Co-funded by the Horizon 2020 programme of the European Union

www.h2020mirror.eu

MIRROR

Migration-Related Risks caused by misconceptions of Opportunities and Requirements

Grant Agreement No. GA832921

Deliverable D3.2

Work-package	WP3: Legal Compliance, Societal Acceptance & Ethical Framework
Deliverable	D3.2: Human Rights Implications Checklist
Deliverable Leader	RUG
Quality Assessor	AItana Radu
Dissemination level	Public
Delivery date in Annex I	M12, May 31, 2020
Actual delivery date	27 July 2020
Revisions	2
Status	Final
Keywords:	Ethics, Privacy and Data Protection

Disclaimer

List of Abbreviations

AI	Artificial Intelligence
CFREU	EU Charter of Fundamental Rights
COE	Council of Europe
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EU	European Union
FRA	Fundamental Rights Agency
GDPR	General Data Protection Regulation
LEA	Law Enforcement Agency
NGO	Non-Governmental Organisation
RUG	University of Groningen
UN	United Nations
UN OHCHR	Office of the United Nations High Commissioner for Human Rights
WP	Work Package

List of Authors

Partner Acronym	Authors
RUG	Jeanne Mifsud Bonnici
	Joseph Cannataci
	Jonida Milaj-Weishaar
	Tiphaine Bouglon
	Mattis van 't Schip
UM	Aitana Radu

Table of Contents

Table of Contents 5

Executive summary 6

1. Introduction 7
  1.1 Background 7
    Borders and technology 7
    MIRROR and its technologies 9
  1.2 Task 3.2 & Methodology 10
    Task T3.2 10
    Methodology followed in the preparation of this document 10

2. Human Rights implications checklist 11
  2.1 Introduction 11
  2.2 Human rights implications checklist: assumptions 13
  2.3 The Human Rights Implications Checklist 14

3. Conclusion 43

Bibliography 44

Appendix 1 48

Executive summary

This document, a *Human Rights Implications Checklist*, was developed as part of Task 3.2 of the MIRROR project. The aim of the task was to carry out a broad human rights analysis of the potential effects from a human rights perspective of using sentiment analysis techniques in border security. The latter is one of the aims of the MIRROR project. Based on this broad analysis, a *Human Rights Implications Checklist* was developed with the intention for this to be used by the technical partners involved in WP4, 5, 6 and 7.

A selection of fundamental rights was made based on a literature review of human rights implications of technologies used to strengthen border enforcement and manage migration and keeping in mind the nature of the tools being developed in the MIRROR project. Four types of tool building are evident in the MIRROR platform:

A. Tools identifying behaviour through the text analysis of social media and other media
B. Tools identifying behaviour through image analysis
C. Tools trying to predict behaviour, perceptions or choices based on the analysis obtained from the text and image analysis
D. Tools integrating the results of all of the above.

The fundamental rights under review are the following:

- the right to non-discrimination
- the right to respect to private and family life
- the right to freedom of expression
- the right to freedom of assembly and Association
- the right to data protection
- the right to be given the basis of an automated decision taken against an individual[1]
- the right to a fair trial.

The approach taken in this document is to assume that none of the members in the teams of WP4, 5, 6, and 7 have extensive human rights knowledge but they are prepared to engage with the legal team within the project on reflecting on the human rights implications of the tools being developed. In light of this, this *Human Rights Implications Checklist* does not assume expert knowledge nor does it attempt to provide a complete human rights training. The *Human Rights Implications Checklist* is not a stand-alone document but an internal tool to facilitate the discussion and responsibilities of the MIRROR consortium towards addressing human rights ramifications of the technologies being developed in the project.

[1] This is not a right found in the Charter of Fundamental Rights of the European Union or the European Convention of Human Rights. It is a right that has been included in the General Data Protection Regulation.

1. Introduction

1.1 Background

Borders and technology

Migration both globally and in Europe is on the rise. Since 2015, with the so-called "refugees and migrant crisis", Europe too has dealt with increasing numbers of asylum seekers. 2.4 million refugees and people in refugee-like situations and 860 thousand asylum-seekers (pending cases) were hosted in EU-27 Member States at the end of 2018.[2]

This increase in numbers of migrants together with the increase in number of travellers at land, sea and air borders have pushed towards a rethinking of the management of border control and migration flows. Technology and new technological thinking are seen as central to this rethink.

The use of technology can be seen:

(a) securing (physical) national borders, e.g. The U.S. Department of Homeland Security relies on a variety of electro-optical cameras, lasers, chemical detectors, X-rays, and other sensors to limit entry of illegal immigrants, drugs, and other contraband.[3] Such technologies include thermal imaging equipment (documented as being used in Austria, Germany) and other kinds of human presence detectors (used in Germany, Belgium, Ireland, Latvia, Slovak Republic).[4]

(b) using advanced analytics including using video and biometric analytics. Border agencies increasingly use data from multiple points rather than only from traditional sources such as visa applications and border crossing points. For example, travel companies and freight forwarders. Through this, more complete profiles of travelers are compiled.

(c) predictive modelling aimed at reducing risk and improving security, e.g. using passenger risk assessments based on Passenger Name Record (PNR), Advanced Passenger Information (API) and incorporating analyses of their social media profiles to clamp down on illegal migration.[5]

(d) use of identification and verification technologies using biometric parameters such as iris, finger prints, facial recognition.[6]

---

[2] https://migrationdataportal.org/regional-data-overview/europe accessed on 27th July 2020.

[3] https://www.militaryaerospace.com/unmanned/article/16707261/the-role-of-technology-in-securing-the-nations-borders

[4] European Migration Network (2012) Practical Measures to Reduce Irregular Migration available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/european_migration_network/reports/docs/emn-studies/irregular-migration/00a_emn_synthesis_report_irregular_migration_october_2012_en.pdf

[5] Accenture (2017) Crossing Boundaries: Emerging Technologies at the border available at https://www.accenture.com/t20170214T094928__w__/us-en/_acnmedia/Accenture/cchange/border-services-report/Accenture-Emerging-Technology-Border-Service-Report.pdf pg 5

[6] EU-LISA (2015) Testing the borders of the future: Smart Borders Pilot: The results in brief accessed at https://www.eulisa.europa.eu/Publications/Reports/Smart%20Borders%20-%20The%20results%20in%20brief.pdf

(e) advanced analytics to monitor sentiment proactively on social media, e.g. the Australian government has invested AU$19 million in a stronger social media monitoring and analysis capability to help combat terrorist content.[7]

(f) several large-scale data bases: e.g. the EU has developed several large-scale IT systems or mechanisms for the collection and processing of data that can be used for border and migration management.[8]

(g) access to data held in databases created for other purposes including financial transactions such as credit card spending, bank accounts, and other transactional data such as that generated by mobile phone or travel activity, in order to better profile individual travelers stopped for routine questioning and other processing at a border point;

(h) big data predictions about population movements[9]

(i) automated decision-making in migration applications (e.g. for reunification of families by comparing information filled in the form to existing information in EU data bases.)[10]

Undoubtedly border control is increasingly becoming more efficient and effective. However, this efficiency may be coming at a cost: profound human rights ramifications and real impacts on human lives. States have an undeniable sovereign right to control the entry of non-nationals to their territory.[11] Yet, while exercising border control, states have a duty to protect the fundamental rights of all people under their jurisdiction, regardless of their nationality and/or legal status. This document reflects a move towards encouraging a reflection on human rights implications from the design stage of any technology used for border security purposes. This approach does not mean that all potential human rights impacts will be eliminated but rather that some of the more evident impacts may possibly be reduced at the start of the process.

[7] https://www.abc.net.au/news/2015-02-20/brandis-announces-program-to-combat-terrorist-propaganda/6160406 and Accenture (2017) Crossing Boundaries: Emerging Technologies at the border available at https://www.accenture.com/t20170214T094928__w__/us-en/_acnmedia/Accenture/cchange/border-services-report/Accenture-Emerging-Technology-Border-Service-Report.pdf pg 8

[8] See table 6 in Fundamental Rights Agency (2018) Preventing unlawful profiling today and in the future: a guide - https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf at pg 113

[9] Such as the Displacement Tracking Matrix developed by the UN IOM available at https://dtm.iom.int/

[10] Accenture (2017) Crossing Boundaries: Emerging Technologies at the border available at https://www.accenture.com/t20170214T094928__w__/us-en/_acnmedia/Accenture/cchange/border-services-report/Accenture-Emerging-Technology-Border-Service-Report.pdf pg 10

[11] See discussion of the rights and obligations of states while exercising border control in Fundamental Rights Agency and Council of Europe (2020) Fundamental rights of refugees, asylum applicants and migrants at the European borders. Available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-2020-european-law-land-borders_en.pdf

MIRROR and its technologies

MIRROR contributes to the technological developments listed above. It aims to produce technical tools to help assess the perceptions and misperceptions of Europe and individual European countries of persons migrating to Europe. By understanding these perceptions and misperceptions, it is hoped the border agencies can adopt a more predictive-oriented approach to their activities and manage migration flows, expectations, as well as their resources better. The analysis of perceptions and misperceptions relies on data sets made up of social media and traditional media (analysing texts, video and images).

