EJPLT

Migrants and refugees in the cyberspace environment: privacy concerns in the European approach

MIRKO FORTI
Researcher Fellow at Sant'Anna School of Advanced Studies of Pisa

European Journal of Privacy Law & Technologies • 2020/2 • ISSN 2704-8012

Abstract

Migrants and refugees use their smartphones during their migration journey in several ways. They rely on the Internet, and more specifically social media platforms, to maintain a bond with families and friends back in the State of origin, to get information about their planned routes, to keep contacts with smugglers and traffickers and as a tool of integration in the national community of intended destination. Although smartphones are useful instruments for their migration plans, these devices could also become a gateway to digital surveillance. This article aims to focus on the relationship between smartphones and migrants and its legal consequences, especially about privacy and data protection concerns. More specifically, the study would like to individuate how the utilization of digital devices in the context of mass migration phenomena could expose migrants and refugees to several threats coming from the cyberspace dimension. Thus, it is fundamental to verify which kind of legal safeguards the European regulatory framework could provide to protect the right to privacy and data protection of these subjects.

Keywords: Migrants - Refugees - Social Media - Smartphones - Privacy - Surveillance.

Summary: Introduction. – 1. Smartphones and social media in the migration context: positive factors and possible vulnerabilities for migrants and refugees. – 2. The GDPR in the context of mass migrations: profiles of (non) regulatory compliance. – 2.1. The definition of "personal data" and the metadata problem. – 2.2. Data protection principles and digital surveillance methods for migrants and refugees: the need for a legal assessment. – 2.3. Information and access to personal data and the cultural gap regarding the concept of privacy. – 2.4. Legal basis for data processing activities in the management of mass migrations phenomena. – 3. Concluding remarks.

Introduction.

Nowadays, a smartphone is an essential part of the toolkit of every migrant ahead of the planned journey, likewise water and food[1]. ICT technologies are increasingly becoming a fundamental factor in the mass migration phenomena for several reasons. Smartphones are the ideal gatekeepers to a potentially indefinite amount of information useful to plan and enable a migration journey.

Although their undoubtful utility, electronic devices could rapidly become a tool for digital surveillance in the hands of border control authorities and also migrant smugglers. Smartphones contain personal data regarding their owners and their online activities, such as web searches, social media accounts and location data. In the migration context, surveillance methods could exploit this information to keep under control migrants, in spite of their fundamental right to privacy and personal identity.

Accordingly, the main focus of this article is to evaluate the profiles of compliance

[1] I Kaplan, 'How smartphones and social media have revolutionized refugee migration', UNHCR Blogs, https://www.unhcr.org/blogs/smartphones-revolutionized-refugee-migration/ (last seen on 27 April 2020).

between the use of smartphones and social media by migrants and refugees and the European regulatory data protection framework in order to formulate a consistent policy and legal approach to safeguard the fundamental rights of the individuals involved. The first step is to understand the real importance of ICTs in the mass migration context, focusing on the positive sides and the downfalls of using an electronic device before and during the journey.

1. Smartphones and social media in the migration context: positive factors and possible vulnerabilities for migrants and refugees.

Migrants and refugees rely on an extended digital infrastructure to plan their journey and to reach their final destination safely. Smartphones can act as an aggregator of several kinds of information and as an enabler of communication channels. Accordingly, migrants are currently using electronic devices for distinct functions which are hereby worth mentioning[2].

Firstly, the Internet can be a valuable tool for navigation and geolocation purposes. Migrants use their smartphones to be continuously updated about their journey and to receive information like the most efficient route, weather and climate conditions, border controls[3]. In the same way, Global Positioning System technology (GPS) is often used by smugglers and migrants themselves to navigate in the Mediterranean waters[4].

The deployment of these digital resources is gradually mutating the ongoing relationships in the migration context; individuals prefer to rely on these technologies and the help of fellow migrants, instead of smugglers, to find the way to the next destination while on the route[5].

