



Article

Data Protection Impact Assessment: A Protection Tool for Migrants Using ICT Solutions

Júlia Zomignani Barboza * and Paul De Hert

Fundamental Rights Research Centre, Faculty of Law and Criminology, Vrije Universiteit Brussel, 1050 Ixelles, Belgium; Paul.De.Hert@vub.be

* Correspondence: julia.zomignani.barboza@vub.be

Abstract: Smart devices have become ubiquitous in everyday life, and it is commonplace that migrants are among the users of connected tools. With the realization that migrants rely on connectivity for multiple purposes, including to access information and services, many initiatives started working on developing ICT tools to assist migrants to integrate into their new society. Technological tools, however, come with inherent risks, many of which are linked to the processing of personal data of their users. This is especially true for migrants, who are often vulnerable due to their migration status, which is not always secure in the host country. To mitigate these risks, we argue that an expanded data protection impact assessment, analyzing not only the impacts related to data protection, but also to the specific situation of migrants, should be conducted at the outset of any technology development project to influence the development of safe and reliable ICT tools for this target population. A practical example of the application of such an assessment is provided, based on the authors' experience as legal advisors in the REBUILD project, which is one of the current initiatives in the EU aiming to develop ICT tools for migrant integration.



Citation: Zomignani Barboza, Júlia, and Paul De Hert. 2021. Data Protection Impact Assessment: A Protection Tool for Migrants Using ICT Solutions. *Social Sciences* 10: 466. <https://doi.org/10.3390/socsci10120466>

Academic Editors: Grazia Concilio, Giuliana Costa and Maryam Karimi

Received: 18 October 2021
Accepted: 1 December 2021
Published: 6 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: ICT tools; migrant integration; data protection; impact assessment

1. Introduction: Integrating Migrants through Connected Tools

Connectivity has become ubiquitous in everyday life and people resort to smart devices in all areas of life, to socialize, to work, to access information, for traffic navigation, entertainment, etc. The COVID-19 pandemic further expanded the use of technological means and internet connection to enable interaction between those who were forced into isolation to prevent the spread of the virus. In this context, it is not surprising that the use of smart devices has penetrated all layers of society and even those considered vulnerable, such as migrants and asylum seekers travelling through dangerous routes, rely on connectivity to obtain information, reach safety, contact their loved ones, and integrate in their new society.

Indeed, at the beginning of the so-called refugee crisis in Europe in the mid-2010s, those waiting to receive migrants arriving at Greek shores were equipped with water, food, blankets, and first-aid supplies, and were thus initially surprised with and unable to respond to new arrivals' constant request for a place to charge their phones and access the internet (Balestra 2019). With the continued arrival of migrants in Europe, however, the idea of connected refugees or connected migrants has become commonplace (Awad and Tossel 2021).

Recognizing that connectivity is essential to allow refugees and displaced persons to communicate with their family members as well as to access basic services such as health and education, in a 2016 report, the office of the United Nations High Commissioner for Refugees (UNHCR) stated its commitment to working with multiple partners to bring connectivity to refugees worldwide (UNHCR 2016).¹

Building on the idea of connected migrants, another recent initiative involving connectivity and migration is the call launched by the European Union (hereafter EU) for projects seeking to address the challenge of migrant integration through ICT-enabled solutions

under the EU's Horizon 2020 research and innovation program. Six projects were selected to receive funding to develop ICT tools to assist migrants to integrate in their new European society.² The envisaged solutions aim to facilitate migrants' access to local services as well as to provide tailored recommendations regarding those services. Potentially, these tools can provide a one-stop shop in which migrants would be able to look for a job, receive suggestions on trainings to improve their professional profile, search for educational offers, book medical appointments, find housing, contact legal services, see local events taking place near them, etc.