The goal of the MIRROR project is to develop an integrated open source information platform, a set of tools on top of this platform, as well as a systematic methodology for the comprehensive intermedia analysis of the perception of Europe, the detection of discrepancies between perception of and reality in Europe, and the creation of awareness for the impact of such misconceptions and the resulting threats, including hybrid threats. In a process driven by perception-focused threat analysis, the MIRROR project combines methods of automated text, image, video, social network and sentiment analysis for various types of media content (including social media) with empirical studies for creating a substantiated picture of the external perception of Europe. Solutions developed in the project include technology and actionable insights.[12]

In addition, MIRROR is built on strong respect for the rule of law and fundamental rights, in particular the rights to privacy, data protection and freedom of expression. This document is part of the process ensuring that MIRROR is actually built in a way where respect for fundamental rights is prominent. In particular, it prepares a *Human Rights Implications Checklist* (as identified in Task T3.2) to be used within the project, especially by the teams in WP4 – Text Analysis Methods for Social and Traditional Media; WP5 – Multimedia Analysis Methods for Social and Traditional Media; WP6 – Methods for Cross-Media Network Analysis and WP7 – MIRROR Architecture and Information Model.

As will be explained later in this document (section 2), the following fundamental rights (chosen following a literature review of human rights implications of technologies used to strengthen border enforcement and manage migration and keeping in mind the nature of the tools being developed in the MIRROR project) are under review in the checklist prepared:

- the right to non-discrimination
- the right to respect to private and family life
- the right to freedom of expression
- the right to freedom of assembly and association
- the right to data protection
- the right to be given the basis of an automated decision taken against an individual[13]
- the right to a fair trial.

[12] MIRROR – Migration-Related Risks caused by misconceptions of Opportunities and Requirement – Grant Agreement No.832921.

[13] This is not a right found in the Charter of Fundamental Rights of the European Union or the European Convention of Human Rights. It is a right that has been included in the General Data Protection Regulation.

1.2 Task 3.2 & Methodology

Task T3.2

In task T3.2 the project commits to "carry out a broad human rights analysis of the potential effects from a human rights perspective of using sentiment analysis techniques in border security. This task will not only focus on the rights of privacy, data protection and association but will explore broader implications such as discrimination, inequality, bias, lack of due process etc. This task will choose a number of existing border security systems using some form of data driven technologies (such as systems being developed in Israel and the United States) as case studies upon which to focus on. This task will build on studies that have been carried out by previous research, different think tanks and civil society organisations. Furthermore, a special focus will be given to the effects of automated decisions being taken on the basis of the analysis carried out. Based on this research, this task will prepare a human rights implications check-list that can be used by WP4, 5, 6 and 7."

Methodology followed in the preparation of this document

A three-step methodology was followed in the preparation of this document.

The first step was to understand the context within which MIRROR tools are being developed. What this step involved was to identify key categories in the field of technological tools developed to strengthen border enforcement and management of migration. To be able to do this, a literature review on border technologies ranging from large scale databases for border management and security purposes, to automated security and tracking programs at the border, to ones using big data for predictions of population movements was carried out. A particular focus in this research was the use of social media monitoring and exploitation of other openly available sources in border management and in particular in the monitoring of migration movements.

The second step focused on the human rights implications documented in literature on the different technological tools identified in the first step. Based on this review of human rights implications in literature, a shortlist of human rights that need to be taken into account in the MIRROR research process and technology development was drawn up.

The third step involved the preparation of the Human Rights Implications Checklist relevant and applicable for the MIRROR project. This third step also included a review of human rights checklists available for other fields and other contexts (e.g. human rights checklists in natural disaster management, for business, for employment practices, etc.) as well as human rights self-assessment compliance tools (developed for business); and human rights impact assessment tools developed by leading human rights institutions. In this process we looked also for human rights checklists or tools specifically designed for technology developers and computer scientists. We did not however come across any and so chose to use the checklists developed in other fields (and for different end users) and other tools meant to assist in respect of human rights were used as an inspiration for the design of the checklist. When preparing the human rights implications checklist, the explanations, examples and questions for further reflection explored below are linked back to the literature reviewed in step one and step two of the methodology.

2. Human Rights implications checklist

2.1 Introduction

What do we mean by *Human Rights Implications Checklist*? For whom has this checklist been compiled?

The intention of the task leading to the development of a human rights implications checklist was to develop a tool to help researchers in the MIRROR project to reflect on the human rights implications of the (AI) tools being researched and developed within the project.

The first topic of reflection which needs to be considered by researchers in the MIRROR project is that even if technology can perform a certain function/we can get technology to perform a certain function, it does not mean that we should automatically use the technological experiments without considering the (possibly) profound human rights ramifications and real impacts on human lives.[14] The aim is for the *Human Rights Implications Checklist* to work as a reflection tool for, in particular the computer scientists and technology developers (in WP4, 5, 6 and 7 of the project). Against this background, the *Human Rights Implications Checklist* is meant to briefly (at high level) explain the concerns that may arise from a human rights perspective and ask the researchers to reflect on the potential use of the technology they would be developing.

While preparing this checklist, we also saw other potential uses for a Human Rights Implications Checklist especially in the period of preparation leading to the deployment of the MIRROR tools by a border authority. We will prepare a draft of this (second) human rights implications checklist to be used, tested and validated during the piloting of the software (as planned in WP10). We will add this (second) human rights implications checklist to deliverable D.3.6, reporting on policy recommendations and supporting policy tools.

The creation of a human rights checklist also led us to reflect on the importance of prior knowledge i.e. at the point of setting out to work on the creation of any aspect of an AI-based system, what does the person concerned, especially if not formally trained in law, know about human rights? This leads us to suggest that all such teams should follow the “Highway code principle”. Society does not allow people to take their driving license without first sitting for a theoretical exam which is heavily based on that country’s highway code, which is in turn based on largely universal sets of rules and symbols agreed at international law[15] aimed at ensuring safety while driving, even for illiterate drivers. It is increasingly clear that society should likewise take all steps to ensure that technical and operational staff are not let loose on “the information highway” and AI-based systems are at least being trained and - very preferably tested – in basic human rights law and practise. It is only through such training aimed at achieving human rights literacy, that these actors can be equipped with the right conceptual framework that would help them appreciate the consequences of their work as well as the true meaning of the MIRROR Human Rights Implications Checklist. The checklist cannot be deployed to maximum effect unless the people

[14] https://edri.org/the-human-rights-impacts-of-migration-control-technologies/

[15] The Vienna Convention on Road traffic , 8 November 1968 last accessed on 26 July 2020 at https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XI-B-19&chapter=11

using it have some form of grounding in basic human rights.[16] A software engineer cannot be expected to properly protect privacy or freedom of expression in his or her work unless and until she or he has received formal instruction ensuring that those concepts are properly understood. So perhaps the first box in a Human Rights checklist for AI workers and other staff in border control contexts should be "Has the staff successfully undergone basic training in Human Rights law and practise?" Most recent experience confirms that such essential training cannot be assumed and should be delivered[17] as a matter of priority.[18]

The approach taken so far in the MIRROR project has been for the members of WP3 to informally discuss at project meetings and at work package meetings for WP4, 5, 6 and 7 individual fundamental rights and the background to each right. While this does not fully address the need for more systematic training, it has helped to raise the awareness of human rights law and practice among MIRROR researchers and compliments the reflections that we wish to continue to pursue with the aid of the *Human Rights Implications Checklist* developed below. Following this approach, the *Human Rights Implications Checklist* is not a stand-alone document but rather an internal tool intended to facilitate the discussion and responsibilities of the consortium towards addressing human rights ramifications of the technologies being developed in the project.