Secondly, ICT technologies enable the first contact between people who are planning to move away and traffickers. Several social media groups are the digital place where smugglers can advertise[6] their services to potential customers who can compare different journey packages and prices[7]. Additionally, these virtual platforms include "reviews" of previous clients who are sharing their knowledge and experience with potentially future migrants.

The continuous flow of information regarding migration journeys and services offered by smugglers available on social networks reveals both positive aspects and possible downfalls[8]. Migrants and refugees can choose from a variety of routes and means of transport advertised on social media groups, therefore, they are able to make more secure choices. However, they often count on unreliable information considering how smugglers and traffickers are led to underestimate every risk factor regarding their journeys. Furthermore, criminals often use social networks like Facebook to sell fake passports and ID cards in order to allow migrants

---

[2] M Gillespie and others, 'Mapping refugee media journey. Smartphones and social media networks', *https://www.open.ac.uk/ccig/sites/www.open.ac.uk.ccig/files/Mapping%20Refugee%20Media%20Journeys%2016%20May%20FIN%20MG_0.pdf* (last seen on 27 April 2020).

[3] B Frows and others, 'Getting to Europe the "Whatsapp" way. The use of ICT in contemporary migration flows to Europe', (2016), 2, RRMS Briefing Paper, http://www.mixedmigration.org/wp-content/uploads/2018/05/015_getting-to-europe.pdf (last seen on 27 April 2020).

[4] J Schapedonk, D Van Moppes, 'Migration and information: images of Europe, migration encouraging factors and en route information sharing', (2007), 16, Working Paper Migration and Development Series, 1,29.

[5] R Khalaf, 'Technology comes to rescue in the migrant crisis', Financial Times, 24 February 2016, https://www.ft.com/content/a731a50a-da29-11e5-a72f-1e7744c66818#ixzz41ks4s7ZX (last seen on 28 April 2020).

[6] Reuters, 'Migrants smugglers use Facebook to promote Turkey-Italy trips bypassing sealed Balkan route', 2 April 2016, https://www.rt.com/news/338087-migrant-smugglers-italy-facebook/ (last seen on 28 April 2020).

[7] B Frows and others, 'Getting to Europe', (n.3).

[8] E Diker, 'Social media and migration', Political and Social Research Institute of Europe Blog, http://ps-europe.org/social-media-and-migration/ (last seen on 28 April 2020).

to pass border controls.

One of the several challenges faced by migrants and refugees during their trip is to understand foreign languages and to communicate with people[9]. Electronic devices can provide valuable help in this regard through websites and translating apps.

Smartphones could also act as a tool of digital witnessing of the migration journey under a double aspect[10]. Firstly, they contribute to strengthening a bond between migrants *en route* and their family and friends back in the country of origin through the sharing of multimedia contents like video, photos of every stage of the journey thus to create a sense of connection in spite of the distance. Additionally, migrants could use smartphones to record every abuse and stressful situation which they have to face during their travelling, such as human right violations[11].

In conclusion, the multimedia capabilities of smartphones and social networks are useful for migrants and refugees in many ways; as an aggregator of information, a tool to keep in contact with family, an instrument to facilitate their journey and to foster their integration in the country of destination. However, ICT's technologies could reveal vulnerable aspects regarding the fundamental rights and personal identity for the same subjects. Smartphones could rapidly become an instrument of digital surveillance according to the potentially indefinite amount of personal data contained in such electronic devices. The growing ability to track movements of persons in real-time through their digital tracks raises new profiles of threats and vulnerabilities for migrants and refugees, more specifically for their fundamental right to privacy and data protection.

Several States in the European Union are currently exploiting this possibility for security purposes or, at least, they are evaluating this kind of policy approach. Belgium recently approved specific normative provisions[12] to allow border authorities and patrols to check asylum seekers' digital devices. This approach is possible according to an extensive interpretation of the terms of the art.13.2 (d) of the Directive 2013/32/EU[13]: the norm states that "*competent authorities may*

search the applicant and the items which he or she is carrying". Likewise, the possibility to check digital profiles of migrants and refugees at border controls is at the centre of political debate in other European countries like Germany[14].