Governments have also engaged in digitalization initiatives for its national residents. In Ukraine, for example, "Ukrainians can obtain electronic versions of their internal ID, passport, driving license, car registration certificate, car insurance, student ID card, taxpayer's number, birth certificate, and an e-IDP³ certificate. They can also change online their residence and voting addresses and pay any outstanding fines and fees to the state" (Kuzemska 2021). While these systems in Ukraine focus on Ukrainian nationals, including internally displaced persons, it is not far-fetched to foresee that such systems will be expanded to migrants in Ukraine and elsewhere, considering the current trends to increase digitalization worldwide in a great number of fields, including those that affect migrants (see more on Section 3 below).

While the goal of these and similar initiatives is often to empower and assist migrants in smoothly accessing information and services, ICT tools come with inherent risks. These risks may relate to cybersecurity and privacy concerns but also in the specific case of refugees and asylum seekers, they may relate to a fear of surveillance and/or interception of data from their devices leading to persecution of their families in their country of origin or negatively influencing their asylum application (Martin 2021).

Against this background, in the current article, we argue that to mitigate these risks, technology developers focusing on ICT tools for migrant use should work with multi-disciplinary experts to engage in an extensive data protection impact assessment process that should inform the development of the concerned tools, ensuring the achievement of the highest possible protection standards. Such an extensive process should not only focus on the applicable legal framework but also be tailored to the context in which the developing tools will apply and thus take the specific needs and vulnerabilities of migrants into account. In this context, Section 2 will extend the proposition that a data protection impact assessment can be used as a protection tool; Section 3 will then discuss the context in which such assessments are deployed, digging deeper into the challenges that ICT tools may bring to migrants; building on this discussion, Section 4 will explain how a data protection impact assessment can be applied to mitigate these risks in practice with the example of the REBUILD project (one of the projects funded by the abovementioned Horizon 2020); finally, conclusions are provided.

2. (Expected) Results: Enlarging the Use of Data Protection Impact Assessments as a Protection Tool for Migrants

2.1. Data Protection Impact Assessments: An Introduction

The European General Data Protection Regulation (GDPR), which has in practice become the gold standard for data protection (Zomignani Barboza et al. 2020), prescribes in its article 35 that when the processing of personal data within new technologies is likely to result in a high risk to the rights and freedoms of natural persons, an assessment of the impacts of the envisaged processing operations on the protection of personal data must be carried out before the processing starts.

This assessment, a Data Protection Impact Assessment (hereafter DPIA), is explained in chapter 5 of the Handbook on Data Protection in Humanitarian Action as follows:

"The purpose of a Data Protection Impact Assessment (DPIA) is to identify, evaluate and address the risks to Personal Data—and ultimately to the Data Subject—arising from a project, policy, program or other initiative. A DPIA should ultimately lead to measures that contribute to the avoidance, minimization, transfer or sharing of data protection risks.

A DPIA should follow a project or initiative that requires Processing of individuals' data throughout its life cycle. The project should revisit the DPIA as it undergoes changes or as new risks arise and become apparent" (Kuner and Marelli 2020).

In practice, it has been proposed that a DPIA should be held in 10 steps (Kloza et al. 2019). The first step is screening, which will assess whether a data protection impact assessment is needed in the first place. The second step is the scoping, which identifies the societal concerns that may be affected by the initiative (e.g., privacy, data protection), the stakeholders affected by it and the techniques that will be used to assess the impacts of the project. Step three concerns the planning and preparation of the assessment, such as determining the assessment team and necessary resources. The fourth step provides a detailed description of the project or tool being developed, its potential benefits and possible drawbacks. Step five then proceeds to conduct an appraisal of these impacts (both negative and positive ones). In step six, recommendations are provided to enhance the expected positive outcomes and prevent the negative ones. Steps seven, eight and nine are ongoing steps that take place during the whole assessment process. In this regard, step seven is the stakeholder participation in decision making, which can be performed through multiple methods such as focus groups, roundtables, or workshops. Ongoing throughout the entire assessment, these interactions allow stakeholders to shape the assessment itself, assisting in identifying possible impacts. Step eight is documentation and represents the process' record keeping. Step nine is quality control of the assessment process. Lastly, step ten is revisiting, meaning that the assessment should be revisited and may be entirely remade every time significant changes are made to the project or technological tool in question.⁴

2.2. Processing Migrant Data: A Tailored Assessment

In this article, we argue that the DPIA can be used as a tool to protect migrants in the development of ICT tools that aim to facilitate their access to information and services to further their integration in their new society. To achieve this goal, the DPIA must be adapted to the context in which it is deployed and ensure that the specific aspects of handling migrants' data are taken into account in the process.