[16] It is to be noted that while some suggestions have been made at promoting human rights impact assessment and AI Literacy see e.g. Unboxing Artificial Intelligence: 10 steps to protect Human Rights available at https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-%20protect-human-rights-reco/1680946e64 , less emphasis has been made on Human rights literacy in the sector. Some work has been done on software engineering ethics e.g. Shannon Vallor and Arvind Naranyanan An Introduction to Software Engineering Ethics, last accessed on 26th July 2020 at https://www.scu.edu/media/ethics-center/technology-ethics/Students.pdf but a Human Rights handbook for software engineers cast in a privacy engineering mould is yet to be written. This should be similar to human rights handbook cast in a law enforcement mould written for Police Officers e.g. Human Rights and Law Enforcement: A Manual on Human Rights Training for the Police produced by UN OHCHR (Office of the High Commissioner of Human Rights) available at https://www.ohchr.org/Documents/Publications/training5en.pdf and which is part of an entire "professional series" including a Pocket Book, a Manual for trainers all available at https://www.ohchr.org/EN/PublicationsResources/Pages/TrainingEducationthree.aspx Another possible model is the recent (15 July 2020) practical guidance issued by the fundamental rights agency addressing border management stuff in the European Union member states work at the operational level. This is found at https://fra.europa.eu/en/publication/2020/border-controls-and-fundamental-rights-external-land-borders

[17] The Conversation, "We should teach human rights law to software engineers" 25 December 2018, last accessed on 26th July 2020 at https://thenextweb.com/syndication/2018/12/25/we-should-teach-human-rights-law-to-software-engineers/

[18] A useful source for such a training is Hildebrandt, Mireille (2019) Law for Computer Scientists accessed at https://lawforcomputerscientists.pubpub.org/pub/doreuiyy/release/7 This also raises the question "What is a computer scientist?" and what, if anything, differentiates a "computer scientist" from an information technology professional such as an analyst or a programmer, since it is the latter two professions which would largely bear the brunt of designing and coding AI systems. The "professional series" type of material prepared for the latter two professions may, on occasion, need to be nuanced from that prepared for the "computer scientist" in terms of both quantity and quality at levels of detail.

2.2 Human rights implications checklist: assumptions

Taking our point of departure as the designing and development of data analysis algorithms, we need to keep in mind that most of the MIRROR tools are there to enhance understanding by identifying correlations, patterns or casual relationships of data being collected, processed and used for the purpose of assisting border authorities. It is therefore this added meaning and its reliability that we need to keep in mind when we are reviewing human rights implications. There are four types of tool-building evident in the MIRROR platform:

A. Tools identifying behaviour through text analysis of social media and other media;
B. Tools identifying behaviour through image analysis;
C. Tools trying to predict behaviour, perceptions or choices based on the analysis obtained from the text and image analysis;
D. Tools integrating the results of all of the above.

An assessment of human rights impacts should take into account both the data used by the data sets and the applied analysis on the data ("the product"). To take an example concerning data sets, bias may be hidden in the dataset and thus not found in the algorithm itself when analysing it. When considering the applied analysis we need to consider that there are varying levels of discretion in the choice of relevant determinants, for instance, what training data to use or how to respond to false positives, and that the power of the operator of the algorithm may lie in his or her knowledge of the structure of the data set, rather than in insight into the exact workings of the algorithms.[19]

This is important to consider especially for tool set C. But the predictability of an algorithms outcome by the operator is important when considering its accountability and the design of adequate governance structures for its use. It is also important to keep in mind the reliability of all of these tools. Can our border control agency rely solely on the tools presented in MIRROR or is human decision-making equally important? Are we presenting the results of the tools as aids for decision-making or as the end result of decision-making? In each of these choices, resulting from these questions, there may be important human rights implications. As noted extensively in literature[20], judging the respective quality in decision-making processes by humans and by algorithms is fundamentally and categorically different. There are different mistakes which may have different outcomes and therefore different consequences.

The *Human Rights Implications Checklist* is divided into four sections:
1. General reflections on the technical process/es being explored
2. What data is being collected
3. Design choices
4. Analysing impacts on human rights

The first three sections are meant to identify clearly the technical process/analysis/algorithm being designed, developed and or applied in your research. The fourth section, based on the contextual information already given, analyses the human rights ramifications and possible real impact on human lives that can arise from that particular technical process/analysis/algorithm.

[19] Algorithms and Human Rights (2018) Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. (2018) https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

[20] See page 11 - Algorithms and Human Rights (2018) Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

2.3 The Human Rights Implications Checklist

Section 1. General reflections on the technical process/es being explored:

Note: This could be a single technical process or a set of processes together if they are pursuing the same aim

1.1. *Aim and Nature of the technical process*: Describe here what the process/algorithm will do (once developed) and why is it being developed.

1.2. *Aim:* What outcome are you hoping to achieve followed by further steps that are taken?

1.3. *Obstacles:* What are the main obstacles or barriers to achieving this aim?

Section 2. What data is being collected

2.1. What data is involved? Is some of the data personal data?

2.2. *Who will carry out the process*: who controls the actions of this process? Who is responsible for carrying it out? Here think ahead: if MIRROR is taken up in practice by LEAs who will be responsible for this process?

2.3. *People affected*: Who will/may be affected? How many people would certainly be affected? How many people could potentially be affected? Say a bit about the people affected (e.g. is a community identified, are individuals identifiable).

2.4. *Is data really needed? Can the aim be achieved in another manner? With less data?*

Section 3. Design choices

3.1. *Design choices*: in designing a process/action we make design choices, have we followed a

> 3.1.1. 'user-centred design' choice? And is the user here an LEA, an NGO, a researcher?
> 3.1.2. 'research subject centred design'? And who is the research subject here e.g. a migrant? An NGO worker?
> 3.1.3 "privacy by design" choice? Which are the immediate privacy concerns that would need to be addressed if the design is, say, either user-centred or research subject centred
> 3.1.4 "privacy by default" choice? Is any personal data being collected absolutely necessary for the objective of the project or else is it simply "potentially likely to be useful" or is it "just in case" one needs it later on? Can we do without it or is it absolutely necessary?

Section 4 Analysing impacts on human rights

An adverse human rights impact occurs when an action or omission removes or reduces the ability of an individual to enjoy her or his human rights.[21]

Three background considerations:
- human dignity
- autonomy
- responsibility.

Human dignity, as article 1 of the European Union Charter of Fundamental Rights states, 'is inviolable. It must be respected and protected'. The respect of the dignity of the human person is not only a fundamental right in itself but constitutes the real basis of fundamental rights. Indeed, the 1948 Universal Declaration of Human Rights enshrined human dignity in its preamble: *'Whereas recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world.'*[22] In essence, the concept of human dignity is the belief that all people hold a special value that's tied solely to their humanity. It has nothing to do with the class, race, gender, religion, abilities, or any other factor other than them being human.[23] Dignity can be thought of as the ability to pursue one's rights, claims or interests in daily life so that one can attain full realization of one's talents, ambitions or abilities, as one would like.[24] Central to the discussion of all human rights is respect to human dignity.[25] In the development of any technological tool we need to ensure that human dignity is respected. What this means in practice is that we can never lose sight in the development of the technology on the effects the technology or the process may have on human beings and that this effect should not be in any way disrespectful or harmful to the person. The discussion on other fundamental rights below helps in and supports the reflection on this fundamental approach that no technological development should in any way harm the dignity of a person.

