all, it can simply be that they come from a country where passports are not forgery-proof or because there are major corruption problems and it is more or less assumed that people can also obtain passports in other ways, etc.». Accordingly, in Germany, the procedure is part of the asylum application process carried out during the registration of the person and thus «in the process where fingerprints are taken, where a picture is taken of the person, where he/she has to provide his/her data, i.e., the reading of the device takes place before the asylum hearing, which would be a further step and is carried out independently of the results of the hearing».

Similarly, the authorities in Denmark amended a law in 2017 to access digital devices if the data might be of significance for the asylum process: «The law in Denmark has a privation that allows authorities to take documents into possession to establish the identity of a person coming to Denmark if there is doubt about that person´s identity and "documents" have sort of been extended, for legal practice and data codifying to law, to mean smartphones, including all the data that can possibly be extracted from smartphones through the use of programs, extraction programs». The legal basis is Section 40 (9) of the Aliens Act from 2017, which allows the police to take documents and objects into custody: «Danish authorities have for years been asking asylum seekers arriving without valid passports to hand their mobile phones over, with the code. They will open it and scan the information, especially looking for info about ID, home country, language, family members and travel route. The asylum seeker has to agree to this as part of collaboration on the case. If not, it can be done by force and the person will normally be detained. This has been a common practice for some time, but not always used. In a new law proposal which is being processed, it becomes part of official law and will be done consequently».

New legislation or extensions of existing Laws have been proposed in other European countries, including the UK, Austria, Norway and Belgium. Following Biselli and Beckmann (2020), Norway was one of the first countries to extract and to evaluate refugee data during asylum registration. In Belgium, an amendment to the law in 2017 allows asylum authorities to access a refugee's digital devices. There is no restriction on the types of digital media covered; even private email exchanges can be evaluated. In Austria, the Aliens Act Amendment Act of 2018 authorizes the security authorities to analyse mobile phones and other data carriers of asylum seekers if there are doubts about the identity of the persons concerned, their country of origin or the declared flight route. In the UK, the Police Act of 2013 gave not only police officers but also immigration officers the right to interfere with mobile phones and other technical devices belonging to asylum seekers. Additionally, the Data Protection Act of 2018 contains far-reaching exceptions to data protection. In most countries, however, legalization only took place as a second step; as a practice, the monitoring of smartphones was carried out before formal legalization, for example, in Denmark, Norway and the UK. Interviews with Danish activists highlighted this issue: "Police have copied data from asylum seekers' mobile phones, SIM cards and other electronic devices in hundreds of cases. A practice that dates back to February last year (2015)". In their newspaper article, Koch Straede and Gjerding (2016) point out that this occurred in the case of 377 asylum seekers during their asylum application.

5. Technology firms and technical innovations of surveillance: DATA reading

The importance of different digital devices, particularly the smartphone, in a refugee's life has not gone unnoticed by technology firms themselves, who are eager to develop ever newer and more effective software in order to access smartphone data. As the analysis of our data shows, in recent years, governments of European member states have increasingly purchased such software to read data from the smartphones of asylum seekers during the asylum procedure. Norway uses OSINT whereas Germany and Denmark make use of the software Cellebrite; both are programs that allow fast data extraction from smartphones. Cellebrite is an Israel-based firm, producing forensic tools which empower authorities to bypass passwords on digital devices, allowing them to download, analyse and visualize data. On the firm's Internet homepage, the Cellebrite software is described as «the global leader in digital intelligence that is marketing its digital extraction devices increasingly to governments». As an employee of the company underlined, the legitimation of this practice is a security issue, the software a tool to know the "truth" of what a person has done, is doing and is going to do: «77% of refugees arrive without document, while 43% have a smartphone during their journey. Most of them do not have any documents. A person's phone allows you to have access, to know who they are, what they have been doing, where they have been, when, and ultimately why they are seeking asylum». More practically, an activist in Germany pointed out that the Cellebrite software is

able to extract «information about which country codes, that tells you with whom the person communicates with. They get a list that shows how many text messages to Moroccan codes the person has sent, how many text messages from certain codes the person receives, how many calls, which domains they call up. Then location data are analysed...there are certainly photos with GPS data, they get a map where a person is supposed to have stayed in Morocco, etc».