Thus, in step one, in which developers of ICT tools decide whether a DPIA is needed, the answer should always be a positive one. This is because migrants, and especially asylum seekers, may be in a vulnerable position, going through refugee status determination procedures or waiting on other migration decisions, and thus relying on authorities to obtain or renew their residence status when this is not yet secure. Most migration decisions are based on personal data of the migrants seeking to obtain a specific migration status and thus the risks of mishandling data of migrants and having such data made available may potentially influence these procedures, having severe impacts on their lives. Accordingly, the processing of their personal data is likely to result in high risks for their rights and should not be performed without a previous DPIA to ensure these risks are eliminated or mitigated as much as possible.

When identifying the societal concerns that are relevant for the assessment in step two, developers of ICT tools that have migrants as their main target users should not limit the concerns to the applicable legal requirements related to the protection of privacy and personal data. Instead, the societal concerns should be expanded to include other factors that may affect migrants specifically, such as their residence status in the country, their cultural background that may affect how they interact with technology, and whether the tool will create an added barrier that prevents them from accessing services instead of achieving its goal to assist them in that regard. Indeed, article 35 of the GDPR already mentions that a DPIA should be conducted when the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons, hinting at the fact that these rights are broader than data protection and privacy. Expanding the scope of a DPIA to include sector specific principles and rules has already been advocated when the data being handled are that of vulnerable populations such as those receiving humanitarian aid (see Zomignani Barboza et al. 2020). Similarly, it has also been argued that a DPIA

should be extended when the tools in question have effects that go beyond the processing of personal data. In this regard:

“The issues concerning data-intensive applications and their use in decision-making processes concern a variety of interests related to several fundamental rights and freedoms. Not only does the risk of discrimination represent one of the biggest challenges of these applications, but other rights and freedoms also assume relevance, such as the right to the integrity of the person, to education, to be equal before the law, and the freedom of movement, of thought, of expression, of assembly and freedom in the workplace” (Mantelero 2018).

Considering the possibly vulnerable situation in which migrants using these tools may find themselves, as well as the fact that ICT tools for integration are likely to interact with many of the above listed rights, it is only logical to extend the scope of the assessment to the reality, the concerns, and the needs of migrants and not limit it to an assessment of compliance with data protection rules. To achieve this, it is also essential that migrants are identified as stakeholders and thus consulted throughout the process to understand their views and incorporate them in the development of the tools, ensuring they reply to users' expectations.

In step three, it should be ensured that not only developers, but also legal and social experts are included in the assessment team so that all relevant legal and social concerns and possible impacts, especially those that are specific to migrants, are identified and appraised in steps four and five. Recommendations provided in step six should keep migrants' interests in mind while step seven should provide migrants a chance to participate in the development process and help shape the tools being designed. Steps eight and nine remain similar in all impact assessments, regardless of their field of application. It should be noted that, to increase transparency, the DPIA report (which is part of the documentation in step eight) may be made public in some situations.

Regarding step ten, an important thing to consider when developing and deploying an ICT tool to assist in migrant integration is that often ICT tools change hands, as after the developers release them, they may be sold to other companies that may integrate these tools in other applications or software from their portfolio. If this happens, it is likely that the DPIA will have to be revisited in part or entirely to assess how these changes will impact the users of such ICT tools, especially if these tools, which are built for migrants, are later merged with other applications that have a wider target audience. If this is the case, the revisited impact assessment will have to assess how these changes will impact the rights and expectations of migrants and, if the impacts are negative, the changes should not be implemented.

