REPORT

Biometrics: the urge to safeguard fundamental rights

We are all equal before the law

Défenseurdesdroits

RÉPUBLIQUE FRANÇAISE

REPORT

Biometrics:
the urge to safeguard fundamental rights

OPENING REMARKS

In recent years, the deployment of biometric devices has accelerated significantly in France and throughout Europe. Present in both the public and private sectors, these technologies are now used in fields as varied as recruitment and human resources management, access to goods and services, security, and even education. This multiplication of uses is closely linked to the latest advances of machine learning algorithms, on which these technologies are widely based and whose computing power now allows for massive uses of large datasets, promising optimisation and efficiency gains.

Ranging from the simple unlocking of a smartphone to the alleged analysis of the emotions of a job candidate, what all these technologies have in common is that they process biometric data, such as the facial features, voice or behavioural characteristics of individuals, in order to authenticate, identify or evaluate them. It is now possible to carry out a transaction with the palm of your hand, to automatically identify a suspect in a crowd, or even to offer targeted advertising to an individual based on their physical appearance.

Even though these technologies may offer certain advantages, they are particularly intrusive and involve a number of risks for the protection of personal data and privacy, something which the ***Commission Nationale de l'Informatique et des Libertés*** (CNIL – French Data Protection Authority) has found several times.[1]

Beyond data protection and privacy, the risks must also be assessed from the outset of their impact on the fundamental rights protected by the Defender of Rights (***Défenseur des droits***) in all of its areas of expertise: equality and non-discrimination, respect for ethics by those carrying out security activities, protection of children's rights, and access to rights and public services.

In May 2020, the Defender of Rights together with the CNIL called for a collective effort to address the discriminatory biases of algorithms, to denounce the considerable risks of discrimination that can burden each and every one of us with the exponential use of these algorithms in all spheres of our social lives and to strengthen the applicable legal framework.[2] Since the consequences of these biases are particularly acute with regard to biometrics, it appeared essential to further this reflection in order to anticipate future complaints and to call on both public authorities and users of the private sector to do more to question the consequences for rights and freedoms arising from the deployment of biometric technologies.

At a time when proposals to strengthen the framework of these technologies are being studied both at the European level and in France, the Defender of Rights wishes to present a list of recommendations which it considers essential to ensure that the rights of individuals are respected beyond the sole and necessary protection of personal data.

BIOMETRIC TECHNOLOGIES: A GENERIC TERM ENCOMPASSING A PLURALITY OF USES

Biometric technologies consist of computer techniques for physical, biological or behavioural recognition and/or assessment of individuals[3] all of which stem from the same process: the biometric characteristics are processed according to standardised procedures and the result of this processing operation is stored in data records called signatures, models or templates. These concentrate the unique physical characteristics of people in digital form allowing them to be singled out.[4]

In France, the first uses of biometric technologies date back to the beginning of the 20th century. In 1902, the police began collecting the fingerprints of those suspected of having committed a crime,[5] and, for a long time, these technologies were confined to a few well-defined use cases such as the establishment of a passport respecting certain security standards.

As a result of scientific advances in the field of machine learning algorithms, these uses have now multiplied. **Facial and voice recognition, emotion analysis, the uses of our biometric data are now numerous**.

There are currently three types of biometric systems: authentication systems, identification systems and assessment systems.

AUTHENTICATION: DETERMINING WHETHER A PERSON IS WHO THEY SAY THEY ARE

Authentication consists of verifying the identity claimed by someone by comparing the biometric data of a person at a specific moment with that of the verified identity being claimed.[6]

The facial recognition unlocking function on a smartphone where the user's photograph is compared to the one previously recorded on the device during set-up,[7] or the European border crossing control system PARAFE,[8] in which the templates stored in the biometric passports of travellers are compared to those produced by dedicated detectors,[9] fall under the authentication objective.

In practice, biometric authentication technologies make it possible to compare a person's templates stored on a secure medium (a badge, passport or telephone) with the body part or with a characteristic of the body of this alleged same person (facial features, fingertips, iris, hand shape, voice sample, etc.) to determine if there is indeed a match between the two.

These systems can be used to secure physical access to a building, make payments, cross a border, etc. In terms of privacy, their advantage is that they generally remain under the exclusive control of the individuals and their proper functioning does not require the use of a centralised database. To use the aforementioned examples, when setting up the unlocking function of a phone or creating a biometric passport, the templates containing the important features of the face (distance between the eyes, shape of the chin) are encrypted and then stored locally on the phone, or on the chip implanted in the passport. In fact, people are generally free to choose whether or not to use authentication devices.

IDENTIFICATION: FINDING SOMEBODY IN A CROWD

Identification aims to find a person within a group of individuals, in a place, in an image,[10] or in a database constructed in particular using facial features (facial recognition),[11] voice (speaker recognition),[12] behaviour (gait recognition)[13] or any other type of biometric data.

Like certain facial recognition technologies, an identification system makes it possible to perform the following operation: the template drawn from the features of a person's face is compared by means of an algorithm with a plurality of other templates stored in a database in order to determine the person's identity. This same approach applies to templates extracted from other parts of the body depending on the type of biometric identification technology considered. In other words, identification technologies compare the biometric data of people filmed, photographed or recorded with a list of wanted individuals.

The most recent identification techniques are special in that they can potentially be applied to an unlimited number of individuals without them even being aware of it. The European Commission has looked into these remote biometric identification systems:[14] they can operate both "in real time" using data collected and analysed instantly, and after the event using images taken from CCTV cameras or other pre-existing data. Regardless of the technology, processes or types of biometric data used, **identification involves the collection of sensitive data[15] sometimes on an extremely large scale, without knowing beforehand whether the person sought will be among those examined.**[16]

To date, uses of biometric remote identification technologies have been identified in Europe mainly in the field of security, for example in the context of the surveillance of public spaces during events,[17] during criminal investigations,[18] for police purposes[19] or when tackling illegal immigration.[20]

ASSESSMENT: INFERRING AN INDIVIDUAL'S PERSONALITY TRAITS AND CATEGORISING PEOPLE BASED ON THEIR BIOMETRIC CHARACTERISTICS

In addition to authentication and identification systems, there is a third, more recent category, which we refer to here as assessment systems.

Based on the biometric data of one or more individuals, assessment technologies aim to perform two major actions:

- Identify or infer emotions, personality traits or intentions (known as "emotion recognition" systems);[21]
- Put the individual(s) in question into specific categories, such as gender, age, hair colour, eye colour, ethnicity, or sexual or political orientation, with a view to taking specific measures (known as "categorisation" systems[22]).

Today, some companies claim, for example, to be able to use biometric data to automatically analyse and measure the nervousness of a candidate in the context of a recruitment procedure.[23] Other systems promise to measure a student's concentration,[24] the tiredness of a motorist,[25] the dangerousness or propensity of a person to commit an offence in a given environment,[26] or the reactions of a consumer to the presentation of goods or services in order to offer them targeted advertising.[27] Finally, some offer to profile individuals according to their apparent physical characteristics in order to restrict access to the goods and services they offer to a specific audience.[28]

The scientific basis of these technologies has received strong criticism from the scientific community, **in particular when it comes to the detection of emotions or affect recognition technologies**. Many experts are calling for tight control of their uses.[29]

The existing scientific literature shows that these technologies are very biased and make a lot of mistakes.[30] For researchers, detecting a person's emotions accurately and reliably would depend on a context beyond their face and body.[31]

Voice samples or onomatopoeias[32] like facial movements[33] would not be sufficient to characterise human emotions, and even less to rigorously assess the future performance of a job candidate. However, these systems are regularly presented to human resources departments as particularly efficient when in reality they are very poorly correlated with work efficiency, as evidenced by the case of personality tests.[34] The risks of discrimination or infringements of fundamental rights linked to their use in the field of employment, as in other fields, must be better known and emphasised more clearly.