There are two different motivations behind this policy approach regarding the ways of patrolling national borders[15]. On a first basis, checking social media accounts and electronic devices could be an alternative manner to control personal identity when ID documents or passports are not available. National authorities could verify if migrants and asylum seekers

---

[9] M Gillespie and others, 'Mapping refugee', (n.2)

[10]M Gillespie and others, ibid.

[11] E Isin, E Ruppert, *Being digital citizens* (1st edition, Rowman & Littlefield Publishers, 2015) 140.

[12] Loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers et la loi du 12 janvier 2007 sur l'accueil des demandeurs d'asile et de certaines autres catégories d'étrangers, 21 November 2017, http://www.ejustice.just.fgov.be/eli/loi/2017/11/21/2017032079/justel (last seen on 28 April 2020).

[13] Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection, [2013] OJ L 180/60.

[14] P Oltermann, J Hentley, 'German proposals could see refugees'phones searched by police', The Guardian, 11 August 2016, https://www.theguardian.com/world/2016/aug/11/germany-security-proposals-refugees-phones-searched-suspicious-posts-social-media (last seen on 28 April 2020).

[15] M G Jumbert and others, 'Smartphones for refugees: tools for survival or surveillance?', (2018) 4, Prio Policy Brief, 1, https://reliefweb.int/sites/reliefweb.int/files/resources/Jumbert%2C%20Bellanova%2C%20Gellert%20-%20Smart%20Phones%20for%20Refugees%20Tools%20for%20Survival%2C%20or%20Surveillance%2C%20PRIO%20Policy%20Brief%204-2018.pdf (last seen on 28 April 2020).

have all the characteristics to ask for international protection, searching for clues and evidences on social media profiles and smartphones or laptops. Lastly, border guards look for potential threats for national security in the context of counter-terrorism actions.

Furthermore, smugglers and traffickers check social media accounts of migrants and refugees, even after the end of the journey, to not lose control over them and to maintain these subjects under the influence of criminal organizations.

In conclusion, relying on ICTs in the context of mass migrations presents a double side effect. On the one hand, it allows migrants and refugee to take more meaningful decisions during their journey and facilitate their integration in the country of destination; on the other hand, raises privacy and data protection concerns which are worth mentioning and expose worrying profiles of vulnerability regarding the sphere of fundamental rights of the people involved.

Thus, it is necessary to individuate which are the feasible normative solutions within the application sphere of the European data protection regulatory framework, especially the Regulation (EU) 2016/679[16] (hereinafter also GDPR), to safeguard the right to privacy and personal identity of every individual in the context of mass migrations.

2. The GDPR in the context of mass migrations: profiles of (non) regulatory compliance.

The Regulation (EU) 2016/679 is the core of the European regulatory framework regarding the right to privacy and data protection. Its features take into account the technological progress, which is continuously raising new challenges for privacy in the digital ages. The actions of the European Union and all the Member States in the management of mass migrations have to respect the normative provisions of the GDPR, although there should be a few problems of regulatory compliance which are worth of mentioning.

2.1. The definition of "personal data" and the metadata problem.

The concept of "personal data" is not an immutable and abstract idea, while it rapidly changes during the time to respond to the needs of an evolving society. The advent of the Internet and, therefore, the global diffusion of a communication network has radically revolutionized the traditional paradigm of privacy, introducing new digital elements capable to identify univocally a single person.

Thus, the GDPR states a broad definition of personal data, readily adaptable to the innovations of digital progress: according to art 4.1 of the Regulation, "personal data" means any information relating to an identified or identifiable natural person called data subject.

Focusing on digital surveillance methods regarding migrants and refugees, the GDPR does not declare anything regarding the so-called metadata[17]. This term indicates the "data about data", namely data reporting information about one or more aspects of data, allowing faster and easier processing of data itself. Metadata, if considered singularly, are inherently anonymous, so they are not able to indicate univocally a single individual. They need to be combined together to point out the above data subject. Thus, the GDPR applies only to aggregated metadata, although illegitimate processing of such information could seriously

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1.