2.3. DPIA as a Protection Tool

When expanded and tailored as explained above, a DPIA not only assesses ICT tools' compliance with the applicable data protection framework, but also identifies how these tools will affect other rights and freedoms of migrants and whether they will achieve their goal of fostering integration or instead place more limits to migrants' access to services. In this way, a DPIA comes closer to a human rights impact assessment with regards to the activities of the initiative or project involving the processing of personal data. The way the DPIA can achieve these results and consequently protect migrants is by anticipating possible risks that may arise from the deployment of the ICT tools and recommending measures to mitigate them before the tools are released. In practice, this means that in the DPIA team, the legal experts will help translate the law into practice; the social experts will assess societal impacts that may arise from the use of such tools by migrant populations; and the developers will explain the technical possibilities and limitations of the tools under development. Together, they will work to adapt the development of the tools to the legal requirements and the needs of users. Lastly, by including the constant feedback of migrants themselves, who will be able to express their views, concerns, and expectations, the tools will be finetuned to the needs of end-users. In summary, following the whole lifetime of

the development, the DPIA process should influence the design from its onset to ensure the final tool is safe and efficient. At the same time, the DPIA process is complemented by other assessments such as human rights, environmental or socio-economic impact assessments, which will look at other impacts an initiative may have that are unrelated to the processing of personal data.

3. Discussion

As mentioned in the introduction to this article, it is commonplace that connectivity and ICT tools are part of a migrant's life and can assist them in accessing information and services as well as contacting loved ones and even finding safety. As was also noted above, however, connected technological solutions have inherent risks, which may be even greater for migrants and especially refugees due to their position of vulnerability in society. In this regard, one of the risks that is often associated with processing personal data of migrants is that should decisionmakers have access to such data, it may impact their decision regarding the concerned person's migration status. This concern is justified when one sees that different countries have enacted legislation that allows the confiscation of asylum seekers' phones and examination of the data therein to confirm their narratives (see [Jasmontaite-Zaniewicz and Zomignani Barboza 2021](#)). Furthermore, it has been said that States have been experimenting with multiple technological tools to automate and increase efficiency over migration management and border control in ways that sometimes may allow them to "create a differentiation of rights between citizens and non-citizens, exercise control over migrant populations, and externalize their responsibilities to uphold the human rights of migrants" ([Molnar 2019](#)).

Apart from migration decisions, for those who already have a secure status in the country, disclosure of data from certain ICT tools can still have important consequences in their integration. For example, if a migrant benefited from a cash-transfer assistance program that was enabled by connected solutions, this information, if made available to banks or other financial institutions, may influence the decision on whether or not to grant the concerned migrant a loan ([Martin 2021](#)).

Another issue to consider is that when ICT tools interact with social media platforms (for example, if the ICT tool for migrant integration allows users to login to the tool with their Facebook account or share content from the tool in social media platforms), information about the concerned migrants from the ICT tool may be used by these platforms to profile them for various purposes, including targeted advertisement.⁵

The technology used in such tools may also have consequences for its migrant users. For example, many of the ICT solutions created in current times are based on artificial intelligence.⁶ When using artificial intelligence, however, there is an inherent risk of bias that must be considered. One of the most well-known examples of such bias in AI is the algorithm used in the US to predict recidivism rates in criminal cases, which incorrectly rated black defendants as being almost twice as likely to reoffend than white defendants ([Angwin et al. 2016](#)). To avoid cases such as this, the Council of Europe recommends that AI developers "adopt a human rights by-design approach and avoid any potential biases, including unintentional or hidden, and the risk of discrimination or other adverse impacts on the human rights and fundamental freedoms of data subjects" ([Council of Europe 2019](#)). Consequently, it is essential that all measures are taken to mitigate the risk of bias and to promptly fix any unpredictable bias that may arise during the development of the ICT tools ([Zomignani Barboza et al. 2019](#)). This is even more relevant when the target population are migrants, who are often subjected to human bias and thus the data that are used to train the developing systems may be biased as well.