In principle, the processing of biometric data for assessment purposes does not fall under Article 9 of the General Data Protection Regulation (hereinafter GDPR) and therefore does not constitute processing of "special categories" of personal data. While such an interpretation has not yet been stabilised, the Defender of Rights recommends that these assessment methods be the subject of specific protection measures since they involve the same type of data as processing for identification purposes and their uses are equally risky. Furthermore, biometric assessment systems can be combined with identification systems.

SIGNIFICANT RISKS OF FUNDAMENTAL RIGHTS VIOLATIONS

While some biometric systems offer undeniable advantages in the fight against crime, to guarantee public safety or in other circumstances where secure and reliable identification of persons is necessary, these technologies should by no means be considered as entirely harmless.

The operation of these systems is based on the processing of particularly sensitive data, which could infringe the right to privacy as well as the right to data protection.

Whether authenticating, identifying or assessing individuals, these systems are inherently probabilistic (they can only estimate a "percentage" match or risk) and the reliability of their results could not therefore be considered as absolute. Thus, not only can the algorithms on which they are based include discriminatory biases from the very design stage, but they can also generate allocation or selection errors, with particularly serious consequences for the affected individuals.

Finally, certain uses, in particular in matters of identification and assessment, can generate a chilling effect in the exercise of certain fundamental rights (freedom of expression, freedom of movement, freedom of assembly, freedom of association, and, more broadly, freedom in access to rights).

AN INHERENT RISK OF INFRINGEMENT OF THE RIGHT TO PRIVACY AND DATA PROTECTION

Enshrined in the European Convention on Human Rights (ECHR)[35] as well as in the Charter of Fundamental Rights of the European Union,[36] the right to respect for private and family life and the right to the protection of personal data aim to protect the autonomy and dignity of individuals,[37] by protecting them from any unjustified interference with their private sphere. The use of biometric technologies involves the collection, comparison and/or recording of so-called sensitive data in a computer system for the purposes of authentication, identification or assessment. It therefore constitutes an interference with the free exercise of those rights.

Indeed, as ruled by the Court of Justice of the European Union (CJEU), "*the image of a person recorded by a camera constitutes personal data [...] inasmuch as it makes it possible to identify the person concerned*".[38] Likewise, the recording of a person's voice necessarily contains personal data. As the CNIL explains in its White Paper on voice assistants, "*voice contains markers specific to an individual, a combination of physiological and behavioural factors. This is what makes it a biometric attribute in its own right, which can be used to identify the individual*".[39] In fact, biometric technologies process personal data.

To be authorised, in France these must comply with the main principles and strict conditions provided for by the General Data Protection Regulation (hereinafter GDPR)[40] and the French Data Protection Act.[41] Among the main principles of these laws is the ban on processing data, which now includes biometric data under the French Data Protection Act, but only when it is processed for the purpose of uniquely identifying individuals.[42] Such processing may only be implemented, by way of exception, in certain specific cases, including with the explicit consent of individuals, to protect their vital interests or on the basis of a substantial public interest.[43] Similarly, this type of processing can only be authorised in cases of strict necessity when it is implemented for police purposes, by virtue of provisions resulting from the "Law enforcement" directive.[44]

As highlighted by the CNIL, the processing of biometric data is never completely harmless.[45] It can seriously infringe the right to respect for privacy and family life, as well as the right to data protection. Widely documented by the various European data protection authorities and bodies,[46] these risks are to be assessed *in concreto*, on a case-by-case basis, taking into account the purposes of each processing operation. Taking the example of facial recognition technologies, it is indeed necessary to assess the "*degree of control individuals have over their personal data, the scope for initiative they have in using this technology, the consequences for them (in the event of recognition or non-recognition) and the extent of the processing implemented*"[47] for each biometric technology.

It is therefore necessary to distinguish so-called active technologies, where the individual voluntarily provides information (for example, by placing a finger on a control device), from passive technologies, where biometric information is detected, sometimes without the knowledge or consent of the data subject. The use of active biometric authentication technologies storing the templates in an individual medium freely available to people (smart card, smartphone, etc.) does not raise the same issues as that of passive biometric technology storing the templates that it processes in a central database, in particular when this use aims to identify individuals and takes place without their knowledge and without having previously obtained their consent.

The endless development and deployment of surveillance and video protection technologies in publicly accessible spaces, on public transport, in the common areas of social landlords and in shops, through the deployment of body worn cameras and drones, is accompanied in law by a significant easing of the conditions of transmission to law enforcement services of the images recorded by multiple actors as well as the interoperability and the interconnection of numerous files. This phenomenon carries significant risks for the respect of privacy, as the Defender of Rights underlined in its opinion no. 20-13 of 21 December 2020.[48] However, the last few years have seen a worldwide rise in passive biometric technologies used for identification purposes. This development is widely criticized and challenged by many civil society organisations. It is part of a larger movement, denounced by the Defender of Rights already in 2015, of too easy reco urse to technology despite the risks to civil liberties.[50] In Russia, automated facial recognition devices have been deployed in public spaces to monitor compliance with health measures and combat the spread of the COVID-19 pandemic.[51] In the United Kingdom, there was talk of deploying this same type of technology to verify the vaccination status of individuals by combining a facial recognition device and a covid passport, a project that was finally abandoned following the mobilisations of civil society.[52] Two American and Polish companies have built up large-scale biometric databases from photographs harvested from social network profiles around the world, access to which they sell to law enforcement services, private companies and sometimes even to individuals, allowing them to find the identity of a person at any time from a simple photograph.[53] One of them was sanctioned by

the Swedish[54] and Canadian[55] data protection authorities and is currently the subject of multiple administrative procedures, including in France.[56] In Italy, the data protection authority banned use of the "SARI" device, a real-time facial recognition tool deployed in public spaces to identify illegal aliens.[57]

While such uses are still at the experimental stage in France, parliamentary debates and the approach of the 2024 Paris Olympic Games show a desire to adopt this type of technology. The CNIL has already had cause to issue multiple warnings following the deployment of biometric identification technologies, sometimes carried out in defiance of essential data protection principles such as the principles of lawfulness[60] and proportionality.[61]

With regard to the right to respect for private and family life and the right to data protection, these practices are rightly alarming, in particular when these deployments are not surrounded by sufficient safeguards.

Indeed, the more biometric data processing based on the use of databases multiplies, the greater the potential for a security breach with particularly serious consequences for data subjects.[62] However, unlike a password, phone number or mailing address, unauthorised disclosure of biometric data cannot be corrected. This type of incident has already occurred.[63] These applications pose a threat to anonymity in the public space by allowing a form of generalised surveillance, insofar as they make it possible to instantly identify and track individuals – this risk was reiterated by the Defender of Rights in its opinion of 17 November 2020 on the draft law on global security.[64] These problems mainly arise when players disregard the applicable law. For example, private uses of biometric technologies are in principle prohibited unless they meet one of the exceptions under Article 9 of the GDPR. Too often, however, no form of consent is collected from individuals who are rarely informed of the fact that processing operations are taking place.

Finally, as raised by a report produced under the mandate of the UN Special Rapporteur on the promotion and protection of human rights while countering terrorism, technological developments, as well as the proliferation and increased dependence on various consumer technologies, have made interference with the exercise of the right to respect for private life both less perceptible to society and the persons concerned and, at the same time, more intrusive, with potentially significant consequences, often going beyond the right to respect for private life.[65]

UNPARALLELED POTENTIAL FOR AMPLIFYING AND AUTOMATING DISCRIMINATION

Because they tend to target the characteristics of individuals that expose them to discrimination (origin, sex, gender identity, physical appearance, state of health, disability, age, etc.), biometric technologies (beyond the margins of allocation errors which tend to decrease with the rapid improvement of systems) and their widespread use are likely to perpetuate or even amplify, for certain social groups, the systemic discrimination operating within society.