Between the personal level, which focuses on the necessity of the smartphone as a survival tool in the context of flight, and the macro level, which turns technological possibilities into an instrument of political power, a new space opens up for sociological questions related to the awareness that digital data are socially and culturally constructed. In doing so, they have a social as well as a cultural life; a vitality of their own. They are not neutral products, but represent deliberate decisions by those who collect and use these data for political purposes. Linked to this, questions related to power relations and new digital vulnerabilities arise.

6. A question of privacy and data protection

Following international human rights law, surveillance is an interference with the right to privacy and therefore needs to abide by numerous principles. For example, any surveillance needs to be *necessary* and *proportionate* to the overall aim and not be discriminatory, based on characteristics such as race or birth origin. This means that national laws requiring invasive surveillance measures can still be a violation of international law if they do not meet these standards. An interviewee stressed the newly created vulnerability of refugees and asylum seekers: «Data protection law applies to all people, including refugees. The mobile phone data analyses are simply not compatible with this. But there are only a few in the field of migration. The political discourse in Germany on this topic is relatively weak simply because, I think, asylum seekers are classically a group that doesn't have a particularly strong lobby». The interviewees emphasized that the reading of the most intimate and personal information from a person's smartphone can be seen as an ulterior step in the criminalization of refugees and asylum seekers. Accordingly, by analysing the data of the smartphone, the refugee is assumed a priori not to be telling the truth, to be hiding something and to be potentially dangerous for the country in which he/she wants to apply for asylum: «The applicant is also not guilty of anything at first: e simply has no papers. The planned search puts refugees under general suspicion of lying about their identity».

As our analysis show, the primary goal is to verify information on identity and origin and, thus, to check the plausibility of the information on the person's origin and identity. However, as interviewees in different European countries stated, governments are not only interested in information related to identity, but are eager to extract as much information as possible on a person if they doubt what they are saying: «There is definitely reason to, besides establishing identity of the person, to extract or use information extracted for the asylum case in general. If there is a suspicion that the person has not given correct information about where he/she is coming from, information on the phone could be used to contradict what the person is saying». Interviewees drew the picture of a reception system that has changed from the idea of protecting people on the flight to a system of a control based on the idea that refugees are «taking advantage of the system to get to Europe, that's a prevailing thought». The migration legislation and restricted policies have created the definition of forced migrants as illegal migrants, «and it is precisely the creation of this labelling that leads forced migrants to be 'produced' as if they were illegal migrants and therefore false refugees». The idea that refugees should be treated with suspicion and that the truth of their statements must be checked and controlled in order to avert a potential threat to security creates legitimacy for surveillance mechanisms: «I have never seen Danish authorities express any doubt about this. It could be that they are, especially in the current political climate in Denmark, that they are mostly interested in information that can be used to reject the asylum application». Linked to this, the aim is to gather as much as information on a person in order to reach the truth. There is trust and hope in technology to find out the truth about someone, to

control and prevent the social order. As one interviewee outlined, «I think there is this very significant potential and temptation, perhaps that now that we have all this new sort of sources of information and sort of crowd-generated and person-generated, new information from all over the world, there is obviously this hope and temptation that maybe, you know, now we can actually figure out what happened in x or y place». Similar another interviewee stated: «there was a certain hope associated with all this technology to make the procedures less complicated, so to speak, or to get more objective clues as to where a person is from».

In particular, interviewees in Germany and Denmark raised critical questions about privacy and data protection. Thus, the practices of smartphone surveillance violate the general right of personality, which is a fundamental right. This also includes the right to guarantee confidentiality in information technology devices, as the Federal Constitutional Court established in 2008. One interviewee explained that in Germany, the invasion of privacy usually takes place without concrete suspicion «that they may have given false information about their identity and origin. For example, if they cannot produce a recognized passport when they register, they are eligible for a readout of their device…The intrusion into the privacy of the refugees is deep».