Autonomy is a second important consideration in all our discussions on human rights. Autonomy refers to the ability of a person to act and to make independent choices that are significant for him or her.[26] The enjoyment of fundamental rights presupposes that one is able to make choices and to act following those choices in an autonomous manner. Any action that reduces this autonomy, e.g. by not allowing a person to make a choice, needs to be further explored. There may be times that a reduction in autonomy is justified by law but this should be considered to be an exception rather than the rule. This means that in the development and design choices in the MIRROR

[21] Office of the United Nations High Commissioner for Human Rights (2012), The Corporate Responsibility to Respect Human Rights: An Interpretive Guide, New York and Geneva: United Nations.
[22] See also the Explanations relating to the Charter of Fundament Rights OJ C303/17 -14.12.2007 found at https://fra.europa.eu/en/eu-charter/article/1-human-dignity
[23] https://www.humanrightscareers.com/issues/definitions-what-is-human-dignity/
[24] See: Edward J. Eberle, 'Observations on the Development of Human Dignity and Personality in German Constitutional Law: An Overview', Liverpool Law Review, November 2012, Volume 33, Issue 3, pp 201–233, available at <https://link.springer.com/article/10.1007/s10991-012-9120-x> and Paolo G. Carozza, 'Human Dignity', in 'The Oxford Handbook of International Human Rights Law' (Dinah Shelton, ed. 2013) (First edition), Oxford University Press, available at https://www-oxfordhandbooks-com.proxy-ub.rug.nl/view/10.1093/law/9780199640133.001.0001/law-9780199640133-e-15
[25] The European Court of human rights has gone so far to declare that 'the very essence of the Convention is respect for human dignity' (in Goodwyn v. UK, § 90; Pretty v. UK, § 65; VC v. Slovakia, § 105; SW v. UK; C v. UK, § 44).
[26] Watts L., Hodgson D. (2019) Human Rights and Autonomy. In: Social Justice Theory and Practice for Social Work. Springer, Singapore

project we need to ensure that the autonomy of any person affected by the technology or the technological processes is as far as possible not impacted. This may include for example that we may need to consider how to support the autonomy of persons whose social media post we may be using as the basis of our further analysis. At times respecting the autonomy of people also means additional steps the project or process needs to undertake to ensure this fundamental consideration.

At this point it is important to realise that going through a human rights implications checklist requires an open mind and the realisation that the results of further reflection on human rights and implications may require fundamental changes to the way we would have planned to design or further develop our technology and technological processes. This checklist is not meant to be just a tick box exercise indicating that we have considered human rights but one where a process of deep thinking on, and possibly extensive consequences for, the design choices have been followed.

The third consideration is responsibility: Do we have a responsibility to respect fundamental rights in the design of our technologies? We have both an ethical and legal responsibility to respect fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union and the European Convention of Human Rights. While, in these documents, the direct responsibility for these rights is directed towards states as the ones ultimately responsible for ensuring respect for fundamental rights, states have articulated many of these responsibilities in subsidiary laws and other legal principles towards different actors in the state. One example of this can be seen in the right to data protection: the right is addressed to states and is found in the Charter of Fundamental Rights of the European Union and the working out of this right and how this right needs to be protected in an everyday context is found in the EU General Data Protection Regulation which in turn requires developers of technology to reflect these data protection rights in the design and development of technical processes when processing personal data of individuals. Together with laws that come from the European and national level to respect the fundamental rights we are at times also guided by the judgements of the European Court of Human Rights, the Court of Justice of the European Union and judgements from national (constitutional) courts. The checklist below at times makes references to these judgements for clarification of certain concept or obligations. This document however does not comprehensively reference to all sources of responsibility. While reflecting on the questions in the checklist below we ask you to assume that technologists do have a responsibility to consider human rights ramifications and impacts of what they are developing. Technologists additionally share responsibility with others, for example an exclusively legal team of WP3, to also consider how these ramifications and impacts can be mitigated.

Structure of human rights table below

The table below consists of four columns. In the first column, we list the relevant human right that we consider needs further reflection during the development of technological processes in the project.

In the second column, we give a brief explanation of the right and what it consists of, we give (as far as possible) examples, sometimes fictitious, at other times related to developments in MIRROR and lastly, we introduce a set of questions to aid reflection on the ramifications and impacts that our technologies may have on this particular right.

In the third column, we note the degree of severity of impacts on this right. In this column we have tried to follow the guidance on establishing impact severity provided by the Danish Institute for Human Rights[27]. The purpose of establishing impact severity is not to establish which impacts need to be addressed, but to determine the order in which the identified impacts should be addressed. Following the UN Guiding Principles[28]

- All human rights impacts need to be addressed;
- Where it is not possible to address all impacts simultaneously, the impacts should be addressed in order of their 'severity';
- Severity is determined by the scope (number of people affected), scale (seriousness of the impact) and irremediability (any limits to restore the individual impacted to at least the same as, or equivalent to, her or his situation before the adverse impact occurred); and
- While it is not necessary for an impact to have more than one of these characteristics to be considered 'severe', it is often the case that the greater the scale or the scope of an impact, the less it is 'remediable'.

In the fourth column, we add some examples of possible mitigating strategies that can be applied by the project to reduce the impact on human rights. When suggesting mitigating strategies, it is important to consider that any alternative measure must also be compatible with human rights standards. We take this opportunity to note that human rights impact cannot be subject to 'offsetting' in the same way that, for example, environmental impacts can be. For example, a carbon offset is a reduction in emissions of carbon dioxide made in order to compensate for or to offset an emission made elsewhere. With human rights impacts on the other hand, due to the fact that human rights are indivisible and interrelated, it is not considered appropriate to offset one human rights impact with a 'positive contribution' elsewhere.[29] Hence, we cannot, for example, offset the wide collection of social media posts filtered on political opinion by not offering automated facial recognition capabilities in other parts of the MIRROR portal.

[27] https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria_toolbox/hria_guidance_and_toolbox_final_jan2016.pdf at pg 70

[28] UN Guiding Principles 12 and 24 and commentaries; Office of the United Nations High Commissioner for Human Rights (2012), The Corporate Responsibility to Respect Human Rights: An Interpretive Guide, New York and Geneva: United Nations.

[29] https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria_toolbox/hria_guidance_and_toolbox_final_jan2016.pdf at pg 76

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
Right to non-discrimination Art.14 ECHR Art.21 CFREU	*Explanation:* Article 21 CFREU stipulates that *"any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited."* The provision includes many different grounds on which one can be discriminated, which means that the anti-discrimination principle has a very broad reach. It is hence very important to establish on which ground a particular social media contributor or contributors are being followed by the MIRROR tools. Is the filtering based on criteria such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation? Given the aims of MIRROR, grounds such as political or other opinion, ethnic or social origin, language and religion may play an important role in the choice of data being selected and used for further analysis. The use of these selection criteria becomes problematic if the treatment of a person is based exclusively or to a decisive extent on any of the mentioned criteria. In addition, we may need to consider whether the use of social media in itself	Critical	Decisions not based exclusively or to a decisive extent on any of the criteria listed in article 21 CFREU Timely discarding of personal data collected for triangulation purposes

	becomes a form of discrimination in the case of MIRROR. In the MIRROR project, those persons who are active on social media, as opposed to persons who are not, are more actively tracked. Their social media information is part of the (mis)perception analysis, which MIRROR builds for its end users. Essentially, a person who is more active on social media is thus submitted to more intensive surveillance of the MIRROR project and forms the benchmark for the perceptions that their peers have of the European Union. The question is whether this activity on social media can be a form of discrimination, as the MIRROR project thus differs in surveillance based on social media activity. This participation on social media, together with the selection criteria which the MIRROR project may be using to follow a particular user, may lead indirectly to discrimination. Likewise, some algorithms may be aimed at detecting persons at borders who are taking counter-measures intended to avoid detection but which will generate false positives. Algorithms aimed at people using false names and images on social media or those avoiding social media may automatically trigger further privacy-intrusive searches including measures aimed at determining credit card and credit worthiness and/or movement/travel information thus also catching non-offenders in the search net.[30] Furthermore, the use of these criteria may impact the analysis of the perceptions that the MIRROR project is trying to produce. Would a perception		

[30] Raising the question at design stage “Where do I discard such data but retain a log of its being consulted?”

	reached on one or more of the above criteria correctly represent the perception of a wider group which may be effectively more heterogeneous then those narrowed down by the use of the above criteria? *Example:* Given an increase of migrants from Syria, social media posts and images in Syrian Arabic are closely reviewed for political and other opinions on Europe. Based on this review of social media posts, decisions can be made at the border to assess the justification put forward by migrants to be accepted into Europe. *Further explanation:* Profiling as a core tool in law enforcement work. Often the reaction to a discussion on non-discrimination within the police context is that it is in the nature of police work to build profiles to discriminate between people of interest for law enforcement matters and other persons. Indeed, as the recent report of the Fundamental Rights Agency[31] explains, profiling is commonly, and legitimately, used by law-enforcement officers and border guards to prevent, investigate and prosecute criminal offences, as well as to prevent and detect irregular migration. In the Police Data Protection Directive profiling is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects		