ERRORS AND BIAS WITH DISCRIMINATORY CONSEQUENCES

By definition, any biometric technology is probabilistic and is based on the use of algorithms with a certain rate of false positives and false negatives.[66]

A technology that recognises emotions displayed in a recruiting process may incorrectly determine that a candidate is "nervous" and assign them a rating that removes any chance of them being hired. Similarly, a voice recognition authentication device deployed to control access to an online bank account may make a mistake when verifying the identity of the person using the device. Finally, a facial recognition device used to identify those subject to a stadium ban may incorrectly determine that a supporter should not be attending a sports match.

The consequences of these errors vary according to the uses and can range from the refusal of physical access to a place or an event to an erroneous arrest by the police.[67]

By taking a close look at the profiles of people who are victims of these errors, many studies have shown since 2018 that they were mainly people from discriminated against and/or vulnerable groups (women, minors, transgender people, people with dark skin, etc.)[68] because of the discriminatory biases of the algorithms on which these technologies are based. As explained by the Defender of Rights in 2020, these biases may stem both from the lack of representativeness of the data used during the algorithm training phase[69] and from the integration, after mathematical translation, of discriminatory past practices and behaviours and of systemic discrimination operating within society.[70]

Significantly, whether for authentication, identification or assessment, when biometric technology is deployed in a space visited by millions of individuals such as an airport or a train station, even a very low rate of false positives and false negatives[71] means that hundreds of individuals fall victim to the errors of these systems and the consequences of such errors.[72]

Thus, although authentication systems, in particular facial recognition, can offer accuracy rates of up to 99.5%,[73] the remaining 0.5% may represent a multitude of individuals exposed to unfair treatment. Not all errors come from discriminatory biases. In this regard, the establishment of alternative routes may constitute a solution but it cannot justify the continued infringement of the principle of non-discrimination. Indeed, regardless of the alternatives proposed as in the framework of the Alicem system,[74] the discriminatory effects of algorithms cannot be ignored: **if the error rates remain high for certain categories of people protected under non-discrimination law, they will be wronged and will have to systematically use the alternative route (which, in fact, will no longer really be an alternative)**. However, taking into account the probabilistic nature of these systems,

they can hardly achieve a zero error rate: there will always be a tiny percentage of false positives and false negatives.[75] In order to avoid any discrimination, the error rate should be decorrelated from the protected categories. To do this, the non-representative datasets on which the authentication algorithms are trained may be the source of biases and therefore need to be corrected. In order to ensure greater reliability of facial recognition algorithms, which we have seen to be biased against women and dark-skinned people, the profiles and data should be more varied to reflect the diversity of the real population and ensure effective training of the algorithm on minority profiles.

Furthermore, a system that aims to authenticate an individual is not automatically a device achieving the best accuracy rates insofar as these depend on several factors (lighting, image quality, etc.). Even today, some authentication devices make many errors with discriminatory consequences that cannot be tolerated simply because their operation would be respectful of data protection law.[76]

However, the control that people maintain over authentication devices allows them to become aware of any errors that might arise: the person's identity verification did not work, they are immediately invited to repeat the test and/or to use an alternative route. This is not always the case when biometric technologies are used for both identification and assessment purposes.

When deployed in public places, biometric identification and assessment technologies do not allow people to oppose their use or to prefer an alternative route: the biometric data of each passer-by is processed in the same way. This is particularly the case with "real-time" facial recognition technologies deployed for the purposes of identifying wanted individuals. Yet, the accuracy of this type of system is significantly lower than that of authentication devices,[77] which is particularly worrying when they are used for law enforcement purposes. Indeed, in addition to the quality defects of the source of the images collected and compared, these errors often find their origins in discriminatory biases, since the training data used for facial recognition algorithms still suffers from a pronounced lack of representativeness.[78] For example, such uses may result in some people being wrongly arrested more frequently because of their skin colour.[79] In the United States, three black men have already been wrongfully imprisoned as a result of errors in facial recognition systems.[80] In the United Kingdom, a study on the use of facial recognition for identification purposes by the Metropolitan police services in London determined that out of 22 individuals arrested on the basis of a computer-generated match deemed credible by a human operator, fourteen of these matches (i.e. 63.64%) were found to be incorrect and only eight (i.e. 36.36%) were correct.[81] The use of this type of device by the British police services also gave rise to the first major court decision on the matter in 2020: the London Court of Appeal concluded that the police services were not sufficiently assured of the absence of discriminatory biases in the software used as to the ethnic origin or gender of the people it was intended to identify,[82] the risks of discrimination arising from the very use of biometric tools.

THE RISKS OF DISCRIMINATION ARISING FROM THE VERY USE OF BIOMETRIC TOOLS

The public debate on the accuracy of biometric technologies is important, in particular insofar as the biases of these systems can lead, as we have mentioned, to discriminatory situations, but it has for too long obscured another reality. Indeed, **even with an accuracy rate of around 100%, the use of biometric identification and assessment tools can generate discrimination. Worse still, it can amplify it**.

In a 2017 survey on relations between the police and citizens, the Defender of Rights noted that identity checks carried out in France particularly target certain territorial areas and give rise to strong discriminatory practices based on origin, suggesting racial and social profiling during checks of young men perceived as black or of Arab/North African descent. While more than 80% of the men surveyed declared that they had not been the subject of an identity check in the last 5 years, "80% of people corresponding to the profile of 'young man perceived as black or Arab' said that they had been checked in the last five years (compared with 16% for the rest of the respondents)". These profiles are therefore twenty times more likely to be checked.[83]

If in the future police services were able to carry out these checks using biometric identification and/or assessment devices coupled with remote verbalisation methods,[84] the risk of a concentrated deployment in geographical areas where young men perceived as Arab/North African or black are overrepresented could multiply discriminatory situations with spot checks of hundreds of individuals carried out because of their gender, origin, age and/or economic situation. These fears are not unfounded when one considers, on the one hand, the development of these technologies for security purposes (this is the case, for example, of the deployment in certain territories of surveillance drones during lockdown), and, on the other hand, the discriminatory targeting by certain police forces, which has already been the subject of court decisions and observations by the Defender of Rights who noted the climate of exclusion and discrimination that it could maintain.[85] As is currently the case in the field of traffic offences (in particular the parking of people with disabilities[86]), remote verbalisation may not take into account people's particular situations. In addition, the development of so-called "smart" cities enabled by the combining of video and identification and assessment technologies poses risks of discrimination: by identifying people who are homeless or begging, cities are able to dispatch appropriate social support to the places concerned, as well as to stigmatise and discriminate against these people in particularly vulnerable situations. While the European Commission has recently proposed banning in principle the use of remote identification devices on public roads for police purposes, many exceptions have been made leaving Member States free to decide whether or not to use this type of device, for example, when an offence is punishable by a sentence of at least three years' imprisonment.[87] Levels of trust in the police do not only depend on the check itself, but also on whether or not it is seen as racial profiling.[88] Thus, the use of biometric identification and/or assessment tools by the police could damage police/population relations if it is not surrounded by sufficient safeguards.

Since 2016, as part of the measures to tackle illegal immigration in Europe, the European Union has been funding a project called iBorderCtrl:[89] foreign travellers wishing to enter the European area must go through a "facial recognition lie detector", which channels them to either fast queues or enhanced checks depending on the results.[90]

This system has been tested at the EU land borders in Hungary, Latvia and Greece. Many civil society organisations have denounced a highly experimental technology, the results of which are unreliable and target people in particularly vulnerable situations.[91]

In general, the risk of seeing discrimination occur cannot be reduced to the law enforcement context. It also concerns uses in the private sector, in particular in terms of assessment. The use of devices to detect an individual's personality traits in the context of recruitment procedures for the purpose of analysing interviews and automatically assigning scores to different candidates based on their so-called personality is particularly telling.[92] These systems can generate significant discrimination, in particular for candidates with disabilities: if the characteristics of their faces or the way in which they stand and/or express themselves differ from the norm and therefore from the overwhelming majority of the data on which recruitment algorithms have been trained to assign scores, these people risk not having their aptitudes for a position recognised, even if their personality traits would be just as beneficial to the exercise of the position they applied for as those of a so-called able-bodied person.[93] As Laurence Devillers, professor of artificial intelligence at Sorbonne University, underlined, "there is an enormous cultural dimension in the way we express ourselves. What do we do with people who stutter, those who speak naturally slowly, those who have an accent?".[94] In addition, these systems can be directly discriminating, in particular by detecting psychological weaknesses or mental problems that fall under the criteria of health discrimination.

