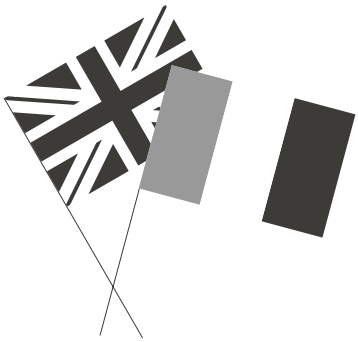
RENAISSANCE numerique

CIVIL LIBERTIES AND ETHICS
JUNE 2021

Regulation of facial recognition technologies:

A COMPARATIVE ANALYSIS OF FRANCE AND THE UNITED KINGDOM



On 21 April 2021, the European commission unveiled its proposal for a regulation of the various use cases of artificial intelligence (AI) technologies within the European Union[1], including facial recognition technologies (FRTs). FRTs are based on artificial intelligence methods that apply so-called "deep learning" techniques using biometric databases. They can be used for authentication (for instance verifying one's identity by recognising one's face) and identification (for example, linking an identity to a given face among a database of known faces) purposes. Facial recognition technologies have become part of citizens' everyday life through different experiences, from unlocking one's smartphone with one's face to automatically identifying friends on pictures posted on social media. There are many potential applications for these technologies, be it for security purposes (border security, unlocking smartphones, online payments, access to public services...), marketing (targeted advertising), or even recreational purposes (face swapping, identification on social media posts)[2].

In its legislative proposal, the European commission chose to opt for a risk-based approach that categorises AI technologies depending on three levels of risk: unacceptable, high or low. Accordingly, four AI applications are forbidden by the proposal, as the Commission considers they bear an unacceptable level of risk. For instance, it is the case for real-time remote biometric identification systems in publicly accessible spaces for the purpose of law en-

1 European Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Unions Legislative Acts", COM(2021) 206 final, 21 April 2021: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence

2 For more information, see Renaissance Numérique (2020), "Facial recognition: Embodying European values", 103 pp.: https://www.renaissancenumerique.org/system/attach_files/files/000/000/235/original/report_facial_recognition.pdf?1592553217

forcement (article 5(1)(d)), which European executives have deemed contrary to the European Union's values[3]. However, the proposal includes three relatively large exceptions to this ban. For example, police forces will be able to use such technologies to identify victims of criminal offenses, including missing children, to locate victims or suspects of criminal acts that can entail prison sentences of at least three years' time, or to prevent a threat to the life or safety of others or in the event of a terrorist attack. Concerning the other use cases of AI services that require remote biometric identification — uses in the private sector for instance —, the European commission proposes to classify them in the category of high-risk applications[4]. Their use can thus be authorised under certain guarantees, notably the creation of a risk management system (article 9), a minimal level of quality of the data used to train the algorithms (article 10), an obligation of transparency and information towards users (article 13) and human supervision (article 14).

The necessity of supervising the deployment of facial recognition technologies in order to protect the fundamental rights and freedoms of European citizens is at the heart of current debates. Indeed, more and more civil society actors — such as those who launched the *Reclaim Your Face* campaign[5] — are denouncing the highly intrusive aspect of these technologies. Albeit forbidding, in principle, the processing of biometric data, the General Data Protection Regulation (GDPR)[6] comprises many exceptions. In a report published in June 2020[7], Renaissance Numérique noted that even though a comprehensive legal framework already exists, its enforcement remains fragmented and partly inefficient, thus endangering European citizens' rights.

In line with previous works on this matter, the think tank organised a seminar on 21 February 2021, aiming at establishing a comparative analysis of the uses of FRTs in two European countries: France and the United Kingdom (UK). This European seminar was prepared in partnership with the British Embassy in Paris and law firm Pinsent Masons, and brought together around fifty private and public actors, members of civil society and researchers. Comparing France and the United Kingdom's uses and regulation of facial recognition technologies proves interesting in several ways. On the one hand, debates around those technologies are now well entrenched in both countries (albeit being fairly recent). On the other hand, there are significant differences in the way those technologies are being deployed and regulated on both sides of the Channel.

This note is fuelled by the discussions that took place during the seminar, and

3 European Commission, *op. cit.*, p. 12.
4 *Ibid.*, Annex III, p.4.
5 See: https://reclaimyourface.eu/
6 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: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679
7 Renaissance Numérique (2020), *op. cit.*

questions the major issues when it comes to regulating facial recognition technologies in France, the United Kingdom, and Europe in a broader sense. The comparison allows us to imagine an appropriate regulatory framework to answer the challenges induced by such technologies.

