SCIENCE AND TECHNOLOGY BRIEFINGS
PARLIAMENTARY OFFICE FOR SCIENTIFIC AND TECHNOLOGICAL ASSESSMENT

Briefing 14 — July 2019

Facial Recognition

123fr©AndriyPopov

Summary

- *Advances in the development of artificial intelligence (in particular deep learning) have led to significant improvements in the performance of facial recognition tools. They now seem to be within everyone's reach: smartphone applications, automated payments, identity checks at borders etc.*
- *Often little known to the public, an extensive economy is developing around the use of this data, giving rise to concerns about how such applications could infringe on fundamental freedoms.*
- *It seems necessary to develop a legislative framework for experimentation in order to test these systems under real conditions and ensure our sovereignty, so that we are not dependent on solutions developed by the tech giants, then to establish a regulatory framework that best suits uses.*

Mr Didier Baichère, Member of Parliament(National Assembly), Vice-Chair

Technological context

Facial recognition technology has appeared recently as a subject of public debate, in particular since the recent test carried out by the City of Nice, and San Francisco's ban on the use of such systems by its services. It therefore appeared necessary for the Office to study the technological, ethical, legal and sociological issues concerning this technology.

Computer vision is a field of artificial intelligence[1] (AI) in which images are analysed automatically. Facial recognition is a branch of computer vision concerned with the biometric analysis of faces present in an image. Significant performance gains have been achieved in these technologies in recent years as a result of advances in algorithms connected to the use of deep learning and sensor technologies.

The process can be schematically described as follows: the algorithm extracts a template from a photo – a sort of signature which is unique to each face – then compares it to templates taken from other images to determine if they correspond to the same person. It is important to remember that facial recognition systems do not provide absolute results; the results are expressed as a match percentage. A match threshold[2] must then be chosen, at which point it will be decided that two templates definitely correspond to the same person.[3]

Facial recognition must not be confused with facial analysis or affect recognition, which aim to determine certain characteristics (age, gender, ethnic origin, emotions etc.) of the individuals present in an image. These latter two fields do not use biometric data and are therefore, strictly speaking, less sensitive than facial recognition. A wide range of commercial applications using facial recognition, facial analysis and affect recognition are being developed: targeted marketing, electronic device unlock,[4] banking applications,[5] as well applications for diagnostic support[6] and detecting stress in vulnerable individuals.[7] However, the automation of tedious and time-consuming processes remains the main application of facial recognition.[8]

For instance, real-time or non real-time analysis of video surveillance images can enable law enforcement agencies to detect scenes of interest more quickly. These systems therefore have potential applications in home security and police matters.[9] In France, their use by police and gendarmerie forces is currently limited to comparing images obtained during an investigation with the "criminal records database" (TAJ) – the only judicial police file that permits the use of facial recognition;[10] the Parafe system[11] for external border crossings; and the ALICEM[12] digital identification system. The organizing committee for the 2020 Olympic Games, which will be held in Tokyo, plans to use checkpoints equipped with facial recognition systems to control access reserved for athletes, staff and reporters.[13]

Lastly, in order to be recognised, an individual must already be "enrolled", meaning he or she must be included in the database against which the images are compared. The data on which facial recognition

processing is carried out is therefore a key issue.

Authentication or identification?

It is important to distinguish between two categories of uses for facial recognition systems:

– *Authentication* means determining if a person corresponds to the person he/she claims to be. It is therefore carried out by comparing a template extracted from a photo taken during the process to a previously recorded template.

➢ Examples: Parafe systems (see below) or to unlock a telephone

– *Identification* means trying to find the identity of a person in an image by comparing it with a large number of previously collected images compiled in a database.

➢ Example: smart video surveillance

A still-imperfect technology

Despite advances in recent years, facial recognition technology is still not completely effective. The conditions under which these systems are used have a significant impact on their success rate. Under controlled conditions (lighting, camera angle, no movement), as is the case for the Parafe system for example, the reliability level can be higher than 99.5%. But it is a different situation altogether when it comes to uncontrolled environments. The National Institute of Standards and Technology (NIST), the American agency responsible for testing facial recognition technologies, published a report on the performance of identification algorithms[14] in November 2018 attesting to the progress which has been made while pointing to the negative impacts of various factors, such as image quality or individuals' aging on the success rate of these algorithms. Studies[15] have also shown that it is possible to fool these algorithms by using masks made with 3D printers for example.[16] A number of tests carried out in other countries have highlighted improvements that can still be made.[17]