Recently, a large American company specialising in this method of recruitment announced that it was abandoning the use of assessment drawn from video analysis of candidates' faces during interviews. However, the automated analysis of their intonation as well as of their behaviour has been maintained even though detecting the emotions in the voice or the meaning of a silence remains very uncertain, as experts pointed out.[95]

While its adoption is still limited in France, some recruitment companies are already marketing software that reduces people's opportunities without their effectiveness[96] being clearly documented and independently audited. These developments are sometimes carried out in breach of labour law, which provides for an obligation of relevance with regard to the information collected by the recruiter. This must in fact have a direct and necessary link with the job on offer or with the assessment of professional aptitudes.[97] A professional association called for the exclusion from recruitment techniques of any data that has no reliable and proven predictive character on the success of candidates.[98]

THE CHILLING EFFECT

One of the peculiarities of biometric identification and assessment technologies when they are deployed in public spaces is based on the chilling effect they can have for the exercise of fundamental rights such as freedom of expression, freedom of movement, freedom of assembly, freedom of association, and, more broadly, access to rights.

The European Data Protection Supervisor, Wojciech Wiewiórowski, pointed out these risks even when these technologies serve legitimate and public interest purposes. The fact that they often operate without knowledge of data subjects and without their control (the so-called absence of friction) tends to dissuade people from exercising their rights, regardless of the scale of their deployment, the fear of surveillance being enough to affect our behaviour.[99] One of the aspects necessary in the exercise of these freedoms is indeed based on group anonymity,[100] in the absence of which individuals may be led to alter their behaviour and not express their thoughts in the same way.[101]

In France, until recently, with regard to the expansion of the use of drones by law enforcement services provided for by the "law for global security preserving freedoms", the Constitutional Council followed in the wake of the CNIL,[102] identifying that these devices are "*capable of capturing, anywhere and without their presence being detected, images of a very large number of people and of tracking their movements over a wide area*",[103] insisting on the need to combine the implementation of these monitoring systems with specific safeguards. This was the meaning of Opinion no. 20-05 of the Defender of Rights[104] and that of the UN Human Rights Council, which, in a report expressed its concerns about the use of drones equipped with cameras, "*likely to have a chilling effect on individuals in public spaces*".[105]

By analogy, biometric remote identification technologies are just as, if not more, intrusive. Indeed, the Constitutional Council has maintained the explicit ban on the processing of drone images by facial recognition software.[106]

Finally, the chilling effect of biometric technologies also results in a risk of exclusion, in particular for people from particularly discriminated against groups such as foreigners. In a report, the UN Special Rapporteur on contemporary forms of racism, Tendayi Achiume, pointed out that the use of biometric technologies could deprive refugees and asylum seekers of access to essential basic services, as a result of their chilling effect.[107] For fear of being identified as "illegal", some migrants could in particular forego the health care to which they are legally entitled, even in an emergency situation.

THE SPECIFIC CASE OF CHILDREN

In France as elsewhere, children like adults are increasingly exposed to biometric technologies, but with undoubtedly a greater risk of trivialisation for a generation born and acculturated to these new technologies without knowing the risks and limits. This phenomenon is not new. As early as 2000, the CNIL had issued an unfavourable opinion concerning the installation of an authentication system for access to a college canteen based on the use of a fingerprint database.[108]

The accountability principle in the GDPR having put an end to the obligation for schools to obtain authorisation to set up this type of biometric solution[109] in 2018, it is now up to them to ensure that they comply with applicable law and document their processing activities.

The introduction of more recent biometric technologies in school grounds has given rise to warnings and sanctions in Europe. In Sweden, the data protection authority sanctioned a school that had deployed a facial recognition device to identify students to verify their attendance.[110] In France, the CNIL considered that the experiment aiming to equip the entrance to two high schools with facial recognition gates in order to identify the pupils of each establishment and to refuse passage to people not attending them contravened the principles of proportionality and minimisation of data posed by the GDPR.[111] In both cases, the authorities considered that the consent obtained was invalid and that the use of facial recognition devices was disproportionate given the existence of much less intrusive means such as badge control.

Children's personal data is subject to rigorous supervision by the GDPR as well as by the French Data Protection Act, which grants them specific protection.[112] This derives from Article 24 of the Charter of Fundamental Rights of the European Union, which provides that in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration.

However, the deployment of biometric remote identification and assessment technologies in publicly accessible spaces goes against these protections insofar as these systems collect in a generalised and undifferentiated manner the biometric data of each person entering their field of operation, children included. Even though this data may subsequently be deleted quickly or even instantly, the mere processing amounts to a risk of serious infringement of children's rights. As the European Union Agency for Fundamental Rights noted in 2018, when facial recognition is used to prevent, detect and investigate terrorism and other serious crimes, it is difficult to see how this can justify the processing of the facial images of children under the age of criminal responsibility.[113]

The Defender of Rights, in its dual mission of defending and promoting the best interests and rights of children, will remain vigilant to ensure that these rights are preserved.

RECOMMENDATIONS

The advances made possible by biometricscannot be made to the detriment of a part of the population, nor at the cost of generalised surveillance. As the Defender of Rights has already reiterated, the right to non-discrimination must be respected in all circumstances, including when a decision involves the use of an algorithm.[114] Likewise, access to rights must remain guaranteed for all.

However, the recent increase in the number of decisions from different European data protection authorities sanctioning the use of biometric devices, in particular facial recognition,[115] testifies to a multiplication of uses carried out in violation of applicable law. The accountability principle in the GDPR coupled with the shortage of the human and financial resources of the data protection authorities[116] moreover suggests that there are probably many more violations than have been reported.

Data protection law provides a first response to the deployment of these technologies by strictly regulating their use through the main principles of necessity, storage limitation and data minimisation or through the specific protection provided to special categories of personal data. In discrimination claims, it constitutes a useful point of support. However, it is sometimes not sufficiently developed to fight effectively against discrimination, in particular against group discrimination.[117] For example, Article 95 of the French Data Protection Act prohibits any profiling that would lead to discrimination against a natural person on the basis of sensitive data. However, the list of so-called sensitive data does not exactly match the list of prohibited discrimination criteria of the Law of 27 May 2008.[118] The issue of gender equality or discrimination based on sex is also completely absent from the GDPR, for which neither gender nor sex are considered special categories of data.[119] Similarly, biometric data is only considered sensitive data when its processing is aimed at uniquely identifying individuals. Consequently, the processing operations carried out for the purpose of assessing individuals hardly benefit from this enhanced protection. In addition, the proxies and correlations of "non-sensitive" data can lead to the same discriminatory effects as the processing operations relating to these special categories of personal data.

Thus, focusing on the impact of biometricson the right to privacy and data protection is necessary but insufficient to understand the overall effect on fundamental rights.[120] In this regard, the CNIL itself has repeatedly highlighted the need to assess the infringements of several other rights.[121]

How can we identify discrimination when it is the result of a biometric tool whose use and/or biases are unknown? How can we ensure that the purposes of using such technology will not be diverted for discriminatory purposes? How can we avoid the emergence of a form of generalised surveillance obstructing access to rights, in particular for the most disadvantaged? How can we ensure that violations of fundamental rights caused by biometric tools can be penalised?

Before carrying out more experiments, it seems essential to be able to answer each of these questions. The recent proposal for an artificial intelligence regulation of the European Commission[122] and the Council of Europe guidelines on facial recognition[123] provide indications.