The regulatory framework surrounding FRTs is in part influenced by the legal tradition of the country

Both in France and in the United Kingdom, facial recognition technologies are used in public and private spaces, and by public and private actors. In France for instance, public authorities use these technologies for the criminal records processing file (*traitement des antécédents judiciaires*, or TAJ), the system for rapid and secure crossing of external borders (*passage rapide et sécurisé aux frontières extérieures*, or PARAFE) and the certified online authentication on mobile phones (*authentification en ligne certifiée sur mobile*, or ALICEM)[8] system which gives access to public services online. There have also been experimentations of these technologies for security purposes across the French territory, such as during the Nice carnival in February 2019[9], or to access two public high schools in the PACA region[10]. In Marseille, a network of around fifty video protection cameras equipped with FRTs has been deployed[11] before the project was eventually suspended at the beginning of 2021[12]. These uses are contentious and several associations like *La Quadrature du Net* and the *Ligue des droits de l'Homme* mobilised against these practices. Contrary to France, where such uses remain partly experimental, facial recognition tools destined to surveillance and based on real biometric databases have been used on a much wider scale in the United Kingdom. This has raised privacy concerns, notably in terms of obtaining individuals' consent to the scanning of their faces. Back in 2019, the King's Cross scandal, in London, revealed that a real estate developer scanned the faces of people in the streets

8 To learn more about ALICEM, see: https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee

9 "Nice: La reconnaissance faciale testée sur la voie publique, au Carnaval, une première en France", *20 minutes*, 18 February 2019: https://www.20minutes.fr/nice/2454127-20190218-video-nice-reconnaissance-faciale-testee-carnaval-premiere-france

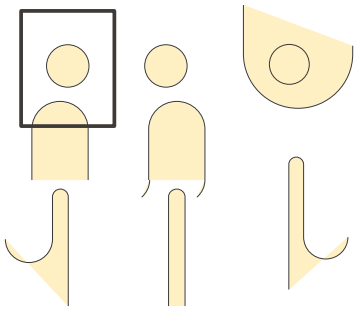
10 "Deux lycées de Marseille et Nice vont tester la reconnaissance faciale", *Le Figaro*, 17 December 2018: https://www.lefigaro.fr/actualite-france/2018/12/17/01016-20181217ARTFIG00207-deux-lycees-de-marseille-et-nice-vont-tester-la-reconnaissance-faciale.php

11 "Marseille : la vidéoprotection «intelligente», comment ça marche", *France 3 Provence Alpes Côte d'Azur,* 5 February 2021: https://france3-regions.francetvinfo.fr/provence-alpes-cote-d-azur/bouches-du-rhone/marseille/marseille-la-videoprotection-intelligente-comment-ca-marche-1941052.html

12 The new municipal administration, which wasn't in power at the start of the project, suspended it in order to lead an audit to determine the relevance and efficiency of the system.

without their consent, and cooperated with the police to identify people they were looking for. The Information Commissioner's Office (ICO)[13] is currently investigating the use of facial recognition that was made in this specific case[14] and called onto the government to adopt a code of conduct on this kind of uses[15]. Moreover, these technologies are, in the United Kingdom, more frequently used by private actors than in France. For instance, some supermarkets scan the faces of entering clients to check if they are identified on a list of suspects. Facial recognition technology systems have also been deployed during massively crowded events in the UK, like concerts or rugby and football matches, for instance during the 2017 UEFA Champions League final in Cardiff.

In the wake of these growing uses, a public debate is emerging on both sides of the Channel as to how these technologies should be regulated. In the United Kingdom, this discussion is fairly recent and has been halted by the Covid-19 pandemic. Lord Clement-Jones introduced a bill on 4 February 2020, which forbids the use of automatic FRTs in public spaces and requires an independent authority to conduct an assessment of such technologies within a year. This evaluation would encompass the following aspects: the implications of these technologies in terms of human rights, equality and data protection, the quality and accuracy of the technologies and the adequacy of the existing regulatory framework. This bill is currently being examined in its second reading at the House of Lords[16]. However, it concerns exclusively public uses of facial recognition technologies. Use cases are hence treated separately between the public and private sector, which entails an absence of comprehensive policy on the matter in the United Kingdom.



In France, the debate has been on the rise as global sports events like the 2023 men's rugby World Cup and the Paris 2024 Olympics are approaching. The organisers of these events envision FRTs as tools to secure access to the different venues[17], which would open the door to experimentations on much bigger scales than what has been done in France until now. Concerning this particular purpose, especially for the Olympics[18], the *Commission nationale de l'informatique et des libertés* (the CNIL, France's data protection authority) does not rule out the possibility of a giving a favourable notice, under certain conditions. However, the subject has been left aside in the debates surrounding the so-called "Sécurité globale" (*global security*) bill as the ma-

13 See the ICO's website: https://ico.org.uk/about-the-ico/

14 ICO, "Statement: Live facial recognition technology in King's Cross", 15 August 2019: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/

