Many people use **facial recognition** technology daily to access their cell phones and other devices that have this option.

However, facial recognition is not always limited to personal use, which raises complex ethical dilemmas.

This way, facial recognition technology is configured as a biometric security category with the individual's face as an identification source.

Although it is widely used, the technology still has flaws, which will be addressed throughout the text.

FAULTS IN THE RECOGNITION SYSTEM

Face recognition is far from perfect, as the recognition technology setup is not always equally accurate for all types of faces.

For example, some recognition technologies may not be able to identify the race or gender of individuals correctly.

This inaccuracy causes flaws in **personal identification**.

Furthermore, it is very easy for recognition to misinterpret nuanced facial expressions.

For example, an expression that conveys a polite greeting in one culture might indicate confirmation or agreement in another.

In this sense, the reliability of the recognition technology must be tested before deciding to make it operational so that, for example, similarity errors do not occur.

In addition to assessing the possibility of errors in the execution of the recognition system, it is necessary to analyze the rights connected to the use of technology.

THE RIGHTS OF PEOPLE IDENTIFIED IN THE IMAGES

Protecting facial recognition data is a point of disagreement in many jurisdictions, as governments often perceive it as an invasion of privacy.

Data and analytics leaders need to ask these important questions:

- Who owns the image of your face?
- Who owns the image of the expressions you make in public?
- Who can manipulate this information?
- What are the **limits of the use** of this technology?

On the one hand, facial expressions made in a public place are potentially available for everyone present to see, so they're not entirely private.

On the other hand, facial expressions are often made subconsciously and are transient.

In that sense, they simply should not be systematically captured, stored, and analyzed.

Companies and governments using recognition technology need to work with their legal teams to understand the intellectual property rights relevant to face recognition images and analytics.

In this sense, the analysis of these rights must take place from the perspective of the rights of the people portrayed.

In addition, the evaluation may occur based on the purpose, that is, the purpose of using the recognition system.

RESTRICTION OF DATA FROM THE PURPOSE OF USE

Firstly, the collected data must be processed for specific, deliberate, and predefined purposes.

For example, face recognition results used outside a parking lot to open barriers and facilitate quick entry and exit of vehicles could also be used by car dealerships as business leads.

However, this data sharing can cause problems as parking lot users have not agreed to share recognition data to facilitate business for car retailers.

In this sense, for any data collected via face recognition technology, it is essential that the lineage of intentions to use the image be explicitly determined in the document and the due restriction of use and only for this predefined purpose.

In conclusion, these are the main notions about **facial recognition technology**. Keep following our blog and follow our Instagram for more content.