Regarding the societal challenges of using ICT tools to assist in the integration of migrants, it is also important to note that even though connectivity seems to be commonplace for most migrants, the usage of these tools is by no means equal within this population. For example, research on the digital life of refugees indicates that fewer women own, access, and use mobile phones than men ([Casswell 2019](#)). Similarly, one of the pointed challenges

to the digitalization of public services for the Ukrainian internally displaced population is that the majority of internally displaced Ukrainians are elderly people, who are less likely to use smart devices or have a stable access to the internet (Kuzemska 2021). Consequently, employing ICT solutions to foster migrant inclusion may instead accentuate differences between such population and even further exclude some of its members, such as women, the elderly or the digitally illiterate. Furthermore, digitalization may sometimes force migrants into using tools that they would prefer not to. In this regard, research has shown that sometimes, for migrants, “mobile connectivity is more of an uncomfortable imposition than (or in addition to) a desired toolkit” (Awad and Tossel 2021).

These are some of the challenges that ICT tools for migrant integration may face in achieving their goals. In practice, however, challenges will vary from initiative to initiative. For example, access to smart devices and good connectivity may not be a great barrier for tools having urban migrants in a well-connected city as their target group. This is why a tailored impact assessment, identifying the positive and negative impacts expected from a specific project, is essential to understand the risks and benefits of a developing tool. To illustrate some of these efforts in practice, the next section presents the work of the authors of this article in the REBUILD project, in which they contributed to the project’s DPIA.

4. Materials and Methods: A Tailored Impact Assessment Applied in the REBUILD Project

As proposed in Section 2, a tailored impact assessment was applied by the authors of this article in REBUILD, a 3-year research project funded by the abovementioned EU Horizon 2020 Research and Innovation program. The aim of the project is to develop ICT tools that will assist migrants, especially refugees and asylum seekers, to integrate into their new societies in Italy, Greece, and Spain by facilitating access to services in the fields of health, education, employment, housing, legal assistance, and social mentoring. These tools would be materialized by the creation of a dashboard for service providers (including both government authorities and non-governmental organizations providing services to migrants) in which they can add information about their services and events that can be of interest to migrants and the REBUILD app. The REBUILD app is an application that will guide migrants through the available services in their area. This is performed through a digital companion, that is, an easy-to-understand chatbot, which helps migrants navigate the app to find the services they need. For example, the chatbot can assist migrants who are seeking employment to complete a professional profile and match such profile with relevant job offers in the region. The end products of the project would thus be aimed at service providers (dashboard) and migrants (the REBUILD app).

According to the EU Regulation that established the Horizon 2020 program, all relevant project activities must comply with ethical principles as well as the law.⁷ In this regard, the authors of this article represent REBUILD’s consortium partner in charge of the project’s legal and ethical impact assessment. Thus, our tasks included determining the legal and ethical framework that applies to the project, following the abovementioned proposal to expand this framework to include the specific context in which the project inserts itself, i.e., migrant integration, as well as working with project partners to ensure project activities are in line with said framework throughout the whole lifecycle of the project.

In this regard, the first year of the project was marked by the development and execution of a tailored data protection impact assessment, consistent of multiple steps. Initially, the legal and ethical framework that applies to REBUILD was determined. This task showed that in the project’s context, protection of participants’ right to privacy and data protection, enshrined in articles 7 and 8 of the EU Charter of Fundamental Rights, interpreted broadly, were at the center of the assessment, especially considering the need to gather a significant amount of participants’ data to train the smart systems that would be used in the envisaged ICT tools. This assessment also considered the risks that can arise to participants’ fundamental rights should the project data not be properly secured. The GDPR was thus the main instrument against which project activities were to be assessed. This assessment, however, also included ethical standards, for example, when ensuring

that participants' consent to the processing of their personal data in REBUILD was freely provided, their comfort, voluntariness and willingness to engage in the project were taken into account, ensuring they were properly informed of the project's goals and activities and allowing them to stop their participation at any time and exercise their rights as data subjects, including having their personal data erased should they decide to terminate their involvement in the project.