[31] Fundamental Rights Agency (2018) Preventing unlawful profiling today and in the future: a guide - https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

	concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".[32] The results of this data processing are used to guide border management and law enforcement actions, such as stop and search, arrests, refusal of access to certain areas, or referral to more thorough 'second line checks' at the border. There are two main uses of profiling: • To identify individuals based on specific intelligence. This uses a profile listing the characteristics of specific suspects, based on evidence gathered about a particular event. • As a predictive method to identify 'unknown' individuals who may be of interest to law enforcement and border management authorities; or to help in anticipating threats or risks (as may be the case in the MIRROR tools). Increasingly, algorithmic profiling is being used, that is, the use of different techniques combined together to profile people based on correlations and patterns in data. The collection and processing of large data sets raises a number of fundamental rights concerns. Avoiding discrimination is central to these concerns together		

[32] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119 (Police Directive), Art. 3(4).

	with risks in relation to the rights to privacy and data protection.[33] The Police Data Protection Directive prohibits discrimination (also in the case of profiling). This does not mean however that personal characteristics (referred to as protected grounds (such as age, gender, ethnicity or political opinion etc.)) cannot be used as legitimate factors for profiling in the context of criminal investigations or border checks. They can, however, only be used subject to a number of conditions: a. protected grounds must not be the sole or main bases for the profiling. b. these protected grounds can used as grounds/criteria when based on reasonable suspicion and they would need to be properly justified. c. to be justified differential treatment must pass the "necessity and proportionality test". (see in Appendix 1 the table produced by the Fundamental Rights Agency to explain the use of protected grounds in profiling.) *Examples of algorithmic profiling:* Following the 09/11 events in the US and the connection that one of the terrorists involved had belonged to a cell in Hamburg, Germany started a data profiling exercise, *Rasterfahndung*, aimed at detecting 'sleepers' in Germany. The criteria included age: 18-40, male, (former) student, resident in the regional state; religious affiliation; legal residency in Germany and nationality or country of birth from a list of 26 states with		

[33] Fundamental Rights Agency (2018) Preventing unlawful profiling today and in the future: a guide - https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

	predominantly Muslim population, or stateless person or nationality "undefined" or "unknown". This programme has not led to any visible success and has been severely criticised as not being in line with fundamental rights. In 2006, the German Constitutional Court ruled that data mining is illegal in the absence of a “concrete danger” to security or lives.341The court expressed concern that the screening focused on a particular religious community (Muslims) and was therefore likely to have a “stigmatizing impact” on those concerned and to “increase the risk of being discriminated against in working and everyday life.”[34] In the court’s view, a general threat situation of the kind that has existed continuously since 9/11 is not sufficient to warrant intrusions of this sort on personal data and privacy.[35] Beware software (USA)[36] - ‘Beware’ provides officers answering emergency calls with colour-coded scores (red, yellow, and green) indicating the threat level of the person or location involved. The software searches databases including arrest reports, property records, commercial databases, in-depth web searches, social media posts, and other publicly available databases. The strengths and weaknesses of this system have not been		

[34] http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg06-040.html. See also G. Kett-Straub, “Data Screening of Muslim Sleepers Unconstitutional,” at 967, 970–71.

[35] Further reading Martina Kant (2006) Nothing doing? Taking stock of data trawling operations in Germany after 11 September 2001 available at https://www.statewatch.org/media/documents/news/2006/aug/profil.pdf and Open Society Justice Initiative (2009) Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory available at https://www.justiceinitiative.org/uploads/8cef0d30-2833-40fd-b80b-9efb17c6de41/profiling_20090526.pdf pg 68 et seq.

[36] As described in Fundamental Rights Agency (2018) Preventing unlawful profiling today and in the future: a guide - https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf at pg 99.

	evaluated. However, the lack of oversight of the decision-making process and the secretive nature of the algorithm, which is protected by trade secrets, have raised concerns about accountability. In addition, the potential inaccuracy of the data collected, and/or the information inferred from the analysis, may reduce the overall effectiveness of the tool.[37] *Questions for reflection:* 1. Are any of the categories listed in article 21 being used as criteria to select media for perception/sentiment analysis? 2. Are there any other criteria that can be used which will reduce the risk of discriminatory behaviour?		
Respect for private and family life Art.8 ECHR Art.7 CFREU	*Explanation:*[38] This right protects persons from an arbitrary interference with the respect of their private life expressed in home, family life and correspondence. This right is not an absolute right. Interferences with this right can be justified but they have to respect the requirements identified in the EU Charter for Fundamental Rights and European Convention of Human Rights. Another element that needs consideration is the necessity of the interference. In general, even if justified, an interference with the private life of an individual can only be regarded as	Critical	Reduce the systematic collection and storage of data from social media users. As much as possible respect people's reasonable expectation of privacy by not carrying out analysis or predictions on 'silent majority' users.

[37] Additional information found in American Civil Liberties Union (ACLU) (2016), Eight Problems With Police "Threat Scores", 13 January 2016 available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/eight-problems-police-threat-scores

[38] See MIRROR Deliverable 3.1 for a broader discussion of this right.

	"necessary in a democratic society" if the interference with the private sphere of the individuals is counterbalanced by adequate guarantees against abuse.[39] While this right is very closely related to the right to data protection (discussed below), the right to private life is broader than data protection. Two aspects of this right are of particular relevance for this project and require close attention. Firstly, this right includes the enjoyment of the development of one's personality and one's thoughts without interference. This right (like the right to data protection) strives to protect the values of autonomy and human dignity of individuals, by granting them a personal sphere in which they can freely develop their personalities, think and shape their opinions. This right is often considered as an essential prerequisite for the exercise of other fundamental rights, such as freedom of thought, conscience and religion, freedom of expression and information, and freedom of assembly and of association.[40] In the MIRROR project context where the research is aimed at understanding the perception that people have about Europe, projecting these perceptions to groups of migrants or individuals, creates the possibility of interfering with their privacy of thoughts and feelings which may go		

[39] *Malone v The United Kingdom*, App no 8691/79 (ECtHR, 2 August 1984), para 81.
[40] Fundamental Rights Agency, Council of Europe and EDPS (2018), Handbook on European data protection law. 2018 edition, Luxembourg, Publications Office, June 2018, p. 19

	beyond what they may have formally expressed in social media. Furthermore, one may need to be particularly cautious in trying to use technology to identify or predict thoughts or behaviour of what is often referred to as the 'silent majority', that is, people who have not directly contributed to social media expressions but whose 'thoughts' and 'perceptions' are being predicted. Secondly, this right extends the enjoyment to the public sphere, that is, the right to the enjoyment of private life is not limited to activities that are kept or enjoyed in private but also to activities that take place in a public or potentially public context. This is also of particular relevance to the project. Even if most of the data sources that are being used in MIRROR come what from what is often referred to as open sources (that is the information is publicly available and that anyone can lawfully obtain by request, purchase, or observation) this does not automatically mean that the people contributing, appearing or reported upon in these sources no longer enjoy a right to private life. The European Court of Human Rights (ECtHR) has confirmed in its judgements that a simple viewing of activities, even if aided by technology, without any recording is considered as compatible with the right to privacy, but the situation changes as a result of new technological developments which enable the systematic and/or permanent recording of the data. In addition, even when participating online, a person may have a reasonable expectation of privacy. This expectation needs to be taken into account when considering the use,		

	one is making of the data obtained. In particular, systematic collection and storage of texts or images of particular persons may be considered as going against this reasonable expectation of privacy of an individual. Furthermore, in *Perry*, the ECtHR reasoned that an individual has a reasonable expectation of privacy when the person could not have been reasonably expecting the use of technology for scopes beyond the normal foreseeability of their use – in the concrete case the use of CCTV cameras for individual identification purposes.[41] The same reasoning would apply also for the MIRROR research since individuals using social media and internet without proper privacy filters are not expecting that their data will be harvested and processed for the purpose of research. *Example:* A likely example would be the use of OSINT technologies to help identify or categorise people crossing borders. If a face recognition programme is trained to also pick up the associates of a known felon or suspected terrorist and the faces on the "hit list" are gleaned from openly accessible social media sources, the likelihood of having one's privacy invaded increases significantly. For example, seating at charity balls are sometimes (but not always) allocated at random and sitting at a table of ten with "a person of interest" is not always a matter of personal choice. If a picture of that table ends up on social media, then it is likely to be used in the		

[41] *Perry v The United Kingdom* App no 63737/00 (ECtHR, 17 July 2003), para 41.