As part of its missions to fight against discrimination and promote equality, respect for ethics by people carrying out security and defence activities and promotion of the best interests and rights of the child, the Defender of Rights wishes to address a number of recommendations to ensure respect for fundamental rights in the era of biometric technologies.

DISCARD IRRELEVANT ASSESSMENT METHODOLOGIES

Today, it seems essential to systematically question the usefulness of biometrics upstream of their deployment, including in the context of experiments. This questioning should be carried out both by the sellers of these "solutions", who would benefit from questioning the uses of the products they design, and by the buyers, who should show a critical mind with regard to the applications sold to them. Since it is not scientifically possible to infer personality traits from a person's mere appearance, intonation or behaviour, buyers should not give in to the ease, time and cost savings promised by the adoption of certain assessment technologies.

In view of the risk of an increase in discriminatory situations implied by the use of these biometric tools, the Defender of Rights calls for stakeholders to take responsibility. With regard to hiring, for example, it should be remembered that Article L.122-1-8 of the French Labour Code specifies that "the methods and techniques to help with recruitment or assessment of job candidates must be relevant with regard to the aim pursued".

The deployment of technologies based on scientifically unproven methodologies is of concern to the Defender of Rights. This deployment goes beyond the field of employment, as noted by the European Data Protection Supervisor and the European Data Protection Board, which advocate a general ban on methods for assessing emotions.[124]

IMPLEMENT STRONG AND EFFECTIVE SAFEGUARDS TO ENSURE THAT THE RIGHTS OF INDIVIDUALS ARE RESPECTED

No biometric device should be deployed without satisfying strict conditions of necessity and proportionality given the seriousness of the interference caused.

LAW ENFORCEMENT USE

In the law enforcement context, the measures useful for the prevention of crime cannot inappropriately infringe on other rights necessary for the proper functioning of a democratic society, such as the right to privacy, the right to freedom of expression, freedom of assembly and freedom of association and the right to non-discrimination. In accordance with Article 10 of Directive (EU) 2016/680 (Law Enforcement Directive), the deployment of biometric identification tools can only be authorised in cases of strict necessity. Although this notion is evaluated "*with regard only to the needs of the intervention during which [the sensitive data] is collected, in particular for the understanding of a fact or the subsequent qualification of an offence*",[125] it must be assessed together with the proportionality to the purpose and its impact on the rights of data subjects.[126] In other words, impact assessments should be taken into account in order to identify potential violations of the fundamental rights of individuals before any use of the device, but also the use of an alternative less intrusive means of identification should be systematically considered. In any event, recourse to biometric identification cannot concern any type of offence.

With regard to the most intrusive uses, such as real-time remote biometric identification devices in publicly accessible spaces, it seems difficult to conceive how the use of these systems could be considered necessary and proportionate currently given the significant risks of misuse that they represent, i.e. the risks of seeing these devices used for processing purposes other than those for which they were deployed,[127] and the biases they carry with regard to discriminated groups.[128] Recently, the European Data Protection Supervisor and the European Data Protection Board jointly called for a ban on the use of technologies for automated recognition of human features in publicly accessible.[129]

Insofar as the legislator has explicitly prohibited the use of facial recognition software in the context of capturing images by drones of the police forces,[130] the Defender of Rights maintains that this ban should logically be extended to the integration of facial recognition features into existing surveillance systems (body worn cameras, CCTVs, etc.). If the legislator were to authorise such technologies, their use should, as a minimum, be strictly limited to the most serious offences and be the subject of specific authorisations, limited in time and space, and issued on a case-by-case basis by the CNIL or a competent certification authority (for example, that provided for by the proposal for an AI regulation of the European Commission), or by a judicial authority.

ALL PURPOSE

Whatever the nature of the use, whether it be authentication, identification or assessment, particular attention must be paid to respect for the principle of non-discrimination.

The discriminatory biases of biometricsmust be controlled at each stage of deployment. Minimum reliability and accuracy rates for the algorithms used must be set and respected, particularly in relation to people from protected groups. The right to redress for victims of discrimination must be ensured and facilitated by the public orprivate entity acting as data controller. Making access to public services conditional on the use of biometric identification technologies violates the users' right of access, even when such devices are highly accurate.[131] In the opinion of the Defender of Rights, the use of paperless administrative procedures must remain an option for the user and not become an obligation.[132] Finally, even though the collection and processing of sensitive personal data is already strictly regulated, the Council of Europe recommends that, in terms of facial recognition, the use of biometrics for the sole purpose of determining the skin colour of a person, his or her religious or philosophical or political beliefs, gender, racial or ethnic origin, age, state of health or social condition is expressly prohibited unless appropriate safeguards are provided by law to avoid any risk of discrimination.[133]

RESHAPE EXISTING CONTROLS

While some of the most recent biometric technologies can operate remotely and without the knowledge of individuals, the guarantee of an alternative path to their use that can be offered in terms of authentication as outlined in the Alicem decision of the Council of State[134] no longer appears appropriate. Indeed, these technologies automatically apply to everyone regardless. Therefore, unlike uses for the purpose of authenticating people, in terms of identification and assessment in public spaces, two parallel paths seem difficult to envisage. How can we then anticipate the risk of discriminatory situations or situations that obstruct access to rights? The Defender of Rights calls for the creation of new control mechanisms to regulate these uses.

Too often, the controls of biometric devices are limited to cybersecurity and privacy standards when they should take into account other requirements such as the removal of discriminatory bias or respect for the rights of children.

The data protection impact assessments required under Article 35 of the GDPR refer to the high risk that processing can cause for the rights and freedoms of individuals. This prior analysis, which is compulsory in the field of biometrics, must contain an assessment of the risks to the rights and freedoms of individuals and therefore already constitutes a means of anticipating discriminatory effects. However, in the context of impact assessments, when they are carried out, data controllers limit themselves to the rights the GDPR guarantees to data subjects (including the right to rectification of personal data, erasure, portability and restriction of processing). [135] As the Defender of Rights had already underlined in its May 2020 declaration, the challenges of discriminatory risks, the importance of which we have underlined with regard to biometric tools, are therefore not explicitly included.[136]

Similarly, in the context of major public procurement projects, the Decree of 25 October 2019[137] provides for an obligation of prior assessment of information systems by the Interministerial Directorate for Digital Affairs (DINUM) when a public contract exceeds the sum of 9 million euros and sets out a series of exceptions.[138] However, this relatively new control does not include any parameters specific to respect for rights and freedoms. The Defender of Rights recommends revising the assessment threshold in the public procurement of IT solutions and integrating into their control, beyond the mere budgetary aspects, an assessment of the risks of discrimination and, more generally, attacks on freedoms and fundamental rights.

To do this, the Defender of Rights invites the legislator to draw on the European Commission's proposal for an artificial intelligence regulation. The European Commission provides in particular for the obligation for suppliers of remote biometric identification devices to comply with certain strict requirements in terms of transparency and risk assessment before putting these systems into service and/or marketing them, as well as an *ex-ante* conformity assessment procedure.[139]

In addition, the impact assessments provided for by the GDPR can now be carried out in complete autonomy by data controllers under the principle of accountability and therefore possibly "oriented". In this regard, the European Commission's proposal provides that remote biometric identification devices will be required to resort to an external and independent audit of their compliance.[140] For the Defender of Rights, such an obligation should be extended to all biometric assessment and categorisation systems.

Finally, since algorithmic biases may appear beyond the stage of prior assessment of the tools, the Defender of Rights reiterates its recommendation in favour of regular monitoring of the effects of algorithms after their deployment on the monitoring model of unwanted effects of medicinal products.[141] In this regard, the CNIL considers that in a context of technological change and in order to ensure an acceptable level of risk, it is necessary to anticipate an impact assessment on a regular basis.[142] For its part, the European Commission has proposed the establishment of a system of controls to be implemented throughout the life cycle of the devices.[143]

NOTES

[1] CNIL Report, "Facial recognition: for a debate living up to the challenges", November 2019; see also CNIL, "Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position" October 2019; CNIL, "La CNIL appelle à la vigilance sur l'utilisation des caméras dites "intelligentes" et des caméras thermiques", June 2020; CNIL, "Caméras dites "intelligentes" et caméras thermiques: les points de vigilance de la CNIL et les règles à respecter", June 2020.