Once the extended applicable framework was established, legal advisors worked on developing a tailored method to assess the possible impacts and risks of the project. Such method included a comprehensive questionnaire to be answered by all partners regarding their activities, especially those involving external participants (mainly migrants) and the processing of their personal data. This process was concluded with the elaboration of the impact assessment report, identifying possible risks, and providing recommendations for project partners to address them. Two monitoring reports follow in years 2 and 3 of the project in the context of continuously monitoring project activities' compliance with the applicable framework.

Throughout the project, legal advisors also engage in constant dialogue with project partners to help shape both activities involving participants and the design of the ICT tools that are to be created. In this regard, legal advisors worked closely with technical partners to translate the legal and ethical requirements into practical actions and assist in the design of the data model that constitutes one of the bases of the future REBUILD app, as it defines which categories of personal data from migrants will be processed. With a strong focus on data minimization, that is, processing the minimum amount of data necessary, legal advisors and other REBUILD partners worked to reduce the amount of data required from participants as well as to ensure no direct identifiers were collected. This is because if data are never processed, it may not be misused in any of the abovementioned ways.

The emphasis placed on data minimization also influenced the design of the app itself, which will contain different layers of interaction according to how much information end users are willing to provide the ICT tool. Thus, users will be able to choose to use only the services that do not require any data processing or to provide data that are needed specifically for the services they wish to use. For example, if a user is interested in REBUILD's job searching functionality, s/he will only be asked to provide data about their employment and education background, as well as professional skills and experience. No further information will be requested at any point to access that specific service. Furthermore, an easy to read and informative privacy policy explaining the data processing that will take place in the future REBUILD app was developed by legal advisors together with technical partners to inform future users during the piloting phase of what to expect from such an app, increasing transparency and trust in the tool.

All the above-mentioned steps, however, are not able to represent the full dimension of the work performed in REBUILD to comprehensively anticipate and mitigate risks, following the proposition of Section 2 of this article. Parallel to the legal and ethical impact assessment, a socio-economic impact assessment also took place. This assessment aims to further one of the project objectives, which is to strengthen social links at a local level and promote social inclusion. This process will thus, among others, consider migrants' literacy level and the perception about their degree of integration while also looking at local service providers' enhancement of their capacities in managing service provision to migrants.⁸ This social-focused analyses complements the legal and ethical assessment mentioned above. Together, these assessments cover a multitude of potential risks and benefits the project may entail to the rights and freedoms of migrants, in particular regarding their integration in their new society, thus ensuring a thorough assessment of the project's impact on its target population.

Furthermore, co-design workshops were organized including project partners, migrants, and local service providers to include all stakeholders in the development process. Including also experts from scientific, technical and social fields, these workshops aimed to identify the scenarios and requirements that the REBUILD toolbox should include, ana-

lyzing existing good practices, identifying migrants' needs, and discussing matters from the current social and cultural barriers to questions related to personal data protection.⁹ Also, efforts were taken to ensure the largest possible population can access the tools, such as the development of pictograms and signs understandable by multiple ethnicities and audiovisual clips for each of the ethnicities present in the regions to be included in the ICT tools developed by the project (Zomignani Barboza et al. 2019).

Together, all these steps seek to ensure the development of safe and adequate tools to assist in the integration of migrants. As mentioned in Section 2, however, an added challenge will arise at the end of the project. Should the developed tools be acquired by other parties or incorporated in existing applications, it may require revisiting the impact assessment, a process that will depend on the new parties controlling the ICT tools.