	searches carried out in relation to a particular suspect. Likewise, the accuracy rate of a system combining face recognition and OSINT must be extremely high in order to avoid the inconvenience and waste of resources which may be created by false positives. *Questions for reflection:* A. Does the process require the systematic collection and storage of personal data obtained from 'open sources'? B. When analysing sentiments or perceptions is the right to respect of private life being interfered with? Is there a justification for this? Is it necessary and proportionate in a democratic society?		
Right to freedom of expression Art.10 ECHR Art.11 CFREU	*Explanation:* one of the important aspects of the media including social media is that it allows the enjoyment of the right to freely express oneself as an individual, as a group and as a society. While limitation to this freedom may be allowed there are certain conditions for the limitations to be justified. In line with the jurisprudence of the European Court of Human Rights, any restriction of freedom of expression must correspond to a "pressing social need" and be proportionate to the legitimate aim pursued.[42] The impact on the right of freedom of expression can be either direct or indirect. A direct impact	Major	

[42] In *Yildirim v. Turkey*, 18 March 2013, no 3111/10.

	would be one where a person is prohibited or put in a position not to express himself or herself, for example, when a person is denied access to publish their opinion in a newspaper or on social media. An indirect impact is usually a result of actions, which do not directly affect a person but generate a situation which could lead a person to decide not to express their opinion. This is often referred to as the chilling effect. In MIRROR this is of particular relevance as will be shown in the example below. *Example*: following the rise of attacks on particular minority groups, a government decides to monitor social media posts that may refer to these minority groups. Some people may feel that this action would be putting them in the spotlight and hence choose to no longer express their opinion on the same minority group. This has the effect that these people's right to freedom of expression is being indirectly impacted. *Questions for reflection:* Can the systematic identification and analysis of social media posts of particular persons of interest in a migrant community possibly lead to chilling effect on the expression of these persons?		
Right to freedom of Assembly and Association Art.11 ECHR Art.12 CFREU	*Explanation:* The internet and in particular social networking services are vital tools for the exercise and enjoyment of the right to freedom of assembly and association, offering great possibilities for enhancing the potential for	Major	

	participation of individuals in political, social and cultural life.[43] The freedom of individuals to use internet platforms, such as social media, to establish associations and to organise themselves for purposes of peaceful assembly, including protest, has equally been emphasised.[44] In line with Article 11, any restriction to the right to freedom of peaceful assembly and to freedom of association must be prescribed by law, pursue a legitimate aim and be necessary in a democratic society. *Example:* An example could be taken from diaspora communities. These are normally created online to provide support to members of a community living in another country and which if they would know they are constantly monitored would perhaps disband.		
Right to Data Protection Art.8 CFREU GDPR Art.8 ECHR	*Explanation:* This right provides for a framework within which personal data of individuals can be processed in a lawful and fair manner respecting the rights to private life and its enjoyment (discussed earlier in this table). It also provides individuals with a set of rights over the processing of their data. 'Personal data' are defined in the GDPR as any information relating to an identified or identifiable	Critical	Carry out a data protection impact assessment.[50] Follow the principles of data protection by design and data protection by default. Minimise processing of personal data.

[43] See Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services.
[44] See Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom and Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users.
[50] This will be done in the MIRROR project as part of Task 3.3.

	natural person ('data subject'). An identifiable natural person, on the other side, is the one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Actual identification is not needed to fall within the remit of the GDPR.[45] As long as the information related to an identified or identifiable person then the provisions protecting the right to data protection kick in. According to Recital 26 of the GDPR, the benchmark is whether it is likely that reasonable means for identification will be available and administered by the foreseeable users of the information; this includes information held by third-party recipients. Special categories of personal data which, by their nature, may pose a risk to the data subjects when processed and need enhanced protection are subject to a prohibition principle and there are a limited number of conditions under which such processing is lawful. The following categories are considered sensitive data: • personal data revealing racial or ethnic origin; • personal data revealing political opinions, religious or other beliefs, including philosophical beliefs; • personal data revealing trade union membership;		

[45] [45] FRA, EDPS and Council of Europe (2018), p. 90

	• genetic data and biometric data processed for the purpose of identifying a person; • personal data concerning health, sexual life or sexual orientation. It is important that the processing of any of these categories of data is assessed to review the lawfulness of the processing. In MIRROR, while we may not be specifically processing such categories of data, information in other data can reveal elements of these data. For example, in the images being processed in WP5, there may be an image with a person with a headscarf that could lead to a revelation of that persons' religious beliefs or ethnic origin. 'Open source' data can also be personal data. The fact that personal information was posted in an open online environment does not automatically mean that this data can be processed without respecting the right to data protection.[46] Respect of this right includes that: • Data must be legitimate, necessary and proportionate; • Data must be processed for a specific purpose based on a specific legal basis; • Individuals must be informed when their personal data is processed; • Processing must comply with the requirements of data minimisation, data		

[46] Bert-Jaap Koops, Jaap-Henk Hoepman, Ronald Leenes, Open-source intelligence and privacy by design Computer Law & Security Review, Volume 29, Issue 6, 2013, Pages 676-688, https://doi.org/10.1016/j.clsr.2013.09.005.

	accuracy, storage limitation, data security and accountability; and • Unlawful data processing must be detected and prevented. Data Minimisation is a complex principle to achieve when creating algorithmic profiles. The challenge is to find a way how to use as much data as necessary to ensure accuracy of the profiling and AI analysis, then run through the data and discard unnecessary personal data to show only relevant data, while somehow keeping an audit trail of all the processing. In addition, individuals have specific rights described in detail in the provisions of the GDPR: • the right to be informed, including to receive meaningful information on the logic involved in an algorithm if one was used in the processing of the data; • the right to access their personal data, • the right to lodge a complaint with a supervisory authority; and • the right to an effective judicial remedy. Furthermore, the GDPR has introduced two important provisions aimed at embedding the respect of the right to data protection in any technical development involving the processing of personal data from the very design stage of the process. These principles referred to as 'Data protection by design' and 'Data protection by default' are regulated by Article 25 of the GDPR.		

	Data protection by design aims to ensure that, both before and during the processing of data, technical and organisational measures are implemented to guarantee data protection principles. For instance, where feasible, personal data could be 'pseudonymised'. Pseudonymisation is a measure by which personal data cannot be linked to an individual without additional information, which is kept separately. The 'key' that enables re-identification of the individual must be kept separate and secure.[47] Contrary to anonymised data, pseudonymised data are still personal data, and therefore must respect data protection rules and principles. Data protection by default ensures that "only personal data which are necessary for each specific purpose of the processing are processed".[48] This has an impact on: • the amount of personal data collected and stored; • the types of processing that may involve personal data; • the maximum storage period; and • the number of persons authorised to access such personal data. *Examples*: The world may be growingly moving towards face recognition and AI-based systems designed for border use. These would notionally include a "black list" or "hit list" against which		

[47] FRA, EDPS and Council of Europe (2018), p. 83.
[48] General Data Protection Regulation (GDPR), Art. 25

	passing travellers would be checked. The quality of the data contained on that list, the application of data minimisation techniques when using OSINT to enhance or triangulate a list are all factors to consider. Related likely design considerations include: i) The frequency with which the list is checked, (once a week, once a month or once a quarter?) and the creation of flags to remind users of the need for the periodic checking or ii) that it is overdue and that the data may therefore be less reliable; iii) the use of "internal externals" in carrying out those frequent "clean-up" checks and internal audits; iv) the establishment of criteria for ensuring that marginal suspects are left out of the list through double and triple triangulation requirements; v) the establishment of procedural requirements for challenging the decision given by such a system; and vi) the security and authorisation measures taken to ensure controlled and limited access to the data. *Questions for Reflection:*[49] 1. What type of personal data are you processing? a. Are you processing content data? b. Are you processing metadata?		

[49] These questions were developed in deliverable 3.1 at the start of the MIRROR project. However, these are not questions that are meant to be answered once only: they should be answered in the case of every technical process/development processing personal data in the life-cycle of the project.

	c. Are you processing sensitive data? (e.g. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation of a natural person) 2. Are you collecting these personal data directly from the data subject? 3. In case you are not collecting data directly from the data subject, which sources are you using for collecting these data? 4. In case you are collecting data directly from the data subject, are you informing them on the purposes of processing their data? a. How do you inform data subjects about the collection of their data? b. Are you informing the data subject on their rights in accordance with the GDPR (e.g., access, erasure, rectification)? 5. Does the collection of personal data include data that are not necessary for the purpose of your data processing? a. What kind of measures have you introduced to avoid collection of data that are not necessary for the purpose of your data processing activity?		

	b. What happens to personal data that are collected but are not necessary for the purpose of data processing? 6. The purpose of this question is for us to understand the jurisdictions from which personal data are collected and processed. a. Are you processing personal data of data subjects located in third countries (only)? i. If yes, from which countries? b. Are you processing also personal data of data subjects located in the EU? c. Can the MIRROR system identify if certain personal data (including metadata) are coming from individuals located in certain geographical areas? d. Is it possible to distinguish data from different locations (e.g. using geographic delimiters at the moment of data collection) for complying with specific third countries national rules? e. Is it possible to distinguish personal data originating from visitors, expats, etc.? f. Is it possible to distinguish between data originating from potential migrants and data originating from individuals that are neither thinking nor ever going to migrate? g. Are you processing personal data based on the nationality of the data subject?		