Following this line of argument, interviewees also referred to the linkage between the smartphone surveillance practices and the demonstration of sovereignty and power by the authorities and institutions. One interviewee, referring to Germany, stated: «In fact, in the background it was a lot about showing the ability to act, to present oneself as a modern authority and to demonstrate that one can get a grip on these problems, with the bad asylum decisions that have been left behind, for example». That the monitoring of smartphones is more a demonstration of power than a benefit has been proven by several activists and lawyers in different European countries: «No, it is actually not particularly useful, that is also what we criticize about it, because on the one hand you have a relatively blatant intrusion into the privacy of the refugees when you read out the devices and, on the other hand, this whole procedure is not particularly useful. In the first half of 2020, there were no usable results in 68% of cases. In 30% of cases, the information from the data medium analysis confirmed the information provided by the protection seekers and in 2% of cases, the identity could be disproved. In absolute figures, this concerned nine applicants out of 656 evaluations». According to the information on asylum statistics for 2018 in Germany, 64% of the readouts in 2018 yielded no usable results, 34% confirmed origin and identity claims of the applicants and only 2% contradicted the origin and identity claims of the applicant (see Biselli, Beckmann, 2019).

The interviewee stated that asylum seekers in Germany «must sign that they agree to the whole thing, but in our practical work with asylum seekers we see that people don't know exactly what is happening and just know OK, my mobile phone is now being read, I am more or less obliged to give it out otherwise I could get problems with my asylum application». This was confirmed by the testimony of two asylum seekers who travelled from Italy to Germany: «All of a sudden the policeman told me to hand over my mobile phone and unlock it. I didn't know at all what exactly was happening, nothing was explained to me». Another asylum seeker from Ghana reported similarly: «I was afraid of being deported. So, I gave him the mobile phone. It was like handing over my whole life». Thus, the entity requesting consent is in a position of power over the individual. The asylum seeker is not in a position to disagree: «if a person fears being denied asylum and deported if they don't hand over their phone, it does not constitute consent. It can hardly be said that consent is fully informed or unequivocal if the person concerned is unlikely to have full knowledge of the scope or types of information that may be extracted and retained». Similarly in Denmark, the Danish Institute for Human Rights has stated concerns about the right to personal freedom on this issue. One interviewee outlined: «often the asylum seekers will not get the phone back until weeks or even months, which is a huge problem, as this is usually their only contact to relatives and friends. Not hearing from them will cause a lot of anxiety and sometimes even make it hard to find each other again». According to the German case, a human rights activist in Denmark critically reflected upon the practice: «It is not really a voluntary consent because if the refugee does not give consent, the police can take the phone into custody, there are...a legal basis in the Administration of Justice Act that allows the police to sort

of confiscate an object that can be used not only in criminal proceedings but also to establish the identity of persons coming to Denmark, so either way, if the police want to access the information on the phone they can take it to custody, either voluntarily with consent or by just taking it».

As our analysis show, asylum seekers themselves, as well as jurists and activists, take agency against this practice. Interviewees provided insight into the methods and strategies with which refugees nevertheless attempt to circumvent this intrusion into their private sphere and, as Goffman (1961) would describe it, to develop strategies of agency despite coercive contexts. The adoptive form of agency is based on a personal and individual level which is not aimed at changing the structural environment, but to create enabling strategies in order to circumvent this massive encroachment on one's own private sphere without having the position and possibilities to give or withhold their inform consent. Interviewees mentioned that «information seems to be flowing between refugees and in certain Facebook groups that they are sort of warned beforehand that this is going to happen and maybe some would wipe their phone before they turn it over to the authorities«. An expert from Denmark outlined: «if...they are not required to unlock the phone so if they have an up-to-date phone with encryption, the latest security update, it could be the case that Cellebrite and XIY are not able to extract any meaningful information from the phone. In that case, the authorities would not gain access to this». Such manoeuvres were also found—albeit rarely—in the interviews with refugees and asylum seekers who have heard of this practice or have already experienced it: «In Germany, they took my mobile phone. Now I know. I have nothing to hide, I don't have to give them my mobile phone«. An activist in Germany outlined: «I think that if people don't want to give away their phone, or somehow know that they might have problems with it, then of course they have the possibility to circumvent this system by bringing a manipulated device or by not bringing a device at all, i.e., they can simply say they don't have a device. That is difficult to check and easier too...yes, in the end, no problem to say it».