[17] R Guenther, J Radebaugh, 'Understanding metadata', National Information Standard Organization (NISO), 2014, https://web.archive.org/web/20141107022958/http://www.niso.org/publications/press/UnderstandingMetadata.pdf (last seen on 30 April 2020).

harm the right to privacy of everyone involved. Metadata could reveal important information about specific individuals and their online behaviour without plainly identifying any data subject; for example, indicating when and where a specific digital resource was created. If adequately processed, metadata could point out habits and intentions of migrants and refugees during their journey. National authorities could process metadata when inspecting laptops and smartphones at border checks, although GDPR may not provide sufficient safeguards for the right to privacy of people involved regarding this type of information. Proposals for reforming the ICT legal framework would probably entail metadata too. The forthcoming Regulation ePrivacy[18] would allow the processing activities of metadata only in case of previous approval of the involved data subject. The metadata issue is one of the main topics at stake in the current debate about such reform effort[19]. The scope of the GDPR is not limited to defining the concept of "personal data". Regulation 2016/679 lists a series of founding principle which every data processing activity shall follow.

2.2. Data protection principles and digital surveillance methods for migrants and refugees: the need for a legal assessment.

Principles of fairness, lawfulness and transparency must characterize every data processing activity (art.5.1a GDPR). Moreover, personal data shall be collected only for *specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes* (art.5.1b GDPR). Information shall be *adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed* (art.5.1c GDPR) and *kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed* (art.5.1e GDPR). Lastly, the controller shall be held accountable for the data processing activities conducted under his/her control (art.5.2.GDPR).

According to these normative provisions, the main question is if the digital surveillance methods, like checking social media accounts and digital devices, used by national authorities in the management of mass migrations phenomena could comply with the fundamental principles of GDPR.

European governments are increasingly focusing their attention to the ICTs environment during border controls, in order to find out every possible evidence of national security threat "hidden" in the digital activities of migrants and refugees. There is a strong convincement that the wealth of data stored in electronic devices can indicate without any possibility of doubt or mistake the "real identity" of the owner of the laptop or the smartphone[20]. However, this is not a self-evident truth for several reasons, especially concerning migrants who are fleeing away from dramatic situations like war zones[21].

For instance, Islamic State agents and Syrian guards often request Facebook passwords during checkpoint controls to verify the allegiance of the subject during the civil war[22]. Accordingly, individuals may have changed their online habits to prevent arbitrary allegations derived from any kind of intrusion in their digital private sphere. Moreover, several people

---

[18] Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM/2017/010 final - 2017/03 (COD).

[19] T Ricci, 'Regolamento ePrivacy: a che punto siamo e cosa aspettarsi con la presidenza tedesca', 30 October 2020, https://www.agendadigitale.eu/sicurezza/privacy/regolamento-eprivacy-eppur-si-muove-a-che-punto-siamo-e-cosa-aspettarsi-nel-2020/ (last seen on 13 November 2020).

[20] M G Jumbert and others, 'Smartphones for refugees' (n.15)

[21] M G Jumbert and others, ibid.

[22] M.Brunwasser, 'A 21st-century migrant's essentials: food, shelter and smartphone', The New York Times, 25 August 2015, https://www.nytimes.com/2015/08/26/world/europe/a-21st-century-migrants-checklist-water-shelter-smartphone.html?_r=1 (last seen on 30 April 2020).

may have used the same device, which, therefore, would contain mixed digital trails originated from different subjects. Not every migrant has a smartphone during the journey and it could happen to lose the electronic device or to run out of battery. In light of the above considerations, government authorities should assess data collected from migrants' digital tools very carefully, not acritically assuming their trustworthiness and taking into appropriate account the context in which data are developed. Thus, it is questionable the effectiveness of this kind of border controls and therefore their legitimacy, considering how they may not provide reliable evidence regarding the online habits of the migrant.