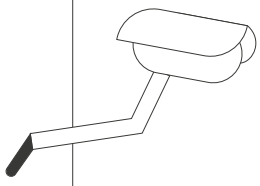
15 ICO, "ICO investigation into how the police use facial recognition technology in public places", 31 October 2019, pp. 36-37: https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

16 UK House of Lords, "Automated Facial Recognition Technology (Moratorium and Review) Bill", 4 February 2020: https://bills.parliament.uk/bills/2610

17 "Reconnaissance faciale : les expérimentations se multiplient avant les J.O de Paris", *Radio France*, 5 September 2020: https://www.francetvinfo.fr/economie/emploi/metiers/armee-et-securite/reconnaissance-faciale-les-experimentations-se-multiplient-avant-les-j-o-de-paris_4095193.html

18 *Ibid.*

jority in Parliament has been divided on whether to use these technologies as part of law enforcement[19]. In this context, MP Didier Baichère presented, at the beginning of May 2021, a bill introducing an "*experimentation and consultation on facial recognition technologies based on artificial intelligence*"[20]. This text aims at building a "transparent and ethical" experimentation framework for FRTs using AI. It also establishes the launch of a public consultation designed to "*foster a civic and educational debate and evaluate how the French people perceive this issue and what constitutes a red line for them*"[21]. Apart from these national initiatives, the goal for France in the coming months will also be to incorporate the European approach promoted in the future AI regulation, in its own policy orientations.



Even though there are multiple use cases for these technologies (security, but also marketing and even recreational purposes), the debates tend to focus specifically on the surveillance purpose of facial recognition technologies (albeit the other use cases are not risk free). It is actually around this very aspect that discussions focused during the seminar on 21 February 2021. On this issue, it has been highlighted during the event that up to now, French authorities have been more cautious than the United Kingdom's when it comes to deploying facial recognition technologies for surveillance purposes. The United Kingdom is the first European country to rely on FRTs fuelled by real biometric databases in its public spaces, whereas in France, such technologies have only been deployed within experimentations limited in time and space. Moreover, said experimentations only took place obtaining the consent of the concerned persons, as was the case, for instance, during the February 2019 Nice Carnival[22]. Furthermore, the *Conseil d'État* (France's Supreme Court) has recently forbidden the use of drones carrying facial recognition devices in public spaces for the purpose of controlling the respect of the covid-related lockdown measures[23]. Also, by ruling against a digital access system used in two high schools in Marseille and Nice, Marseille's administrative Court aligned itself on the CNIL's position on the matter[24], pointing out that other, equally efficient, access control systems already existed[25].

It seems that the French authorities are more reluctant than their British

19 Les Jeux olympiques ouvrent la voie aux technologies sécuritaires", *Reporterre*, 16 March 2021: https://reporterre.net/Les-Jeux-olympiques-ouvrent-la-voie-aux-technologies-securitaires

20 Assemblée nationale, "Proposition de loi d'expérimentation créant un cadre d'analyse scientifique et une consultation citoyenne sur les dispositifs de reconnaissance faciale par l'intelligence artificielle", 4 May 2021: https://www.assemblee-nationale.fr/dyn/15/textes/l15b4127_proposition-loi.pdf

21 Didier Baichère, press release, "Publication de ma proposition de loi d'expérimentation et de consultation sur les dispositifs de reconnaissance faciale par l'intelligence artificielle", 7 May 2021: https://www.didierbaichere.fr/blog/publication-de-ma-proposition-de-loi-d-experimentation-reconnaissance-faciale

22 "Expérimentation de reconnaissance faciale : Nice ravie, la Cnil sceptique", *Le Journal du Net*, 28 August 2019: https://www.journaldunet.com/economie/services/1443319-reconnaissance-faciale-nice-ravie-la-cnil-sceptique/.

23 Conseil d'État, "Avis relatif à l'usage de dispositifs aéroportés de captation d'images par les autorités publiques», 18 July 2020: https://www.conseil-etat.fr/ressources/avis-aux-pouvoirs-publics/derniers-avis-publies/avis-relatif-a-l-usage-de-dispositifs-aeroportes-de-captation-d-images-par-les-autorites-publiques

24 CNIL, Avis sur l'expérimentation de la reconnaissance faciale dans deux lycées, 29 October 2019: https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

25 Administrative Court of Marseille, 9th ch., ruling of 27 February 2020: https://www.legalis.net/jurisprudences/tribunal-administratif-de-marseille-9eme-ch-jugement-du-27-fevrier-2020/

counterparts to use facial recognition technologies for security purposes. Indeed, the participants in the seminar convened that when the British judges condemn a certain practice, it is generally more out of concern for personal data privacy or disrespect of the non-discrimination principle, rather than out of concern about using FRTs for security reasons *per se*. This is notably reflected in the Court of appeal's decision on the use of facial recognition technologies by the South Wales Police department[26]. In this case, the ICO stated in its investigative report that data collection should be proportionate, relevant and appropriate, which was not the case here as the South Wales Police department's lists of suspects were particularly large[27]. Even though the Court of appeal judged that the police was wrong to consider that the personal data of persons outside of surveillance lists were public, it still mentioned the interest of using facial recognition technologies[28].