Conclusions

This article has specifically highlighted the role of smartphones in describing the ambivalent potential within digital devices: despite being a fundamental necessity for refugees, phones are turned into a threat, as the traces they leave behind make refugees vulnerable to surveillance by those they are trying to escape. In doing so, in accordance with other research (Donà, 2015; Kaufmann, 2018, Diminescu, 2018) , the article has shown that smartphones and ICT in general demonstrate creative resources allowing refugees new ways to mobilize and to act in a transnational way and across borders. The study adds to the existing literature in showing how this is also true for precarious migrants with low economic and cultural capital, and/or with vulnerable migration status who often find them in situations of forced immobility and border contexts (Leurs, Smets, 2018). The results give insights into how, even in vulnerable situations, refugees are capable of making innovative uses of ICT and digital devices in order to circumvent restrictive migration regimes.

Nevertheless, the results also show that the same digital tools that enable refugees' agency are used against them more and more often by European governments in order to transform unknown individuals into controlled individuals. The article adds to the existing literature in giving insights into how asylum in the EU has moved away of being a process that provides protection for the individual, putting state security centre stage (Loh, 2016). This has been accelerated in particular since the years after the so-called refugee crisis, where anti-refugee populism in Europe increased, alongside restrictive national migration policies that have shaped the reception of refugees and asylum seekers. Linked to this, the results show how the digital space demonstrates itself as a highly hierarchized space, constructed along the intersection of different discrimination axes (ethnicity, legal status, etc.) and within specific social, political and economic contexts (Georgiou, 2018). Linking the individual level (the need of refugees to use smartphones for communication, information and orientation) to the political level is an emerging international market of surveillance and security

technologies that has developed in recent years. Technology firms have contributed to develop and to promote the digital turn in surveillance and security-focused practices based not exclusively on the physical body, but on the digital devices as 'extended bodies'. As such, technological innovations have become an integral part of the migration control dispositive, as Ceyhan (2008) points out, that builds on, observes and collects information on individuals' behaviour. The interior of refugee's lives is exposed to invisible overseers. Zuboff (2019) terms this process 'surveillance capitalism', a force that is as profoundly undemocratic as it is exploitative. The findings that have been reported point to at least three possible further research fields and specific questions/ implications that would lead to a deeper understanding of the empowerment-control nexus in the context of refugees, as a valuable lens to better understand the impact of digitalization processes on migration issues. First, results show that studies focusing on individual or ethnographic (Kaufmann, 2018, Twigt, 2018) work should be linked to and embedded in a global political-, technological- and market-oriented context and, thus, new power relations that make use of individual necessities in order to use them against them. Drawing on Lupton (2013), sociologists' critical and reflexive perspectives on social life are more important than ever in this context and can contribute to better understand the interrelations not only on a micro but also on a macro scale. Second, a research focus on refugees' awareness of digital surveillance and security practices could broaden the knowledge of the impact that a higher awareness could have on refugees' digital behaviour. Finally, asylum seekers and refugees are deprived of control not only over their biometric data, but also over their electronic data. Consequently, they lose control and autonomy over their digital agency and the freedom or possibility to decide who has access to it and who does not. As Dragana (2020) points out, 'protecting the right to privacy informed consent is key to building trust with this vulnerable group and to fostering greater digital agency'. Further research could therefore put digital agency centre stage and attempt to direct efforts on a European level to rebuild digital agency among refugees as a particular vulnerable group within the surveillance society (Lyon and Bauman, 2013).