Furthermore, it is likewise doubtful the compliance of these digital surveillance methods with the principles of data minimisation and purposes limitation, considering how the amount of data collected may not serve to reach the scope of identifying migrants and their future actions.

Data processing activities shall enshrine the above-mentioned principles but, to be effective, they shall take into account the cultural divergencies of people involved in such procedures.

2.3. Information and access to personal data and the cultural gap regarding the concept of privacy.

One of the fundamental cornerstones of the European regulatory framework of privacy is the right to information and access to personal data (Art 13-15 GDPR). More specifically, the controller shall provide the data subject with all the information related to the processing activities (purposes, the legal basis etc.) Furthermore, the data subject is entitled to know every feature regarding the ongoing processing of his/her personal information.

The rationale behind these normative provisions is to allow the data subject to maintain a sort of control over his/her own personal data; in the digital age, the concept of privacy is gradually overlapping with the idea of informative autonomy[23]. The traditional paradigm of privacy intended as "*the right to be let alone*[24]" has no more room in the cyberspace era: everyone is permanently connected to the Internet network, continuously sharing personal data thus it is no more possible to individuate a completely intimate sphere for the individual. The right to data protection is nowadays integrating the scope of application of the concept of privacy, in order to allow the data subject to have full disposal about the own information shared[25].

However, the idea of "*right to be let alone*" is not inherently abstract, but it founds its own roots in a specific western societal background. The right to privacy was a sort of corollary to the right to private property, which was the founding core of the European and American society in the first years of the last century; any intruder is not allowed to enter the home (private sphere) of an individual without his/her permission. Thus, the right to privacy found its rationale through an individualistic perspective as a tool to permit the self-fulfilment of every subject[26], although it may cause contrasts with the needs of the entire collectivity[27].

However, the idea of privacy is too elaborated and multifaceted to be reduced to a single static concept[28], not considering the several influences of different cultural backgrounds.

In light of the mass migrations context, it is therefore worth mentioning the role of

---

[23] S. Rodotà, *Tecnologie e diritti,* (1st edition, Il Mulino,1995) 19.
[24] S D Warren, L D Brandeis, 'The right to privacy'*,* (1890) 4, Harvard Law Review, 193.
[25] A.F.Westin, 'Privacy and freedom'*,* (1968) 25:1, Washington and Lee Law Review, 166.; L.Lusky, 'Invasion of privacy: a clarification of concepts', (1972) 87:2*, Political Science Quarterly,* 192.
[26] A F Westin, ibid.
[27] P.M.REGAN, *Legislating privacy:technology, social values and public policies,* (5th edition, NCUP, 1995) 212.
[28] D J Solove, *Nothing to hide: the false tradeoff between privacy and security,* (10th edition, YUP, 2011) 24.

privacy in the African society in order to bridge the cultural divide between European immigration officers and migrants coming from the African continent[29] regarding the needed information to share.

Societies not characterised by an individualistic perspective may difficultly accept the concept of privacy as elaborated through the western experience[30].

The traditional representation of African society sees the individual as a part of the entire community and not as a single unit with autonomous needs and aspirations[31]. Ubuntu philosophy thinking, typically originated in African countries, puts at the top of the social pyramid the group, which could be for instance the family, the clan or the tribe; the self-fulfilment of the subject is subordinated to the needs of the above-mentioned group of membership[32]. There is no space for a concept of privacy as intended in the western world, as an intimate sphere outside of the public collectivity.

Thus, it is understandable why the African Charter on Human and Peoples' Rights, a regional treaty on fundamental rights, does not clearly state a right to privacy[33].

However, African culture is not static, but it is in constant motion and evolution[34]. The Internet network is rapidly growing through the entire continent, and African cyberspace users are currently experiencing the same challenges to their right to data protection of European and American citizens. Moreover, socio-economic factors like the growing urbanization, which is characterizing the African continent nowadays, is radically transforming the traditional paradigm of societal aggregation based on the basic unit of the social group for a more individualistic point of view. Farms and small factories run by families are giving way to industrialization approach inspired by the western model[35].