Biases persist

Many studies have reported performance gaps for facial recognition algorithms between different segments of the population. Joy Buolamwini, a researcher at Massachusetts Institute of Technology (MIT), has demonstrated[18] that algorithms tend to have more difficulty recognising black women than white men. Similarly, in a report published in April 2019,[19] the NIST underscored that all of the algorithms systematically performed less well for recognizing women than for recognizing men. This is primarily due to the lack of diversity in the image databases used to train the algorithms. This is an especially important issue and must be studied. Many of the individuals interviewed to prepare this briefing spoke about their efforts to increase diversity within their databases. The situation seems to be improving, as Joy Buolamwini found in another study.[20]

A legal framework does exist

A number of existing French and European legal provisions apply to the use of facial recognition systems. The framework to be applied depends mainly on the way in which these systems are used:

- Use by the State as part of its official powers as a public authority

In France, processing of biometric data on behalf of the State as part of its official powers as a public authority is subject to Articles 31 and 32 of the Law on information technology, data files and civil liberties (*loi "informatique et libertés"*)[21] and Article 10 of European Directive no. 2016/680.[22] These provisions limit the scope of such processing[23] and require a decree issued by the *Conseil d'État* (Council of State) with the favourable opinion of the CNIL[24] before it can be implemented. The use of facial recognition coupled with a video surveillance system or other judiciary police records must be in keeping with this legal framework.

- Use in other contexts

Since 25 May 2018, personal data processing within the European Union has been governed by the General Data Protection Regulation (GDPR).[25] Because the use of facial recognition systems involves biometric data – which is particularly sensitive since it makes it possible to uniquely identify an individual – it must therefore comply with the provisions set out in this regulation. In particular, the controller must carry out a data protection impact assessment[26] and send it to the CNIL, for prior consultation, if a high level of residual risk is detected. The CNIL is therefore no longer systematically informed about these systems being put in place and must no longer give its approval in advance. In turn, this new system aims for accountability[27] on the part of those processing data and their subcontractors, who are considered to be jointly accountable. For this type of use, consent[28] is one of the possible legal bases,[29] which raises the question of how this consent is to be obtained (notices at entrances to shops etc.) The GDPR provides for the possibility for exemptions from certain rules if processing is carried out for the purposes of scientific research.

But this framework is incomplete

The test carried out in Nice[30] highlighted the need to supplement the current legal framework.

Test carried out in Nice during the 135th edition of Carnival (February 2019)

Over a three-day period, the City of Nice carried out France's first test of a facial recognition system under real conditions. A number of different scenarios were tested during this trial (looking for lost children and vulnerable persons, making flows more fluid at access points, restricted access control etc.) carried out on consenting individuals.

This test was carried out within the framework established by the GDPR, with the legal basis being scientific research rather than security. Although the CNIL was not required to give prior authorisation, the CNIL and the City of Nice worked together ahead of the Carnival to ensure compliance with the provisions of the GDPR.

Representatives from industry, regulatory bodies and the public sector have expressed their wish for legal provisions to be developed to authorise large-scale testing of facial recognition systems in order to test the advantages and limitations of this technology under real conditions, from both a technical and sociological viewpoint, so as to better understand these aspects and propose a legal framework which is best suited to uses, while respecting fundamental freedoms.

The development and distribution of facial recognition systems outside of Europe is inevitable, given the proliferation of applications and the growing number of players investing in this technology, led by tech giants including the GAFA (Google, Amazon Facebook, Apple and Microsoft) and BATX (Baidu, Alibaba, Tencent and Xiaomi) companies. In order for France to safeguard its sovereignty, it must therefore support research and innovation[31] in this technology as part of the AI sector.

A technology that requires a public debate

Local authorities have already been confronted with these issues through the deployment of video surveillance cameras to varying degrees in urban areas. As demonstrated in discussions with the Association of French Mayors (AMF), elected officials are aware of the consequences of the "*safe city*"[32] on personal freedoms; citizens' acceptance is a key issue in the potential deployment of facial recognition systems.

The CNIL has recently called for a democratic debate on these issues.[33] This debate must give the various stakeholders the opportunity to express their views on the question of the authorisation, regulation and prohibition of certain uses, which may only be addressed in a sustainable way after these systems have been tested under real conditions.

