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 against, 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 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 used 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	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

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	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 creditworthiness and/or movement/travel information thus also catching non-offenders in the search net.[1] Furthermore, the use of these criteria may impact the analysis of the perceptions that the MIRROR project is trying to produce. Would a perception reached on one or more of the above criteria correctly represent the perception of a wider group which may be effectively more heterogeneous than 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 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 concerning that natural person's performance at work, economic		

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

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	situation, health, personal preferences, interests, reliability, behaviour, location or movements. 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 raise a number of fundamental rights concerns. Avoiding discrimination is central to these concerns together with risks in relation to the rights to privacy and data protection. 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 be 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		

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	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 a 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. The 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.' 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. Beware software (USA) - '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 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.		

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	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:*[2] This right protects persons from 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 'necessary in a democratic society' if the interference with the private sphere of the individuals is counterbalanced by adequate guarantees against abuse. 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	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.

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

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	religion, freedom of expression and information, and freedom of assembly and of association. 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 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 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 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.		

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	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. The same reasoning would apply also for the MIRROR research since individuals using social media and the 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 is 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 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 Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
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 limitations 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. The impact on the right of freedom of expression can be either direct or indirect. A direct impact 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?	Major	

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
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 participation of individuals in political, social and cultural life. 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. 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 if they would know they are constantly monitored would perhaps disband.	Major	
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 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.	Critical	Carry out a data protection impact assessment.[3] Follow the principles of data protection by design and data protection by default. Minimise processing of personal data.

[3] This will be done in the MIRROR project as part of Task 3.3.

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	Actual identification is not needed to fall within the remit of the GDPR. As long as the information is 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 that, 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; • 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 person's 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.		

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	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 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 the 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		

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	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. 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. 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 passing travellers would be checked. The quality of the data contained on that list, and 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;		

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	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:* 1. What type of personal data are you processing? a. Are you processing content data? b. Are you processing metadata? 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 the collection of data that are not necessary for the purpose of your data processing activity?		

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	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 the 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?		

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	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?		

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	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 analyses. Given the differences in the 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. 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	Critical	

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	significance and envisaged consequences of such processing should be made available or explained to the data subject. *Example:* An example could be 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) and the visa is granted or refused based solely on the analytical process carried out by the system supporting the visa application portal. *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 in the analytical 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	Critical/ Moderate	Ensure the explainability of the dataset used and of the analytical process/algorithm. Key principles: transparency accountability risk assessment

Right Impacted	Explanation, Example(s) & Questions for reflection	Severity	Possible mitigation
	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?		