In conclusion, the concept of privacy is present in the African culture, although with peculiar features compared to the Western way of thinking. The focus is not only on the individual but on the subject in relationship with the entire collectivity.

Thus, immigration officers should consider these peculiarities in approaching migrants just arrived in Europe from Africa, knowing which kind of data are these people willing to share with European national authorities. Moreover, several interviews on the field report how migrants are often confused regarding sharing personal information about themselves without knowing the reasons behind these data processing activities[36]. Migrants should overcome language and cultural barriers, to not mention the shock of a long and perilous journey, to fully understand the bureaucratic practices behind the migration management activities and, more specifically, identification process.

In light of the above-mentioned considerations, it is highly questionable if migrants can really enjoy a proper right to access and information as stated by the GDPR.

Moreover, they are pushed to share their personal data also for humanitarian purposes:

---

[29] M Latonero and others, 'Digital identity in the migration and refugee context. Italy case study', https://datasociety.net/library/digital-identity-in-the-migration-refugee-context/ (last seen on 2 May 2020).

[30] L A Bygrave, '*Privacy protection in a global context – A comparative overview*', (2004) 47, Scandinavian Studies in Law,139.

[31] E.J Lassiter, '*African culture and personality: bad social science, effective social activism or a call to reinvent technology?*', (2000) 3, African Studies Quarterly,1

[32] M N Kamwangamalu, 'Ubuntu in South Africa: a sociolinguistic perspective to a Pan-African concept', (1999) 2, Critical Arts: South-North Cultural and Media Studies, 24

[33] African Charter on Human and Peoples' Rights (Banjul Charter), 28 June 1981, https://www.achpr.org/legalinstruments/detail?id=49 (last seen on 3 May 2020).

[34] L.A.Bygrave, 'Privacy and data protection in an international perspective', (2010) 56, Scandinavian Studies in Law, 176.

[35] A B Makulillo, '"A person is a person through other persons" – A critical analysis of privacy and culture in Africa' (2016) 1, Beijing Law Review,192.

[36] M Latonero and others, 'Digital identity' (n.27).

NGOs and national authorities operating on the field need to identify every single subject to provide everyone with fundamental help, namely food and medical treatments. Do migrants have a real choice in deciding when and how to give their own information or not? Is consent a suitable legal basis for data processing activities in the mass migration context?

2.4. Legal basis for data processing activities in the management of mass migrations phenomena.

The GDPR sets out a list of alternative legal grounds based on which processing data activities are considered lawful (art.6). One of the options is when the data subject has given *consent to the processing of his or her personal data for one or more specific purposes*. The controller has the legal duty to demonstrate that a free, informed and specific consent has been effectively provided. Moreover, the data subject can withdraw at any moment his/her consent previously stated without incurring in any legal or technical obstacle (art.7).

Thus, national authorities shall respect these legal requirements in the context of mass migrations management, even though it could be not a simple task to guarantee these rights to migrants and refugees and, more specifically, regarding digital data and online activities trails.

Firstly, there is a language and cultural barrier to overcome to reduce the understanding gap between immigration officers and migrants. As mentioned before, the concept of privacy could have several meanings and features according to the different cultural backgrounds, therefore, people could utilize non-identical words to define this idea. There is plenty of room for misunderstanding, although the GDPR affirms the principle of transparency as a fundamental one. Migrants cannot provide valuable consent if they do not understand the administrative procedures of collecting their personal data.

NGOs and national authorities need to identify every person before providing them with fundamental help, namely food, water, medical treatment[37]. Thus, migrants are in front of an apparent dilemma: to provide every data asked to receive help for their basic needs or to maintain a sort of control over their own personal and digital identity? The answer is obvious and self-evident.