5. Conclusions

In a world where political discourse is increasingly anti-migration and technological tools are often trying to strengthen border control and thus prevent migration altogether, ensuring the protection of migrants in the development and deployment of ICT tools that will have an impact on their lives is of utmost importance for initiatives that wish no harm for those they affect. In this regard, a DPIA can be used as a protection tool to anticipate and mitigate the risks that such a tool may bring to the rights and freedoms of their migrant users. Expanding the DPIA to include not only the applicable data protection framework but also other social and ethical concerns that relate to the context in which the tool will be deployed will lead to a stronger assessment and thus a safer tool. The participation of migrants in the development process is particularly important to ensure their views are considered and the social concerns related to them are correctly identified and addressed. This will include assessing migrants' relationship with technology and evaluating whether the tool being developed is the right means to achieve the integration goal in the specific context in which the tool will be deployed. At the same time, clear communication between legal and social experts and developers is needed to translate the legal and social concerns into practice within the realm of possibilities of current technology.

In this context, we hope that the proposed use of a tailored DPIA and the practical experience of legal advisors in REBUILD, not only assessing project activities' compliance with the applicable framework but in practice assisting partners implement this framework in their work and consequently in the ICT tools resulting from the project, is seen as the best practice to be followed.

Author Contributions: Conceptualization, J.Z.B. and P.D.H.; methodology, J.Z.B. and P.D.H.; investigation, J.Z.B.; writing—original draft preparation, J.Z.B.; writing—review and editing, P.D.H.; supervision, P.D.H.; project administration, J.Z.B. and P.D.H.; funding acquisition, P.D.H. All authors have read and agreed to the published version of the manuscript.

Funding: The research done in the context of the REBUILD project was funded by the European Union's Horizon 2020 research and innovation program, grant number 822215.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Helsinki, and approved by the Institutional Review Board (or Ethics Committee) of Universitat Autònoma de Barcelona (protocol code 4387, approved on 29 March 2019).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Notes

- ¹ Three years later, in 2019, UNHCR published a follow-up report, presenting the work they had done to reach that goal, the achieved results and lessons learned. The report, *Connections*, is available online: <https://www.unhcr.org/innovation/wp-content/uploads/2019/11/CfR-Publication-Connections.pdf> (accessed on 25 May 2021).

- ² The list of projects as well as more information about them and about Horizon 2020 is available online: https://ec.europa.eu/info/dt-migration-06-2018-2019-projects_en (accessed on 25 May 2021).
- ³ IDP stands for internally displaced person.
- ⁴ A more detailed description of the steps can be found in (Kloza et al. 2019).
- ⁵ For more on the risks that social media usage may pose to vulnerable populations, see (Kuner and Marelli 2020, chp. 13).
- ⁶ According to the Council of Europe, artificial intelligence can be defines as “[A] set of sciences, theories and techniques whose purpose is to reproduce by a machine the cognitive abilities of a human being” (Council of Europe 2021).
- ⁷ “[A]ll the research and innovation activities carried out under Horizon 2020 shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols.” Article 19, Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020, the Framework Programme for Research and Innovation (2014–2020) and repealing Decision No 1982/2006/EC Text with EEA relevance OJ L 347, 20 December 2013.
- ⁸ See more on REBUILD’s website: <https://www.rebuildeurope.eu/en/work-package.aspx> (accessed on 1 December 2021).
- ⁹ See more on REBUILD’s website: <https://www.rebuildeurope.eu/en/area-partner.aspx> (accessed on 1 December 2021).