Concerns are frequently expressed[34] about the risks the distribution of facial recognition systems poses to our fundamental freedoms (freedom to move anonymously, freedom to demonstrate etc.) and the possibility of the development of widespread surveillance of citizens. China[35] is the most striking example, with its incorporation of information collected using facial recognition technology in the social credit system,[36] or its control of Uyghur populations in Xinjiang.[37] Such concerns must be taken into consideration and the distribution of these systems must be carried out without infringing on fundamental rights. For Laurent Mucchielli, a sociologist at CNRS, "Technology is neither good nor bad in and of itself. It all depends on how we choose to use it and the financial decisions behind our choices".[38] According to Jean-Gabriel Ganascia, Chairman of the CNRS Ethics Committee, these concerns could be addressed by distinguishing between different uses and authorising only those which do not pose a risk.

The French Digital Council and the World Economic Forum Centre for the Fourth Industrial Revolution (C4IR) have launched a twelve-month pilot project to inform the democratic debate on how to regulate facial recognition technologies at the French, European and international levels. This project aims to jointly develop facial recognition regulation to ensure the protection of personal freedoms.[39]

Tech giants have publicly expressed their consideration for the social issues raised by these systems. Microsoft's president, Brad Smith, has asked lawmakers to regulate this technology[40] and the company has established principles to structure its facial recognition strategy.[41] Google CEO Sundar Pichai has taken a similar step by publishing his company's seven principles of AI.[42] Qwant has made the decision to integrate tools that make it possible to blur all the faces in the facial recognition systems it puts in place.[43] Meanwhile, Amazon has adopted a less proactive approach and does not consider itself responsible for possible uses of its tools.[44]

France could position itself as a model for these issues, in light of its top researchers and the fact that it is home to some of the most successful companies in the world – such as global biometrics leader IDEMIA and global digital security leader Gemalto – and dynamic startups like the XXII Group.

These technologies could also be widely developed for military purposes.[45] In the French Ministry for the Armed Forces, the Defence Innovation Agency, a part of the Directorate General of Armaments (DGA), was created on 1 September 2018. Defence Minister Florence Parly has also announced the creation of a "Ministerial Ethics Committee to address defence topics." These two bodies will be responsible for carefully studying the ethical issues involved in applications of this technology in the defence sector.

A subject debated in numerous countries

The installation of video surveillance systems in the United Kingdom has made it an ideal location for the rapid deployment of facial recognition systems.[46] The Metropolitan Police Service has carried out many tests,[47] most of which have fallen short of their expectations. Commercial applications are already in use as well, for example by Children's Charity Plan UK, who targets its advertising campaign in buses depending on a passenger's gender. The framework governing the use of these systems is evolving rapidly. In June 2018, the Home Office published a strategy for biometric technologies[48] intended to supplement the existing provisions.[49]

In the Netherlands, law enforcement agencies have partnered with the Netherlands Forensic Institute to study the possibility of using facial recognition technology in criminal investigations or to fight terrorism by equipping patrol officers with body cameras connected to a database. In a commercial context, the supermarket chain Jumbo Ten Bring Food has recently installed facial recognition systems to prevent shoplifting.

Facial recognition is currently a widely debated topic in the United States as well. The technology brings together a number of companies that are at the forefront in this field and is widely used by law enforcement agencies. However, the situation varies from one state to another; there is no federal legislation regulating these systems. Recently, there have been calls for regulation: many cities have followed the example set by San Francisco, which has recently announced a ban on the use of this technology by city services, and a bipartisan bill[50] has been introduced to this end.

Conclusions and recommendations

Facial recognition systems are already present in our everyday lives and are becoming increasingly effective. Widespread use of the technology seems inevitable and raises social, legal and ethical issues. In order to allow for the development of these technologies while ensuring that fundamental human rights are protected, the following recommendations may be made:

– Quickly develop a legislative framework which makes it possible to support testing,[51] to the benefit of France's industrial and academic ecosystem. The CNIL should be given the role of supporting innovation and encouraging "privacy by design"[52] in the field of facial recognition and more generally, for all new technologies that use personal data, based on the model of the role played by the French Electronic Communications and Postal Regulatory Authority (ARCEP),[53] while ensuring respect for fundamental freedoms, French sovereignty and the development of ethical AI.

– As proposed in Cédric Villani's report on artificial intelligence,[54] establish, within a chosen body, a group of multidisciplinary experts who have the skills required to audit facial recognition systems in order to ensure that the technologies brought to market are effective according to different categories of needs, and that they are unbiased.