[2] Declaration of the Defender of Rights, "Algorithmes, prévenir l'automatisation des discriminations", May 2020.

[3] Commission Nationale de l'Informatique et des Libertés, Biometrics.

[4] European Data Protection Supervisor, "14 misunderstandings with regard to identification and authentication", June 2020

[5] Thales, "Biometrics: definition, use cases and latest news".

[6] *Ibid*, p.1.

[7] Castelluccia, Claude, Le Métayer, Daniel. Analyse des impacts de la reconnaissance faciale – Quelques éléments de méthode. [Research report] Inria Grenoble Rhône-Alpes, 2019.

[8] "Passage Automatisé Rapide Aux Frontières Extérieures".

[9] Ministry of the Interior, "Passez les contrôles aux frontières plus rapidement", July 2019.

[10] This can come from photograph or video, including live. This is referred to as "real-time" facial or behavioural recognition.

[11] Commission Nationale de l'Informatique et des Libertés, Definition, Reconnaissance faciale.

[12] T. Kinnunen, E. Karpov and P. Franti, "Real-time speaker identification and verification", in IEEE Transactions on Audio, Speech, and Language Processing, vol. 14, no. 1, pp. 277-288, January 2006, doi: 10.1109/TSA.2005.853206.

[13] O. Costilla-Reyes, R. Vera-Rodriguez, P. Scully and K. B. Ozanyan, "Analysis of Spatio-Temporal Representations for Robust Footstep Recognition with Deep Residual Neural Networks", in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 41, no. 2, pp. 285-296, February 2019, doi: 10.1109/TPAMI.2018.2799847.

[14] European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence, April 2021, p. 19.

[15] Sensitive data within the meaning of Article 6 of the French Data Protection Act (data directly or indirectly revealing the racial or ethnic origin of individuals, political opinions, religious or philosophical convictions, or even trade union membership).

[16] *Ibid*.

[17] Based on cross-referencing between the images of people present within the perimeter of the event and a list of wanted people. For example, see the CNIL warning on the deployment of facial recognition in the FC Metz stadium.

[18] This is the case with the processing of criminal records in France, which is used, pursuant to Articles 230-6 to 230-11 of the French Code of Criminal Procedure, within the framework of judicial inquiries in order to facilitate the ascertainment of offences, the gathering of evidence of these offences and the search for their perpetrators.

[19] Such technologies have been used in particular by the police in South Wales, "Facial recognition use by South Wales Police ruled unlawful".

[20] This is the case with the SARI facial recognition system in Italy, "Italy: Interior ministry's facial recognition system is unlawful"; "Riconoscimento facciale: Sari Real Time non è conforme alla".

[21] European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence, April 2021, p. 42.

[22] *Ibid*, p.42; see also the Opinion of the Article 29 Data Protection Working Party no. 3/2012 on developments in biometric technologies, p.6

[23] Some companies offer to automatically assign an "employability" score to job candidates based on their speed of diction, the choice of words they use and/or their facial movements during a video interview. See: "Votre entretien d'embauche sera peut-être jugé par une IA", *Numerama*, May 2020.

[24] Some examination fraud systems used for exams held remotely claim to be able to automatically identify suspicious student behaviour by tracking their eyes and heads, recording the sound in the room they are in, and by analysing mouse and keyboard movements. See: Feathers & Rose, "Students are Rebelling Against Eye-Tracking Exam Surveillance Tools", *Vice*, September 2020.

[25] By analysing the facial movements of a driver and by deducing signs of fatigue from blinking speed or yawning, for example. See: Elgan, "What happens when cars get emotional", *Fast Company*, June 2019.

[26] For example, by analysing the gait of people in a shop, some systems claim to be able to calculate their propensity to commit thefts. See: Wiggers, "Cashierless tech could detect shoplifting, but bias concerns abound", *Venturebeat*, January 2021.

[27] Italy, Garante per la protezione dei dati personali, Installazione di apparati promozionali del tipo "digital signage" (definiti anche Totem) presso una stazione ferroviaria, 21 December 2017.

[28] Schiffer, Zoe, "This girls-only app uses AI to screen a user's gender — what could go wrong?", *The Verge*, February 2020.

[29] K Crawford, "Time to regulate AI that interprets human emotions", Nature, April 2021.

[30] AI Now Institute, AI Now 2019 Report, December 2019; see also Lauren Rhue, "Racial Influence on Automated Perceptions of Emotions", 2018.

[31] Zhimin Chen and David Whitney, "Tracking the Affective State of Unseen Persons", Proceedings of the National Academy of Sciences, 2019.

[32] Jack Gillum and Jeff Kao, "Aggression Detectors: The Unproven, Invasive Surveillance Technology", *ProPublica*, 25 June 2019.

[33] Lisa Feldman Barrett, Ralph Adochs, and Stacy Marsella, "Emotional Expressions Reconsidered:Challenges to Inferring Emotion From Human Facial Movements", Psychological Science in the Public Interest 20, no. 1 (July 2019): 1–68, see also Barrett et al., "Emotional Expressions Reconsidered.".

[34] O'Neil, "Personality tests are failing American workers", *Bloomberg*, January 2018.

[35] Article 8 of the European Convention on Human Rights.

[36] Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union.

[37] European Union Agency for Fundamental Rights, Council of Europe and European Data Protection Supervisor, *Handbook on European data protection law*, June 2018, p. 19.

[38] CJEU, no. C-212/13, František Ryneš c / *Úřad pro ochranu osobních údajů*, 2014, point 22.

[39] CNIL, White paper on voice assistants, p.40.

[40] 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.

[41] Law no. 78-17 of 6 January 1978 on computing, data storage and freedom of information (French Data Protection Act).

[42] Under Article 9 of the GDPR, this concerns the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical convictions or trade union membership, processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, health data or data relating to a person's sex life or sexual orientation.

[43] CNIL, "Facial recognition: for a debate living up to the challenges", *op cit*.

[44] Directive 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; i.e. when these processing operations take place for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including protection against threats to public security and the prevention of such threats.

[45] CNIL, "Facial recognition: for a debate living up to the challenges", *op cit*.

[46] Speech by the European Data Protection Supervisor, EDPS 07.10.2020 "The State of Biometrics", July 2020; Opinion of the Article 29 Data Protection Working Party no. 3/2012 on developments in biometric technologies, European Data Protection Supervisor, *Guidelines 3/2019 on the processing of personal data through video devices*, January 2020; Spanish Data Protection Agency, *Report on Facial Recognition*, May 2020; ICO, *Guide to data protection*, November 2019.

[47] CNIL, "Facial recognition: for a debate living up to the challenges", *op cit*.

[48] Defender of Rights, Opinion no. 20-13 of 21 December 2020 relating to the proposed law on global security.

[49] More than 175 associations have signed an open letter calling for a worldwide ban on the use of facial recognition and remote biometric recognition allowing mass surveillance and discriminatory targeted surveillance; see Access Now, "Ban Biometric Surveillance", 7 June 2021.

[50] Defender of Rights, Opinion no. 15-25 of 1 December 2015 relating to security in stations in the face of the terrorist threat: Mission d'information sur la sécurité dans les gares face à la menace terroriste, p.3.

[51] "La reconnaissance faciale s'insinue dans la vie des Russes", L'Express, March 2021.

[52] Brewster, "Facial Recognition Firms Pitch Covid-19 'Immunity Passports' for America and Britain", Forbes, 2020; see also Ada Lovelace Institute, "International monitor: vaccine passports and COVID status apps", 10 May 2021, p.58.