References

Ball, K., Webster, P. (eds.) (2004). *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*. London: Pluto Press

Beer, D., Burrows, R. (2013). Popular Culture, Digital Archives and the New Social Life of Data, *Theory, Culture & Society,* volume 30- number 4. pp. 47-71. DOI.org/10.1177/0263276413476542

Beer, D., (2013). Public Geography and the Politics of Circulation, *Dialogues in Human Geography,* volume 3 - number 1. Pp: 92-95. DOI.org/10.1177/2043820613486427

Biselli, A., Beckmann, L. (2019). Das Smartphone, bitte! Digitalisierung von Migrationskontrolle in Deutschland und Europa". freiheitsrechte.org/home/wp-content/uploads/2019/12/GFF-Studie_Digitalisierung-von Migrationskontrolle.pdf.

Bowen, G. (2009). Document Analysis as a Qualitative Research Method, *Qualitative Research Journal*, volume 9- number 2. pp. 27-40. DOI:10.3316/QRJ0902027.

Broeders, D. (2009). "Tracing, identifying and sorting: The role of EU migration databases in the internal control on irregular, migrants". In H. Fassmann, M. Haller D. Lane (eds). *Migration in Europe: Threat or Chance*. Cheltenham: Edward Elgar.

Candidatu, L., Leurs, K., Ponzanesi, S. (2018). "Digital diasporas: Beyond the buzzword. Towards a relational understanding of mobility and connectivity". In R. Tsagarousianou J. Retis (Eds.). *The handbook of diasporas, media, and culture.* New Jersey: Wiley-Blackwell.

Ceyhan, A. (2008). Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics, *Surveillance & Society*, volume 5- number 2. pp. 102-123. doi.org/10.24908/ss.v5i2.3430.

Clarke, A.E. (2003). Situational Analyses: Grounded Theory Mapping after the Postmodern Turn, *Symbolic Interaction, volume 26*- number 4, pp. 553- 576. doi.org/10.1525/si.2003.26.4.553 .

Corbin, J.M., Strauss, A.L. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Thousand Oaks, California: Sage Publications, Inc.

Diminescu, D. (2008). The connected migrant: An epistemological manifesto, *Social Science Information,* volume 47- number 4. pp. 565–579. doi.org/10.1177/0539018408096447.

Doná, G. (2015). Making Homes in Limbo: Embodied Virtual "Homes" in Prolongued Conditions of Displacement, Refuge, volume 31, number 1. pp. 67-73. doi.org/10.25071/1920-7336.40298,

Dragana, K. (2019). Data Protection and Digital Agency for Refugees. www.cigionline.org/publications/data-protection-and-digital-agency-refugees.

Georgiou, M. (2018). Does the subaltern speak? Migrant voices in digital Europe, *Popular Communication*, volume, 16- number 1. pp. 45-57. DOI:10.1080/15405702.2017.1412440.

Gillepsie, M., Ampofo, L., Cheesman, M., Faith,B., Iliadou, E., Issa, A., Osseiran,S. Skleparis, D. (2016). *Mapping Refugee Media Journeys: Smartphones and Social Media Networks.* www.researchgate.net/publication/310416833_Mapping_Refugee_Media_Journeys_Smartphones_and_Social_Media_Networks.

Goffman, E. (1961). *Asylums: essays on the social situation of mental patients and other inmates. New York: Doubleday & Company.*

Hine, C. (2015). *Ethnography for the internet: embedded, embodied and everyday*. London: Bloomsbury.

Horst, H.A., Taylor, E.B. (2014). The role of mobile phones in the mediation of border crossings: A study of Haiti and the Dominican republic, *The Australian Journal of Anthropology,volume* 25, number 2, pp. 155–170. doi.org/10.1111/taja.12086.