– Reassert the responsibility of all the stakeholders involved: developer, integrator, controller. It is inconceivable that certain stakeholders, including tech giants, should not be held accountable.

– Ensure human verification for the most sensitive uses (legal proceedings etc.).

– Carry out studies on the acceptability of these technologies for different segments of the population.

– Improve training on the data economy to make it possible to make informed decisions, free of the myths surrounding these technologies.

OPECST website:
http://www.assemblee-nationale.fr/commissions/opecst-index.asp
http://www.senat.fr/opecst/

Persons interviewed

Ms Véronique Borré, Deputy Director of the Office of the Mayor of Nice, Mr Gildas Berthier, Head of Municipal Police Services, Ms Sandra Bertin, Chief of the Municipal Police, Messrs Grégory Pezet, Head of the Urban Supervisory Control, Franck Curinga, Head of the Information Systems and Smart City Department, Jean-François Ona, "Security" Project Leader and Stephan Louppe, Director of Operations for Confidentia, during a mission in Nice on 14 June 2019

Mr Jean-Christophe, Founder, Director of R&D and member of the Executive Committee, Mr Pascal Fallet, Senior Vice-President for Europe for "Identity and Public Security", and Ms Céline Stierlé, Press Relations and Public Affairs Director for IDEMIA

Ms Florence Fourets, Head of Public Projects, Émilie Seruga-Cau, Head of the Public Affairs and Local Authorities department and Tiphaine Havel, Advisor for Institutional and Parliamentary Affairs for the Commission nationale de l'informatique et des libertés (CNIL - the French Data Protection Authority)

Messrs Julien Groues, General Manager, Stéphane Hadinger, Innovation Manager and Lionel Benatia, Public Policy Manager for Amazon Web Service (AWS) France

Ms Nathalie Koenders, First Deputy Mayor of Dijon, President of the Security Commission, Mr Juan Companie, "Security" Project Leader for the Director General and Ms Charlotte de Fontaines, Head of Parliamentary Relations for the Association of French Mayors (AMF)

Messrs Éric Léandri, Co-Founder and CEO, Christophe Sevran, Scientific Director, Sébastien Ménard, Special Advisor to the Executive Committee, Maxime Portaz, Researcher for Qwant

Ms Aurélie Misséré, Head of AI Projects, Messrs Florent Montreuil, expert in AI and automatic multi-sensor recognition and Mattis Paulin, Project Architect for the *Direction Générale de l'Armement* (DGA - the French Directorate General of Armaments) of the French Ministry of Armed Forces

Messrs Cédric O, Secretary of State to the Prime Minister, in charge of Digital Technology and Bertrand Pailhès, National Coordinator for the French Artificial Intelligence Strategy

Mr Bernard Ourghanlian, Technical and Security Director and Ms Camille Vaziaga, Public Affairs Manager for Microsoft France

Mr Ludovic Péran, Public Policy and Government Affairs Manager for Google France

Mr Renaud Vedel, Prefect, Artificial Intelligence Coordinator for the Ministry of the Interior, General Bruno Poirier-Coutansais, Head of the Technology for National Security department ($STSI^2$), and Mr Vincent Niebel, Head of Information and Communication Systems for the French Ministry of the Interior.

Experts consulted

Ms Virginie Tournay, member of the Scientific Council for the Office, Director of Research at the CNRS (French National Centre for Scientific Research), Sciences Po Centre for Political Research (CEVIPOF)
Mr Serge Abiteboul, Director of Research at INRIA (French Research Institute for the Digital Sciences) and at ENS, member of the French Academy of Sciences, member of the Board of the *Autorité de régulation des communications et des postes* (ARCEP - French Electronic Communications and Postal Regulatory Authority)
Mr François Brémond, Director of Research at INRIA, STARS group
Mr Jean Cattan, Advisor to the President of ARCEP
Mr James Crowley, Director of Research at INRIA, Pervasive Interaction group
Mr Mohamed Daoudi, Professor of Computer Science at IMT Lille Douai, CRIStAL laboratory
Mr Jean-Luc Dugelay, Professor of Computer Science at EURECOM
Mr Jacques Ehrmann, Executive Director of "Heritage, International Development and Innovation" for the Carrefour group
Mr Jean-Gabriel Ganascia, Professor of Computer Science at Sorbonne University's Faculty of Science, member of Institut Universitaire de France, Chairman of the CNRS Ethics Committee
Mr Lofred Madzou, Project Lead for "Artificial Intelligence and Machine Learning", Centre for the Fourth Industrial Revolution), World Economic Forum
Mr Laurent Mucchielli, Director of Research at CNRS, Mediterranean Sociology Laboratory
Ms Judith Rochfeld, Professor of Law at University Paris 1 Panthéon-Sorbonne
Ms Mélinda Souef, Head of Parliamentary Relations for the Aéroports de Paris group (ADP)