[53] Hill, Kashmir, The secretive company that might end privacy as we know it, *New York Times*, January 2020; see also Laufer, Meineck, "PimEyes: A Polish company is abolishing our anonymity", *Netzpolitik.org*, July 2020.

[54] European Data Protection Board, "Swedish Dpa: Police unlawfully used facial recognition app", February 2021.

[55] Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta, February 2021.

[56] See for example F. Reynaud, "Reconnaissance faciale: une enquête demandée à la CNIL sur les pratiques de Clearview", *Le Monde*, May 2021.

[57] Opinion of the Italian Data Protection Authority on the Sari Real Time system, 25 March 2021.

[58] Proposed law no. 4127 on experimentation creating a framework for scientific analysis and citizen consultation on facial recognition devices using artificial intelligence.

[59] Reltien, Philippe, "Reconnaissance faciale: officiellement interdite, elle se met peu à peu en place", Radio France Investigation Unit, September 2020.

[60] Under the principle of lawfulness, any processing of personal data can only be legally carried out if it has a "legal basis" for processing (consent, legitimate interest, legal obligation, task of public interest, contract, protection of vital interests) or if it is necessary for the performance of a task carried out by a competent authority when the processing takes place for the purposes of the prevention and detection of criminal offences, investigations and prosecutions in the matter or execution of criminal penalties.

[61] Under the principle of proportionality, the personal data being processed must be relevant and strictly necessary for the purpose of such processing. See also CNIL, "Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position" October 2019; CNIL, "Reconnaissance faciale et interdiction commerciale de stade: la CNIL adresse un avertissement à un club sportif", February 2021.

[62] "Publicly accessible biometric database highlights key failings", *Computer Weekly*, August 2019.

[63] See Lequesne Roth, Caroline, *Les nouvelles technologies de surveillance dans l'espace public: enjeux et perspectives pour la législation européenne*, Urban Agenda for the European Union, April 2021; See also "Major breach found in biometrics system used by banks, UK police and defence firms", *The Guardian*, August 2019.

[64] Defender of Rights, Opinion 20-06 of 17 November 2020 relating to the text adopted by the Law Commission, on the proposed law on global security, p.4; See also CNIL, "Facial recognition: for a debate living up to the challenges", *op cit*.; Castelluccia, Claude, Le Métayer, Daniel. Analyse des impacts de la reconnaissance faciale – Quelques éléments de méthode. [Research report] Inria Grenoble Rhône-Alpes, 2019.

[65] Huszti-Orbán, Krisztina and Ní Aoláin, Fionnuala, Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?, Human Rights Center, University of Minnesota, July 2020.

[66] A false positive corresponds to a situation where the algorithm mistakenly thinks there is no match while a false negative corresponds to a situation where the algorithm mistakenly thinks there is a match.

[67] Hill, Kashmir, "Wrongfully accused by an algorithm", *New York Times*, August 2020.

[68] Errors according to gender: Buolamwini, Joy and Gebru, Timnit, "Gender Shades, Intersectional Accuracy Disparities in Commercial Gender Classification", Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 2018; errors according to gender, age, skin colour: Grother, P., Ngan, M., and Hanaoka, *Ongoing Face Recognition Vendor Test (FRVT). Part 1: Verification*, April 2019; errors according to age: Raji, Inioluwa Deborah, Gebru, Timnit, Mitchell, Margaret, Buolamwini, Joy, Lee, Joonseok and Denton, Emily. 2020. "Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing". In *Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics, and Society* (AIES '20), February 7–8, 2020, February 2020, European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, November 2019.

[69] When the algorithms are mainly trained on photos of white men, poor performance is observed when they are used on other types of profiles; see Buolamwini, Joy and Gebru, Timnit, "Gender Shades, Intersectional Accuracy Disparities in Commercial Gender Classification", Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 2018

[70] Declaration of the Defender of Rights, "Algorithmes, prévenir l'automatisation des discriminations", May 2020.

[71] *Op. Cit*. Note no. 65.

[72] European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, November 2019, p. 9.

[73] As is the case with the Parafe system. See Grother, P., Ngan, M., and Hanaoka, *Ongoing Face Recognition Vendor Test (FRVT). Part 1: Verification*, April 2019.

[74] ALICEM (certified online authentication on mobile) is a device using facial recognition currently being tested in France. In its Alicem decision of 4 November 2020, the Council of State considered that "since users who do not consent to the processing anticipated in the context of the creation of an Alicem account can access online [via the FranceConnect service], using a unique identifier, all the remote services offered, they cannot be regarded as suffering damage within the meaning of the aforementioned General Data Protection Regulation". In this case, the Council of State thus considered that the FranceConnect portal (a device allowing Internet users to identify themselves on an online service through an existing account (ameli.fr, impots.gouv.fr, etc.) was a sufficient alternative way to the use of the Alicem device to verify the identity of Internet users.

[75] See Privacy International's submission for the UN High Commissioner for Human Rights' report on the right to privacy and artificial intelligence, May 2021, p.4.

[76] See for example: Lomas, "Uber under pressure over facial recognition checks for drivers", *TechCrunch*, March 2021.

[77] This is because of the quality of the image source, whether it is a photo or a video. In an uncontrolled environment, the parameters of lighting, exposure, etc. change and may affect the accuracy of the device.

[76] See *Op. Cit*. notes 66 & 67.

[79] FRA European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement.

[80] Hill, Kashmir, "Another arrest and jail time due to a bad facial recognition match", *New York Times*, December 2020.

[81] Fussey, Pete and Murray, Daragh, Independent Report on the London Metropolitan Police Service's Trial of Facial Recognition Technology, The Human Rights, Big Data and Technology Project, July 2019.

[82] Court of appeal, *R (Bridges) v Chief Constable of South Wales Police*, 2019, EWHC 2341 (Admin).

[83] Defender of Rights, Enquête sur l'accès aux droits. Vol.1: Rapports police / population. The study on access to rights (vol. 1) carried out on a representative sample of more than 5,000 people was published in 2017.

[84] Namely by recording offences by video and then sending, for example, a ticket by post.

[85] Defender of Rights, Decision 2020-102 of 12 May 2020 relating to observations before the judicial tribunal of X in the context of proceedings for State liability for discriminatory identity checks, p.9.

[86] See the Defender of Rights' Report, "La défaillance du forfait de post-stationnement: rétablir les droits des usagers", 13 January 2020.

[87] European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence, April 2021, Art. 5 paragraph 1 point d (iii).

[88] European Union Agency for Fundamental Rights (FRA), "Being Black in the EU: Second European Union Minorities and Discrimination Survey: Summary", *op.cit*.

[89] European Commission, "Intelligent Portable Border Control System", Horizon 2020; see also "IBorderCtrl: Intelligent Portable Control System Project".

[90] iBorderCtrl first asks travellers to upload photos of their passport, visa and other documents, which are then transmitted to the artificial intelligence that awaits them at border control. This AI then asks questions via a loudspeaker and analyses the human responses using a webcam in order to detect the micro-expressions present on the faces of travellers. Following this machine interrogation, a token is issued to the traveller: if he or she is suspected by the iBorderCtrl system of having lied, the token leads him or her to a queue where border guards will retrieve biometric data (fingerprints and hand-vein pattern, facial recognition) to continue the check; if the machine has not detected a lie, the token given to the traveller takes them to a "low risk" queue, with fewer checks.

[91] See: E. Chelloudakis, "Greece: Clarifications sought on human rights impacts of iBorderCtrl", *EDRi*, November 2018. In 2018, the system was credited with a success rate of around 75%, which leaves a quarter of travellers who may be suspected of lying when this is not the case. An MEP has also started legal proceedings in order to shed light on the origins of this unethical experiment, aimed at obtaining answers concerning in particular the profile of individuals who return false positives in order to identify potential discrimination caused by this system. See P. Breyer, "EU-funded technology violates fundamental rights", *about:intel*, 22 April 2021; see also European Parliament, Question for written answer E-000152/2020 to the Commission, Rule 138, Patrick Breyer (Verts/ALE), January 2020.