A disproportionate relationship between immigration officers and migrants could not lead to choosing free consent of the data subject as a legal basis for data processing activities[38].

Furthermore, border guards should consider another important factor before identifying every individual: the state of shock and psychological distress mixed with the relief of being saved from the perilous journey would not allow migrants to understand which kind of data are sharing and for which purposes[39].

In light of the above considerations, it could happen that consent would not be a suitable legal basis for data processing activities on many occasions in the context of mass migrations, due to the specific vulnerabilities of the data subjects involved. Thus, the GDPR states other possible legal grounds and, for the purposes of this study, are particularly important the vital interest of the data subject or another natural person (art.6.1d) and the public interest of the collectivity (art.6.1e)[40].

It is undisputable the interest of the migrants in receiving help, even though this assistance would mean processing their personal data for identification purposes. However, this legal

---

[37] C.Kuner, M.Marelli, 'Handbook on data protection in humanitarian action', 2020, https://www.coe.int/en/web/data-protection/-/new-handbook-on-data-protection-in-humanitarian-action, (last seen on 12 November 2020).

[38] M Latonero and others, 'Digital identity' (n.27).

[39] M Latonero and others, ibid.

[40] C.Kuner, M.Marelli, 'Handbook on data protection' (n.35).

basis can legitimate only actions directed to provide help to migrants. Furthermore, data subjects should be informed about their right to object and to request the privacy policy which illustrates the modalities and goals of the data processing activities.

It is likewise unquestionable how the correct management of the mass migrations phenomena is a matter of public interest. Nevertheless, the data subjects should be made aware as soon as possible of every data processing activity regarding their identity and about their privacy rights.

Focusing more specifically on the scope of this study, it is worth questioning the legitimacy of digital surveillance procedures concerning the online trails on electronic devices and social media accounts. Although the legitimate interest of the European Union to identify every subject arrived into its territory in the context of migration flows is surely understandable, inspecting smartphones and laptop may not be compliant with the fundamental rights of people involved. Consent may not be a suitable legal basis, because it is not technically possible to previously inform migrants involved in these controls about the type of data which will be found in the electronic device (metadata, geo-localization indicators etc).

Even considering the legal obligation of every State to preserve the integrity of their own borders and the national security of their citizens, the data subject has the right to be informed as soon as possible regarding the data processing activities and the possibility to object: is this feasible in the context of similar digital controls?

3. Concluding remarks.

Although they can go unnoticed, migrants and refugees are inhabitants of the cybernetic dimension with specific needs and necessities worthy of attention. They use information and communication technologies to share experiences about their migration journeys, to acquire knowledge regarding their future destination and all the administrative and bureaucratic procedures to enter into the European Union and to maintain a bond between them and their family back in their homeland.

However, their online activities could expose their digital identities to relevant dangerous threats in terms of privacy and data protection vulnerabilities. Smugglers and human traffickers could utilize these virtual tracks to maintain a sort of illicit control over these people, even after the end of the migration journey. Furthermore, criminal organizations constantly use social networks to make the first contact with people interested in reaching the European territory in an illegal manner.

Additionally, a few European States are focusing their attention on how to exploit virtual trails left by migrants during their permanence in the cyberspace dimension to establish digital surveillance methods to protect their national borders. Border patrols could inspect electronic devices to find out possible evidence of national security threats.

\The European regulatory approach should reach a balance between the legal obligation of every State to preserve the integrity of the national borders and the safeguards to the rights of privacy and data protection of every individual, including migrants.

The fundamental basis of the European regulatory framework in this regard, the GDPR, does not explicitly state any normative provision about the collection of personal data in the management of mass migrations context[41], although the relevant peculiarities of this field.