Huysmans, J. (2006). The Politics of Insecurity: Fear, Migration and Asylum in the EU. London: Routledge.

Karamanidou, L., Kasparek, B. (2018). *Border Management and Migration Control in the EU*,

Kaufmann, K. (2018). Navigating a new life: Syrian refugees and their smartphones in Vienna, Information. Communication & Society, volume, 21, number 6. pp. 882–898. doi.org/10.1080/1369118X.2018.1437205.

Latonero, M., Kift, P. (2018). On Digital Passages and Borders. Refugees and the New Infrastructure for Movement and Control, *Social Media & Society, volume* 3, number 1, pp. 1–11. doi.org/10.1177/2056305118764432.

Leung, L. (2011). *Mind the Gap: Refugees and Communications Technology Literacy*. Sydney: Australian Communications Consumer Action Network.

Leurs, K., Prabhakar, M. (2018). "Doing Digital Migration Studies: Methodological Considerations for an Emerging Research Focus". In: Zapata-Barrero R., Yalaz E. (eds). *Qualitative Research in European Migration Studies. IMISCOE Research Series*. Cham: Springer. doi.org/10.1007/978-3-319-76861-8_14.

Leurs, K., Smets, K. (2018). Five questions for digital migration studies: Learning from digital connectivity and forced migration in(to) Europe, *Social Media and Society, volume 3*, number 1. pp.: 1-16. doi.org/10.1177/2056305118764425.

Loh, T.Y. (2016). Digitizing Refugees: The Effect of Technology on Forced Displacement. *Gnovis*, volume 16 number 2. pp. 49-57.

Lupton, D. (2012). Digital Sociology: An Introduction'. Sydney: University of Sydney. hdl.handle.net/2123/862.

Lupton, D. (2013). Digital sociology: beyond the digital to the sociological. In Osbaldiston, N., Strong, C. and Forbes-Mewett, H. (eds). Melbourne: TASA. *The Australian Sociological Association 2013 Conference Proceedings: Reflections, Intersections and Aspirations, 50 Years of Australian Sociology*. www.tasa.org.au/tasa-members/2013-conference-papers/

Lyon, D., Bauman Z. (2013). *Liquid Surveillance*. London: Polity Press.

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*, Oxford: Open University Press.

Lyon, D. (2004). "Surveillance Technology and Surveillance Society". In T. Misa, P. Brey, A. Feenberg. *Modernity and Technology*. Cambridge, MA: MIT Press, pp. 161–84.

Madianou, M., Miller, D. (2012). *Migration and new media: Transnational families and polymedia.* London: Routledge.

Nedelcu, M.,, Soysüren, I. (2020). Precarious migrants, migration regimes and digital technologies: the empowerment-control nexus, *Journal of Ethnic and Migration Studies*. doi.org/10.1080/1369183X.2020.1796263.

Orton-Johnson, K., Prior, N. (2013). *Digital Sociology. Critical Perspectives*. Basingstoke, Hampshire: Pallgrave McMillan.

Twigt, M. (2018). The mediation of hope: Digital technologies and affective affordances within Iraqi refugee households in Jordan, Social Media and Society, volume 4, number 1. pp. 1-14. doi.org/10.1177/2056305118764426.

Wall, M., Campbell, M.O., Janbek, D. (2015). Syrian refugees and information precarity. *New Media & Society,* volume, 19, number 2. Pp.: 240–254. doi.org/10.1177/1461444815591967. Working Paper 2018/14, Global Migration Consequences and Responses, prepared within the Horizon 2020 project RESPOND – Multilevel Governance of Migration and Beyond. www.respondmigration.com/wp-blog/2018/8/1/comparative-report-legal-andpolicyframework-of-migration-governance-pclyw.

Zuboff, S. (2019). *The age of* surveillance capitalism: the fight for the future at the new frontier of power. London: Faber and Faber.