[92] Modelled on the American HireVue, the French company Itwapp, for example, offers to carry out AI-enhanced deferred video interviews that will sort candidates according to the data suggested by their facial and oral expressions. By analysing body language and speech, the AI would analyse the candidate's openness (curiosity), conscientiousness (control, discipline, etc.), extroversion, agreeableness and negativity. The machine classifies candidate language elements, the richness of their vocabulary, the intonation, the modulation of their voice, the length of their sentences, revealing their ability to summarise, their speech rate, etc. and this data is correlated with the Big Five test, a classic personality test. The start-up claims not to use facial analysis, since the technology is far from being advanced. For now, the service it offers its clients is the transcription of everything the candidate says in order to evaluate it according to five criteria: prosody (accentuation, intonation), fluency, verbal ability, speed of speech and verbal content. It takes less than three minutes for the machine to analyse these criteria and propose a graded classification between the candidates who responded to the same job offer.

[93] A. Engler, "For some employment algorithms, disability discrimination by default", Brookings, October 2019.

[94] Krassovsky, Julie, "Recrutement: quelles sont les limites de l'intelligence artificielle?", *Capital*, April 2020.

[95] Knight, Will, "Job screening service halts facial analysis of applicants", *Wired*, January 2021.

[96] These techniques are supposed to make it possible to assess the candidate's future professional performance, his or her ability to manage or even certain desired qualities. The effectiveness consists here in identifying the candidate who will actually perform well once in the job.

[97] French Labour Code, Art. L.1221-6 section 2.

[98] See ***A compétence égale***, Charter "Algorithmes, intelligence artificielle et recrutement".

[99] Speech by the European Data Protection Supervisor, EDPS 07.10.2020 "The state of Biometrics", July 2020; see also ACLU, "Does Surveillance Affect Us Even When We Can't Confirm We're Being Watched? Lessons From Behind the Iron Curtain", 2012.

[100] International Justice and Public Safety Network (2011), Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field, 30 June 2011.

[101] Human Rights Council (2019), Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, A/HRC/41/35.

[102] CNIL, Deliberation of the limited bench no.SAN-2021-003 of 12 January 2021 concerning the Ministry of the Interior.

[103] Decision no. 2021-817 DC of 20 May 2021.

[104] Defender of Rights, Opinion no. 20-05 of 3 November 2020 relating to the proposed law on global security.

[105] Report OL FRA 4/2020 Mandates of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; and the Special Rapporteur on the right of peaceful assembly and freedom of association, 12 November 2020.

[106] Law no. 2021-646 of 25 May 2021, art. 47 (V).

[107] Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, 10 November 2020.

[108] CNIL, Deliberation 00-015 of 21 March 2000.

[109] Former Article 25 of the French Data Protection Act of 6 January 1978.

[110] EDPB, "Facial recognition in school renders Sweden's first GDPR fine", August 2019.

[111] CNIL, "Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position", October 2019.

[112] GDPR, Recitals 38 and 58.

[113] FRA (2018), *The revised Visa Information System and its fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights*, FRA Opinion 2/2018 [VIS], Vienna, 30 August 2018, pp. 67-69.

[114] Declaration of the Defender of Rights, "Algorithmes, prévenir l'automatisation des discriminations", May 2020.

[115] The Hamburg Commissioner for Data Protection and Freedom of Information, "Administrative order on Information issued against Clearview AI -Transparent answers on Data Protection required!", August 2020; CNIL, "Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position", October 2019; CNIL, "Surveillance des examens en ligne: les rappels et conseils de la CNIL", 20 May 2020.

[117] European Parliament, Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application, March 2021.

[116] Tisné M., "Collective data right scan stop big tech from obliterating privacy" *MIT Technology Review*, 25 May 2021, see also Tisné, "The data delusion: protecting individual data isn't enough when the harm is collective".

[118] Law no. 2008-496 of 27 May 2008 laying down various provisions for adaptation to Community law in the field of the fight against discrimination, Art. 1.

[119] Xenidis R., Gerards J., Algorithmic discrimination in Europe, Challenges and opportunities for gender equality and non-discrimination law, Publications Office of the EU, March 2021, p.49.

[120] Huszti-Orbán & Ní Aoláin, Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business? - Summary of findings and recommendations, Human Rights Center University of Minnesota (2020).

[121] CNIL, "Facial recognition: for a debate living up to the challenges", November 2019; see also CNIL, "Expérimentation de la reconnaissance faciale dans deux lycées: la CNIL précise sa position", October 2019; CNIL, "La CNIL appelle à la vigilance sur l'utilisation des caméras dites "intelligentes" et des caméras thermiques", June 2020; CNIL, "Caméras dites "intelligentes" et caméras thermiques: les points de vigilance de la CNIL et les règles à respecter", June 2020.

[122] European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence, April 2021, p. 19.

[123] Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention 108, Guidelines on Facial Recognition, January 2021.

[124] CEPD-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, p.2.

[125] Council of State Decision no. 439360, paragraph 13.

[126] Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention 108, Guidelines on Facial Recognition, January 2021, p.3.

[127] For instance a police officer who would like to find somebody without valid reason.

[128] See European Data Protection Supervisor, "Artificial Intelligence Act: a welcomed initiative, but ban on remote biometric identification in public space is necessary", April 2021.

[129] CEPD-EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 18 June 2021, p.2.

[130] Law no. 2021-646 of 25 May 2021 for global security preserving freedoms, Art. 47.

[131] See Lequesne Roth, Caroline, *Les nouvelles technologies de surveillance dans l'espace public: enjeux et perspectives pour la législation européenne*, Urban Agenda for the European Union, April 2021.

[132] Defender of Rights, Report, Dématérialisation et inégalités d'accès aux services publics, 2019, p.29.

[133] Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention 108, Guidelines on Facial Recognition, January 2021, p.3.

[134] *Op. Cit.* Note 72.

[135] See also Renaissance Numérique, «Facial Recognition : Embodying European Values», Civil liberties and ethics, June 2020, p.73.

[136] Declaration of the Defender of Rights, "Algorithmes, prévenir l'automatisation des discriminations", May 2020.

[137] Decree no. 2019-1088 of 25 October 2019 relating to the State information and communication system and the Interministerial Directorate for Digital Affairs.

[138] This threshold of 9 million is set in Article 1 of the Decree of 5 June 2020. See Order of 5 June 2020 relating to the State information and communication system and the Interministerial Directorate for Digital Affairs.

[139] The proposal provides, among other things, for the obligation to provide for adequate risk assessment and mitigation mechanisms, to guarantee a high quality of data mobilised by the system in order to minimise risks and discriminatory situations, to ensure the traceability of any use of the device, to provide detailed documentation gathering all the necessary information on the system and its purpose so that the authorities can assess its compliance, to inform the user in clear and understandable terms about the operation of the device, to plan appropriate human supervision measures to minimise risks, and to guarantee a high level of reliability, security and accuracy of the system; see T. Christakis, "Facial recognition in the draft European AI regulation: final report on the high-level workshop held on April 26, 2021", 27 May 2021.

[140] European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence, April 2021, Art. 43

[141] Declaration of the Defender of Rights, "Algorithmes, prévenir l'automatisation des discriminations", May 2020.

[142] CNIL, "Everything you need to know about data protection impact assessment (DPIA)", 22 October 2019.

[143] European Commission, Proposal for a Regulation laying down harmonised rules on artificial intelligence, April 2021, Art. 43.

Defender of Rights

TSA 90716 - 75334 Paris Cedex 07

Phone: 09 69 39 00 00

defenseurdesdroits.fr

All our news:

defenseurdesdroits.fr

Défenseurdesdroits

RÉPUBLIQUE FRANÇAISE