Thus, one of the goal of this study is to point out the most relevant profiles on non-compliance between the GDPR norms and the digital control procedures regarding migrants and refugees. Firstly, it stands out how these surveillance methods may not respect the

[41] M Latonero and others, 'Digital identity' (n.27).

fundamental principles of transparency and proportionality. It is not always possible to individuate exactly which kind of data national authorities collect from the cyberspace to identify every migrant. Furthermore, it is disputable the real necessity of this kind of controls, considering how misleading could these digital data be. For instance, migrants could modify their online habits to avoid being surveilled by national authorities. Furthermore, it is not unusual that different subjects could use the same device during the migration journey, making therefore impossible to individuate which individual the data are indicating.

However, the study of the regulatory compliance of these digital surveillance methods with the GDPR is only the first step to address the fundamental issue of the right to digital identity for migrants and refugees.

Every individual holds the right to personal identity[42] and to be not discriminated in front of the Law[43], even though these words could be not applied in reality[44] due to the lack of valid proof of legal identity[45]. For instance, asylum seekers need ID cards or whether identification documents would not be able to acquire legal status in the destination country[46]. In this regard, technology could provide useful tools to identify every individual, even the ones without legal ID documents, and therefore enable them to enjoy the same opportunities of the rest of the citizens[47].

However, relying on technological means for identification purposes could expose migrants and refugees to several threats concerning possible discriminations and abuses[48]. Technology tools are neutral instruments; thus, they are not aprioristically "good" or "evil", but depending on their utilization in the hand of human beings. They can provide valuable help in reaching non-discrimination goals, but they can also be used for discriminatory practices[49] such as tailored surveillance methods.

States should use digital data collected exclusively for the aim to identify migrants and not to establish abusive surveillance controls: national authorities are legally obliged to reach a balance between the State's and the individual's interests[50]. Accordingly, identity platforms providers should design their software in light of the regulatory framework concerning privacy and data protection and focusing on the specific context of mass migrations to adequately safeguard the right to digital identity of migrants and refugees.

In this regard, the GDPR introduces the concepts of privacy by design and privacy by default (art.25) which can act as useful guidelines in preventing digital abuses and data breaches[51]. According to these principles, providers shall implement, since the very first phases of the data processing activities, all the appropriate measures to safeguard the fundamental rights of every data subject in light of the specific peculiarities of the context.

Besides implementing the necessary technical and legal measures, the European Union,

---

42 Art.6 Universal Declaration of Human Rights; Art.16 International Covenant on Civil and Political Rights.

43 Art.1,2,7 Universal Declaration of Human Rights: Art.26 International Covenant on Civil and Political Rights.

44 S Friedman, 'Substantive equality revisited' (2016)14, International Journal of Constitutional Law, 712.

45 A Beduschi, 'Digital identity: contemporary challenges for data protection, privacy and non-discrimination rights', in,(2019)1, Big Data and Society,1.

46 A Beduschi, ibid.

47 M J Haenssgen, P Ariana, 'The place of technology in the capability approach', (2018) 46, Oxford Development Studies, 98.

48 A Beduschi, 'Digital identity: contemporary challenges'(n.43)

49 A Beduschi, ibid.

50 European Court of Human Rights, Judgement 4 December 2008, *S.and Marper v.United Kingdom,* application n.30562/04, 30566/04

51 A Rachovitsa, 'Engineering and lawyering privacy by design: understanding online privacy both as a technical and an International human rights issue', (2016) 24, International Journal of Law, Information and Technology, 374.

alongside all the member States, should move forward in the management of mass migration phenomena also under a cultural and societal perspective. Nowadays, migrants and refugees do not trust the administrative procedures of identification at the European borders: they believe that sharing their personal data, they would be under constant digital surveillance. Therefore, they try to avoid any form of control, modifying their online habits and refusing to share their information. In this way, they firstly harm themselves; they are not able to integrate into the European community suffering from the exclusion from the cyberspace context. In a few words, they are not free citizens and therefore possible victims of criminal organizations.

To conclude, a working European regulatory and policy approach should clearly understand the fundamental importance of ICTs technology for migrants and refugees, both as survival tools during the migration movement and as instruments of integration, to bridge the digital and cultural gap in terms of privacy and data protection between the European world and the African and Middle East lands.