References

- Angwin, Julia, Jeff Larson, Surya Mattu, and Lauren Kirchner. 2016. Machine Bias: There’s Software Used across the Country to Predict Future Criminals. And It’s Biased against Blacks. *ProPublica*. Available online: <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> (accessed on 1 June 2021).
- Awad, Isabel, and Jonathan Tossel. 2021. Is the smartphone always a smart choice? Against the utilitarian view of the ‘connected migrant’. *Information, Communication & Society* 24: 4–611. [CrossRef]
- Balestra, Giulia. 2019. The Final Frontier for Inclusive Connectivity. *UNHCR Innovation Service*. Available online: <https://medium.com/unhcr-innovation-service/the-final-frontier-for-inclusive-connectivity-7b279550c277> (accessed on 25 May 2021).
- Casswell, Jenny. 2019. The Digital Lives of Refugees: How Displaced Populations Use Mobile Phones and What Gets in the Way. *GSMA*. Available online: <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/07/The-Digital-Lives-of-Refugees.pdf> (accessed on 27 May 2021).
- Council of Europe. 2019. Guidelines on Artificial Intelligence and Data Protection. Available online: <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8> (accessed on 1 June 2021).
- Council of Europe. 2021. Glossary. Available online: <https://www.coe.int/en/web/artificial-intelligence/glossary> (accessed on 1 June 2021).
- Jasmontaite-Zaniewicz, Lina, and Júlia Zomignani Barboza. 2021. Disproportionate surveillance: Technology-assisted and automated decisions in asylum applications in the EU? *International Journal of Refugee Law* 33: 89–110. [CrossRef]
- Kloza, Dariusz, Niels Van Dijk, Simone Casiraghi, Sergi Vazquez Maymir, Sara Roda, Alessia Tanas, and Ioulia Konstantinou. 2019. Towards a Method for Data Protection Impact Assessment: Making Sense of GDPR Requirements (d.pia.lab Policy Brief No. 1/2019). *d.pia.lab*. Available online: https://cris.vub.be/ws/portalfiles/portal/48091346/dpialab_pb2019_1_final.pdf (accessed on 26 May 2021). [CrossRef]
- Kuner, Christopher, and Massimo Marelli. 2020. *Handbook on Data Protection in Humanitarian Action*, 2nd ed. Geneva: ICRC.
- Kuzemska, Lidia. 2021. How Useful Is ‘State in Smartphone’ for the IDPs in Ukraine? *RLI Blog on Refugee Law and Forced Migration*. Available online: https://rli.blogs.sas.ac.uk/2021/05/10/how-useful-is-state-in-smartphone-for-the-idps-in-ukraine/?utm_source=Refugee+Law+Initiative&utm_campaign=3d4ef34b50-EMAIL_CAMPAIGN_2017_10_03_COPY_01&utm_medium=email&utm_term=0_304c0b75a9-3d4ef34b50-581036941 (accessed on 1 June 2021).
- Mantelero, Alessandro. 2018. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review* 34: 754. [CrossRef]
- Martin, Aaron. 2021. Connecting with Confidence: Managing Digital Risks to Refugee Connectivity. *UNHCR*. Available online: <https://www.unhcr.org/innovation/wp-content/uploads/2021/03/CWC-Managing-Digital-Risks-To-Refugee-Connectivity-Report.pdf> (accessed on 25 May 2021).
- Molnar, Petra. 2019. Technology on the margins: AI and global migration management from a human rights perspective. *Cambridge International Law Journal* 8: 2–305. [CrossRef]
- UNHCR. 2016. Connecting Refugees: How Internet and Mobile Connectivity Can Improve Refugee Well-Being and Transform Humanitarian Action. *UNHCR*. Available online: https://www.unhcr.org/innovation/wp-content/uploads/2018/02/20160707-Connecting-Refugees-Web_with-signature.pdf (accessed on 25 May 2021).
- Zomignani Barboza, Júlia, Sergi Vazquez Maymir, and Paul De Hert. 2019. Deliverable: D7.1 Report data protection, privacy, ethics and societal acceptance (ARTES framework). *Rebuild Project Deliverable*. Available online: https://www.uninettunouniversity.net/en/p1_rebuilddeliverables.aspx?page=4 (accessed on 1 December 2021).
- Zomignani Barboza, Júlia, Lina Jasmontaite-Zaniewicz, and Laurence Diver. 2020. Aid and AI: The Challenge of Reconciling Humanitarian Principles and Data Protection. In *Privacy and Identity Management—Data for Better Living: AI and Privacy*, 1st ed. Edited by Michael Friedewald, Melek Önen, Eva Lievens, Stephan Krenn and Samuel Fricker. Cham: Springer, pp. 161–76. [CrossRef]