	7. Are the personal data you are processing pseudonymized/anonymized/encrypted? 8. Do you process personal data for individual or for group profiling? 9. Is the identification of the data subject necessary for the purpose of your data processing? 10. Is information identifying the data subject processed? 11. We would like to understand if there is a risk to still identify an individual even if the data are anonymized - for example by creating a mosaic effect (connecting different databases). a. If so, which databases are connected? 12. What is the time span of data collection? a. How far back in time are you going for collecting personal data? b. For how long do you retain the personal data? 13. What happens to the personal data you have collected once they are not needed anymore for the purpose of data processing? As pointed out earlier in the explanation when discussing data minimisation, the answer to this question is key when designing the algorithms since it should be assumed that before a human user would see any “product” coming from an AI-based system, the system would have run		

	through and discarded a lot of personal data and only show up the relevant data, while somehow keeping an audit trail of all the processing. 14. What happens to the results of data processing once they are not needed anymore? 15. Who has access to the personal data collected and/or to the results of processing and are these data/results shared with other partners or third parties? 16. What security measures have you adopted with regards to the retention of personal data? 17. Are you keeping any records on data processing activities? 18. Does the processing of personal data include any automated decision-making process which produces legal effects regarding the data subject? 19. Can the MIRROR system distinguish between reliable and non-reliable data? 20. Can the MIRROR system identify the context/origin/intent in which a social media post was published? 21. Is it possible that the system presents erroneous results?		

	a. Is it possible to identify erroneous results of data processing? b. Is it possible to remedy erroneous results?		
Right to understand the basis of an automated decision again him or her Art.13(2)(f) GDPR Art. 14(2)(g) GDPR and related to Art. 22 GPDR	*Explanation:* This is not a right found in the Charter of Fundamental Rights of the European Union or the European Convention of Human Rights. It is a right that has been included in the General Data Protection Regulation. Not being in the Charter or the Convention does not diminish its importance and relevance for our reflections. However, it is important to note that it has another source for its existence and it is still in the early stages of development as a 'right'. Increasingly, decisions at the border are based on the results of different automated processes and analysis. Given the differences in reliability of the different automated processes, the legislator in the General Data Protection Regulation gives the right to data subjects not to be subject to a decision based solely on automated processing including profiling especially if this decision produces legal effects concerning or affecting the data subject.[51] In cases where a decision is an automated one the legislator requires that meaningful information about the logic involved in the automated decision as well as its significance and envisaged consequences of such processing should be made available or explained to the data subject.[52]	Critical	

[51] Art. 22 GDPR
[52] Art.13(2)(f) GDPR and Art. 14(2)(g) GDPR.

	Example: An example could be of a portal for refugees from a particular country set up to help families reunite. The refugee fills in an online form applying for visa services. Their data is checked again EU records (found in the several EU large-scale data bases[53]) and the visa is granted or refused based solely on the analytical process carried out by the system supporting the visa application portal.[54] *Questions for reflection:* Will a decision having legal effects on a data subject be based on any of the tools in MIRROR?		
Rights to a fair trial and due process Art.6 ECHR	*Explanation:* One of the important principles in the right to a fair trial is that all parties to assist criminal process should have, what is called, equality of arms. This means that all parties in the legal process should be in a position to understand the facts and evidence presented in the legal process and to question those facts. When information is presented and this results from an analytical process that is carried out by a machine, it is important that this process is clear to any person working with this information and also the origins and contents of the dataset used should be clear. This is often referred to as being transparent. Unless there is transparency of the analytical	Critical/ Moderate	Ensure the explainability of the dataset used and of the analytical process/algorithm. Key principles: transparency accountability risk assessment

[53] See table 6 in Fundamental Rights Agency (2018) Preventing unlawful profiling today and in the future: a guide - https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf at pg 113

[54] A similar example can be found at https://www.accenture.com/t20170214T094928__w__/us-en/_acnmedia/Accenture/cchange/border-services-report/Accenture-Emerging-Technology-Border-Service-Report.pdf at pg10.

	process and of the dataset the full enjoyment of the rights to a fair trial may be impacted. *Example:* following a string of racial hatred-initiated attacks in the US and Europe, there is considerable discussion on how algorithms can be used to identify social media accounts that generate extremist or racial hatred content. If the results of these algorithms were to be used as evidence in court one would need to consider the reliability of the results of these algorithms, the explainability of the results obtained and the original dataset used to train the system. Failure to be able to explain the information in court could lead to a person being unfairly convicted and fundamental rights impacted. *Questions for reflection:* Can the information obtained from this tool be used as evidence in a criminal law process? Can the analysis leading to the information be explained?		

3. Conclusion

This document set off to produce a *Human Rights Implications Checklist* to be used by the technical partners in the MIRROR project. While it is evident that the different technological experiments being developed in Europe and elsewhere to strengthen border control and manage migration have profound human rights ramifications, the discussion on human rights implications is rarely carried out at the time they are being designed and developed by the technical experts. Often (at least as seen in literature) a discussion takes place later when some of the experiments would have already been transformed into practice. Human rights implications discussions seem to be the remit primarily of human rights agencies, civil society and a few victims of alleged violations that eventually make it to the European Court of Human Rights or the Court of Justice of the European Union. While this later discussion is also important and should be encouraged and maintained, it is increasingly evident that the discussion about human rights should first take place at design stage. The MIRROR project is attempting to do this: encouraging awareness of human rights responsibilities and an understanding that there may still be opportunities to opt for methods, solutions and selection criteria for data in data sets that are more human rights friendly than the initial proposed solutions.

The *Human Rights Implications Checklist* is not meant to be a stand-alone document independent of the MIRROR project and hence does not give an encyclopaedic description of the pertinent fundamental rights. Instead, it provides basic knowledge on fundamental rights accompanied by examples and questions for further reflection. It is meant as a tool to initiate and support discussions within the project between the technical teams and the legal team on the human rights implications of the tools being developed.

What we intend to continue doing in the project, now aided by this *Human Rights Implications Checklist,* is to discuss with colleagues in work packages 4, 5, 6,and 7 their reflections on the questions set for each particular fundamental right, in order to continue to work together to find ways how to mitigate the human rights impact of the MIRROR tools while still keeping in mind the needs, aims and responsibilities of border agencies as end-users of these tools.

Bibliography

Legislation

European Convention of Human Rights, 4 November 1950 found at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005

Charter of Fundamental Rights of the European Union OJ C 326, 26.10.2012, p. 391–407 found at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN

Explanations relating to the Charter of Fundament Rights OJ C303,12.2007, p.14 found at https://fra.europa.eu/en/eu-charter/article/1-human-dignity

The Vienna Convention on Road traffic , 8 November 1968 found at https://treaties.un.org/Pages/ViewDetailsIII.aspx?src=TREATY&mtdsg_no=XI-B-19&chapter=11

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)

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119 (Police Directive)

Council of Europe Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services.

Council of Europe Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom and Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users.

Books and articles

Accenture (2017) Crossing Boundaries: Emerging Technologies at the border available at https://www.accenture.com/t20170214T094928__w__/us-en/_acnmedia/Accenture/cchange/border-services-report/Accenture-Emerging-Technology-Border-Service-Report.pdf

American Civil Liberties Union (ACLU) (2016), Eight Problems With Police “Threat Scores”, 13 January 2016 available at https://www.aclu.org/blog/privacy-technology/surveillance-technologies/eight-problems-police-threat-scores

Paolo G. Carozza, 'Human Dignity’, in 'The Oxford Handbook of International Human Rights Law' (Dinah Shelton, ed. 2013) (First edition), Oxford University Press, available at https://www-

oxfordhandbooks-com.proxy-ub.rug.nl/view/10.1093/law/9780199640133.001.0001/law-9780199640133-e-15

Council of Europe (2018) Algorithms and Human Rights Study on the human rights dimensions of automated data processing techniques and possible regulatory implications. https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5

The Danish Institute for Human Rights (2016) Human Rights Impact Assessment: Guidance and Toolbox found at https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria_toolbox/hria_guidance_and_toolbox_final_jan2016.pdf

Edward J. Eberle, 'Observations on the Development of Human Dignity and Personality in German Constitutional Law: An Overview', Liverpool Law Review, November 2012, Volume 33, Issue 3, pp 201–233 available at <https://link.springer.com/article/10.1007/s10991-012-9120-x>.