Contributions

Embassy of France in the United States: Office for Science and Technology
Embassy of France in the United Kingdom: Office for Science and Technology
Embassy of France in the Netherlands: Internal Security, Cooperation and Cultural Action and Science and Technology departments

References

(1) For this subject, see the report (n° 4594) by Mr Claude de Ganay and Ms Dominique Gillot, submitted on behalf of the Office in March 2017, "Pour une intelligence artificielle maîtrisée, utile et démystifiée" (Toward a Controlled, Useful and Demystified Artificial Intelligence).

http://www.assemblee-nationale.fr/14/rap-off/i4594.asp and its summary
http://www.senat.fr/fileadmin/Fichiers/Images/opecst/quatre_pages/OPECST_rapport_Intelligence_artificielle_synthese_4pages.pdf

(2) The way this threshold is determined depends greatly on how the system will be used, since the required confidence level will not be the same for a general use application on social media, authorisation to access a protected site or as evidence in a criminal case. The tool currently used by law enforcement agencies in France proposes several profiles which could match images of wanted individuals, which makes it possible to increase the probability of obtaining an exact response.

(3) Two types of errors could be made: either the system does not recognise the individual (this is referred to as a false negative), or it recognises an individual it should not recognise (this is referred to as a false positive).

(4) Briefing N° 1 on Connected Objects:
http://www2.assemblee-nationale.fr/content/download/65396/664019/version/8/file/note+1+-+4+pages+objets+connectes.pdf
5 A bank has made it possible to open an account remotely without a mandatory deposit, using biometric facial recognition through a dynamic selfie developed by IDEMIA in order to identify the future customer:
https://www.idemia.com/fr/actualite/societe-generale-et-idemia-revolutionnent-louverture-de-compte-distance-2018-06-01

*(6) Gurovich, Yaron & Hanani, Yair & Bar, Omri & Nadav, Guy & Fleischer, Nicole & Gelbman, Dekel & Basel-Salmon, Lina & M. Krawitz, Peter & Kamphausen, Susanne & Zenker, Martin & M. Bird, Lynne & W. Gripp, Karen. (2019). "*Identifying facial phenotypes of genetic disorders using deep learning" Nature Medicine *25. 10.1038/s41591-018-0279-0: https://www.nature.com/articles/s41591-018-0279-0*

(7) INRIA and the CMRR of the Nice CHU (University Hospital) partnered to create the CoBTeK team to study this topic: http://cmrr-nice.fr/?p=cobtek-presentation

(8) For example, the flow of passengers in a train station or airport can be made more fluid by having them pass through certain control points in an automated way using facial recognition systems. This type of tool is used in several American and Asian airports and companies such as Aéroports de Paris (ADP - Paris Airports) and Carrefour have tested such systems.

(9) These systems are used to control border crossings in many countries, for example at airports or train stations.

(10) This is only one piece of information and does not in any way constitute proof. Article 1 of Decree no. 2012-652:
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025803463&categorieLien=id

(11) French Acronym for "Rapid Automated Crossing for External Borders" for passengers who have a biometric passport. Border control is now carried in an automated way for certain consenting passengers. The Parafe system verifies travellers' identity by comparing a photo taken at the checkpoint with the image on their passport and the one stored in the chip.

(12) With the support of the Agence nationale des titres sécurisés (ANTS - the French National Agency for Secure Identity Documents), the Ministry of the Interior put in place the ALICEM system (mobile-based certified online authentication) in May 2019, making it possible for anyone with an Android telephone and a secure identity document (passport, residency permit) to have a secure digital identity. In an opinion published on 18 October 2018, the CNIL regretted the absence of an alternative to facial recognition and criticised the retention period for application access logs (6 years).