Evelyn Ellis and Philippa Watson, *EU Anti-Discrimination Law* (Oxford University Press) 142.

Fundamental Rights Agency (2018) Preventing unlawful profiling today and in the future: a guide - https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf

EU-LISA (2015) Testing the borders of the future: Smart Borders Pilot: The results in brief accessed at https://www.eulisa.europa.eu/Publications/Reports/Smart%20Borders%20-%20The%20results%20in%20brief.pdf

European Migration Network (2012) Practical Measures to Reduce Irregular Migration available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/european_migration_network/reports/docs/emn-studies/irregular-migration/00a_emn_synthesis_report_irregular_migration_october_2012_en.pdf

Fundamental Rights Agency, Council of Europe and EDPS (2018), Handbook on European data protection law. 2018 edition, Luxembourg, Publications Office, June 2018

Fundamental Rights Agency (2018) Handbook on European non-discrimination law found at https://fra.europa.eu/en/publication/2018/handbook-european-non-discrimination-law-2018-edition

Fundamental Rights Agency (2020) Practical guidance issued by the fundamental rights agency addressing border management stuff in the European Union member states work at the operational level. This is found at https://fra.europa.eu/en/publication/2020/border-controls-and-fundamental-rights-external-land-borders

Fundamental Rights Agency and Council of Europe (2020) Fundamental rights of refugees, asylum applicants and migrants at the European borders. Available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-2020-european-law-land-borders_en.pdf

Mireille Hildebrandt (2019) Law for Computer Scientists accessed at https://lawforcomputerscientists.pubpub.org/pub/doreuiyy/release/7

Martina Kant (2006) Nothing doing? Taking stock of data trawling operations in Germany after 11 September 2001 available at https://www.statewatch.org/media/documents/news/2006/aug/profil.pdf

Bert-Jaap Koops, Jaap-Henk Hoepman, Ronald Leenes, Open-source intelligence and privacy by design Computer Law & Security Review, Volume 29, Issue 6, 2013, Pages 676-688, https://doi.org/10.1016/j.clsr.2013.09.005.

Open Society Justice Initiative (2009) Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory available at https://www.justiceinitiative.org/uploads/8cef0d30-2833-40fd-b80b-9efb17c6de41/profiling_20090526.pdf

Shannon Vallor and Arvind Naranyanan An Introduction to Software Engineering Ethics, last accessed on 26th July 2020 at https://www.scu.edu/media/ethics-center/technology-ethics/Students.pdf

Watts L., Hodgson D. (2019) Human Rights and Autonomy. In: Social Justice Theory and Practice for Social Work. Springer, Singapore
Unboxing Artificial Intelligence: 10 steps to protect Human Rights available at https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-%20protect-human-rights-reco/1680946e64

UN OHCHR, Human Rights and Law Enforcement: A Manual on Human Rights Training for the Police produced by UN OHCHR (Office of the High Commissioner of Human Rights) available at https://www.ohchr.org/Documents/Publications/training5en.pdf

UN Office of the United Nations High Commissioner for Human Rights (2012), The Corporate Responsibility to Respect Human Rights: An Interpretive Guide, New York and Geneva: United Nations.

UN Guiding Principles 12 and 24 and commentaries; Office of the United Nations High Commissioner for Human Rights (2012), The Corporate Responsibility to Respect Human Rights: An Interpretive Guide, New York and Geneva: United Nations.

Websites

https://edri.org/the-human-rights-impacts-of-migration-control-technologies/

https://www.humanrightscareers.com/issues/definitions-what-is-human-dignity/

The Conversation, “We should teach human rights law to software engineers” 25 December 2018, last accessed on 26th July 2020 at https://thenextweb.com/syndication/2018/12/25/we-should-teach-human-rights-law-to-software-engineers/

https://migrationdataportal.org/regional-data-overview/europe

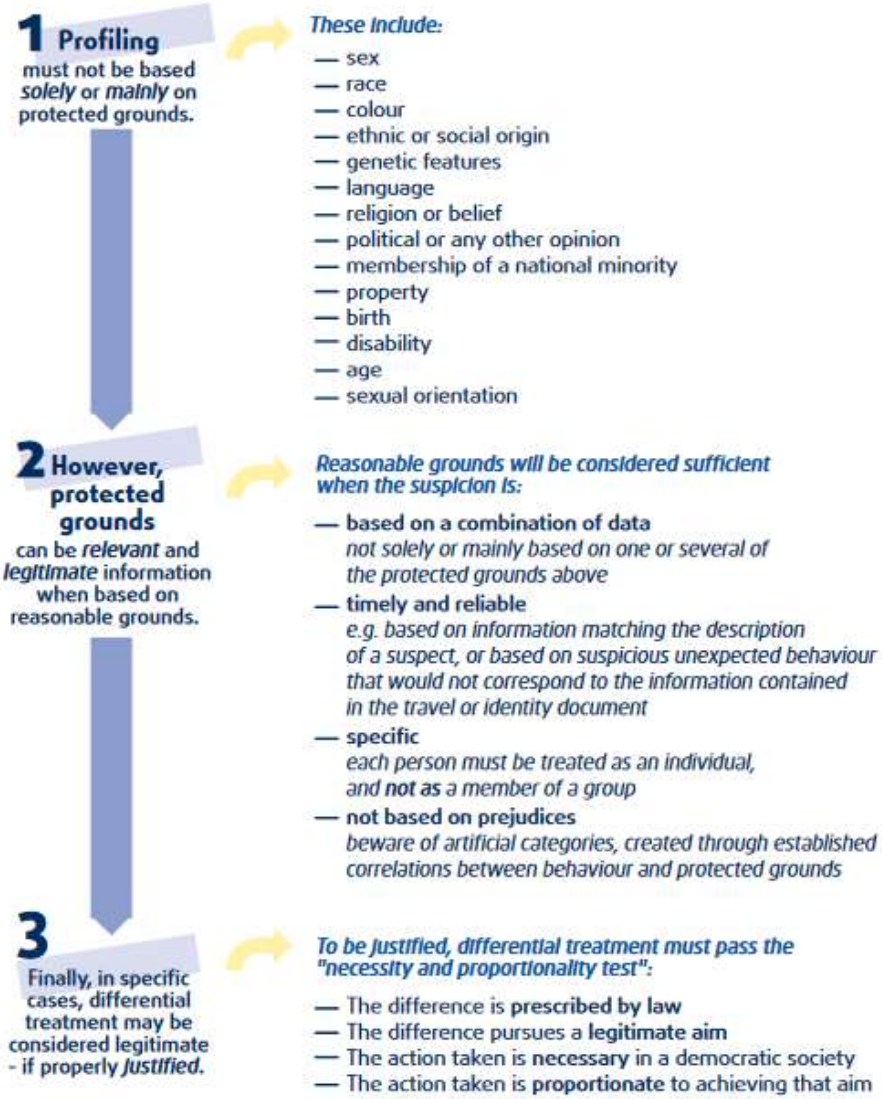
https://www.militaryaerospace.com/unmanned/article/16707261/the-role-of-technology-in-securing-the-nations-borders

Displacement Tracking Matrix developed by the UN IOM available at https://dtm.iom.int/

Appendix 1

Table developed by the Fundamental Rights Agency on non-discriminatory profiling.[55]

Figure 9: Elements of non-discriminatory profiling



Notes: *The list of protected grounds varies across Member States. For an overview of the grounds of discrimination that are included in the criminal codes of each and every Member State, see FRA (2018d). See also the website of Equinet, the European Network of Equality Bodies, which lists the grounds of discrimination covered by national equality bodies.*

Source: *FRA, 2018*

[55] Fundamental Rights Agency (2018) Preventing unlawful profiling today and in the future: a guide - https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-preventing-unlawful-profiling-guide_en.pdf