Decree no. 2019-452 of 13 May 2019 authorising the creation of an electronic identification method called "Authentification en ligne certifiée sur mobile" (Mobile-Based Certified Online Authentication: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038475477&categorieLien=id

Opinion of the CNIL: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000038475742

(13) The question which therefore arises is the use of facial recognition tools during the Olympic Games to be held in France in 2024. It is essential that a sustainable legal framework be put in place before this event.

(14) NIST, Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification, November 2018: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf

(15) https://www.forbes.com/video/5978671815001/#744af9722461

(16) Briefing N° 2 on 3D Printing:
http://www2.assemblee-nationale.fr/content/download/65485/665121/version/4/file/notescientif_impression+3D+ENG20190409.pdf

(17) For example the Notting Hill carnival in the United Kingdom (https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure) for which the London police used facial recognition technology with an error rate of 91%; or the facial recognition trial on drivers in New York (https://www.wsj.com/articles/mtas-initial-foray-into-facial-recognition-at-high-speed-is-a-bust-11554642000) during which no exact identification was made.

*(18) Joy Buolamwini, Timnit Gebru; "*Proceedings of the 1st Conference on Fairness, Accountability and *Transparency*", PMLR 81:77-91, 2018: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

(19) NIST, *"Ongoing Face Recognition Vendor Test (FRVT) Part 1: Verification", June 2019:*
https://www.nist.gov/sites/default/files/documents/2019/06/20/frvt_report_2019_06_20.pdf
(20) Inioluwa Deborah Raji, Joy Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products": https://dam-prod.media.mit.edu/x/2019/01/24/AIES-19_paper_223.pdf .
Three tools studied in 2017 (Microsoft, Face++ and IBM) decreased their error rate for women by an average of 13 points; although per-

formance differences remain, the algorithms studied have an average error rate for black women which is 15 points higher than that for white men.

(21) Articles 31 and 32 of Law no. 78-17 of 6 January 1978 on information technology, data files and civil liberties:

https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

(22) EU 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:

https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680#d1e950-89-1

(23) In particular, this processing is only authorised "subject to the provision of appropriate safeguards for rights and freedoms of the data subject" and solely "to protect the vital interests of the data subject or of another individual; or when the processing relates to data which are manifestly made public by the data subject".

(24) Commission nationale de l'informatique et des libertés (CNIL - French Data Protection Authority).
(25) (EU) Regulation 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 the free movement of such data, and repealing directive 95/46/CE (General Data Protection Regulation, GDPR): https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679

(26) Chapter 4, Section 3 of the GDPR

(27) With the entry into force of the GDPR, the upper limits of the administrative fines applicable by the supervisory authorities have increased significantly. In the event of a repeated infringement, they can reach up to 4% of the total worldwide turnover and up to €20 million. Article 83(6) of the GDPR.

(28) Paragraph 11 of Article 3 of Chapter 1 of GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes, by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

(29) Article 8 of the GDPR.

(30) https://www.lemonde.fr/societe/article/2019/02/18/nice-va-tester-la-reconnaissance-faciale-sur-la-voie-publique_5425053_3224.html

(31) The development of facial recognition algorithms requires a large quantity of data. The current regulatory provisions, drawn mainly from the GDPR, impose certain constraints on researchers and businesses carrying out research in this field in Europe. At present, this regulatory framework does not allow French players to compete globally. For example, it is impossible for them to use databases of images collected in foreign countries without the consent of the persons involved or to conserve databases of images obtained legally beyond the end of their study. These provisions therefore represent a significant hurdle to the development of these algorithms in France and Europe, whereas tech giants are able to compile extensive image databases without having to comply with these regulatory constraints. On 15 July 2019, the CNIL launched a public consultation on these issues in order to "allow for a better understanding of personal data processing in scientific research, clarify the applicable legal framework and develop suitable practical guides." Consideration should also be given to the possibility of putting in place European or French legal provisions permitting the use of the exemptions provided for in the GDPR, in order to allow research and innovation players in France to better position themselves to be more competitive internationally.

https://www.cnil.fr/fr/la-cnil-lance-une-consultation-publique-aupres-des-chercheurs-sur-les-traitements-de-donnees-des

(32) "Safe city" an adaptation of the "smart city" concept for security.

(33) https://www.cnil.fr/fr/la-cnil-appelle-la-tenue-dun-debat-democratique-sur-les-nouveaux-usages-des-cameras-video

(34) https://www.laquadrature.net/2019/06/21/le-vrai-visage-de-la-reconnaissance-faciale/

(35) https://www.lesechos.fr/tech-medias/hightech/en-chine-la-vie-sous-loeil-des-cameras-997774

(36) https://www.lemonde.fr/asie-pacifique/article/2018/04/11/en-chine-le-fichage-high-tech-des-citoyens_5283869_3216.html

https://www.franceinter.fr/monde/la-chine-distribue-des-bons-et-des-mauvais-points-a-ses-citoyens

(37) http://www.lefigaro.fr/flash-actu/pekin-utilise-la-reconnaissance-faciale-pour-surveiller-les-ouighours-presse-20190415

(38) Laurent Mucchielli specifies, "new technologies in general, and security technologies in particular, are subject to very powerful collective beliefs and perceptions in our societies today. This contributes to a certain credulity and naivety which leads people to naturally believe that the technological innovations proposed by industry and certain politicians are inherently good or of interest; they necessarily represent progress. *But this reasoning is flawed. Technology is neither good nor bad in and of itself. It all depends on how we choose to use it, and the financial decisions behind our choices." Extracts from* "Note sur l'évaluation des nouvelles technologies de sécurité. Cas de la vidéosurveillance et de la reconnaissance faciale"*(Note on the Assessment of New Security Technologies. The Case of Video Surveillance and Facial Recognition Technology): https://halshs.archives-ouvertes.fr/halshs-02178394 .*

(39) The first meeting, in which the rapporteur took part, was held on 26 June 2019: https://cnnumerique.fr/regulation_reconnaissance_faciale

(40) https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/

(41) For example, Microsoft is committed to developing facial recognition tools in a transparent way by involving independent organisations in controlling its algorithms and making the results available publicly:
https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

(42) For its part, the internet giant has made a commitment to ensure the scientific excellence of the devices it develops and not to reinforce societal biases. Furthermore, Google Cloud has decided not to offer general-purpose facial recognition tools before it has resolved certain questions related to technical aspects or to conditions for using these devices:

https://blog.google/technology/ai/ai-principles/ ; https://www.blog.google/around-the-globe/google-asia/ai-social-good-asia-pacific/

(43) At present, there is no evidence that it is impossible for the original faces to be recomposed ("unblurred") using more or less sophisticated video processing techniques. https://brighter.ai/

(44) Since these tools must be supplemented in order to become operational, according to Amazon, the persons in charge of integrating the tool and of processing are responsible.

(45) The United States is carrying out several research projects in this area: controlling access to military bases, "smart" sight, drones etc: https://www.military.com/daily-news/2019/06/01/armys-next-infantry-weapon-could-have-facial-recognition-technology.html

(46) The British police already use facial recognition technology in public places in order to find wanted individuals. The cost of the widespread use of facial identification been estimated at £500 million (approximately €550 million), which amounts to £10 per person identified. The use of this technology is not limited to internal security, but also extends to access to financial and government services and to certain airports.

(47) In addition to the test during the Notting Hill Carnival, the MPS also carried out an experiment in the very busy Stratford station.

(48) This strategy limits the cases in which facial recognition can be used (law enforcement, passport control and national security in the case of related legislation) and is accompanied by the creation of independent regulatory bodies, such as the recently created Law Enforcement Facial Images and New Biometrics Oversight and Advisory Board, which oversees the use of this technology by law enforcement agencies. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/720850/Home_Office_Biometrics_Strategy_-_2018-06-28.pdf

(49) Parliamentary Office of Science & Technology (POST): https://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0578

*(50)The purpose of the Commercial Facial Recognition Privacy Act (*https://www.congress.gov/bill/116th-congress/senate-bill/847/text*) is to oversee the commercial use of facial recognition, control the performance of systems available on the market and require companies to obtain individuals' consent.*

(51) These tests should then make it possible to develop a sustainable legal framework which would be operational at the latest by the 2024 Olympic Games in Paris, which could serve as a full-scale demonstration.

(52) Privacy by design: guarantee that privacy is integrated in new applications starting from the design stage.

(53) In the area of telephony, the Autorité de régulation des communications électroniques et des postes *(ARCEP - French Electronic Communications and Postal Regulatory Authority) has put in place a "sandbox" approach, giving certain stakeholders the opportunity to carry out tests while exempting them from certain rules.*

(54) Report by Member of Parliament Cédric Villani, commissioned by the Prime Minister: "Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne" (For a Meaningful Artificial Intelligence: Towards a French and European Strategy) (March 2018).

https://www.aiforhumanity.fr/