When it comes to facial recognition technologies being used for surveillance purposes, British authorities sometimes have a less strict reading of the GDPR rules, especially concerning the principle of proportionality. In the United Kingdom, the use of FRTs is generally authorised as long as the biometric data is collected in a specific area, for a limited period and is destroyed when the latter ends. This approach entails more flexible legal rulings in the United Kingdom and reveals the existing cultural differences when it comes to regulating these technologies in France and in the United Kingdom.

Beyond the legal aspects related to the use of such technologies, there are larger cultural differences that must be considered. Even though France has seen a surge in the number of CCTV devices being deployed, they are still much more developed in the United Kingdom. Also, the United Kingdom's decentralised structure sometimes entails different approaches to the subject, depending on the territory. For example, Scotland is much more reluctant than England to use facial recognition technology for its policing in the name of the precautionary principle.

---

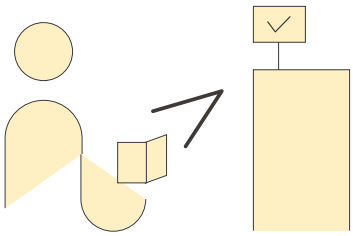
26 Court of appeal, R (Bridges) v-Chief Constable of South Wales Police & Ors, 11 August 2020: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

27 ICO, "ICO investigation into how the police use facial recognition technology in public places", 31 October 2019, pp. 16-17 and p. 25: https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf

28 *Ibid.*, p. 30.

Using facial recognition technologies requires safeguards that go beyond technical criteria

In order to regulate them in the best possible way according to the place we want to make for them in our society, it is necessary to clearly identify the risks and opportunities that come with the use of facial recognition technologies. As noted by certain participants in the seminar, they may offer some advantages. Biometric data cannot easily be stolen nor forgotten, contrary to a password for example. Therefore, FRTs based on such data can diminish the risk of identity theft in online banking or administrative procedures. Moreover, facial recognition technologies may be particularly efficient for certain tasks, such as identifying people at border control posts or using online banking services. Facial recognition technologies' effectiveness and security are two arguments that are often used to justify their use.



However, the very nature of FRTs carries many risks, as the algorithms that power them can never be 100 % reliable. Several studies have shown that the latter reproduce our social biases[29] (racism, sexism, ageism), subsequently entailing important discrimination risks such as access denial to a service or even abusive arrests. Therefore, although the technological reliability of facial recognition technologies is often put forward by those who use it, those technologies are not, and never will be, completely trustworthy.

And even if they were 100 % reliable, completely free of any social bias, choosing to use FRTs raises questions that go way beyond technical issues. Indeed, many people question the compatibility of these technologies with the fundamental rights and liberties of the individuals to which they are applied, especially in terms of legality, necessity and proportionality. One of the major difficulties brought by these technologies concerns individuals' consent, which is particularly hard to obtain, especially in public spaces. In this regard, having an obligation of transparency and information towards citizens, and informing them that their biometric data is likely to be collected, appears essential. Although a legal framework dealing with personal data protection[30] exists in the UK, difficulties in its application can occur. Moreover, the different existing legislations do not encompass all the potential cases of harm, such as the question of biometric data confidentiality in high-risk situations.

---

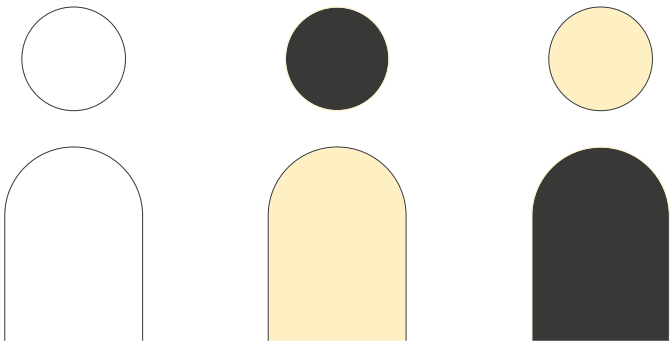
29 See for instance the "*Gender Shades*" project by the Massachusetts Institute of Technology (MIT), 2018: http://gendershades.org/overview.html

30 Among the most important ones are the Human Rights Act of 1998, the Investigatory Powers Act of 2016 or the Data Protection Act of 2018.

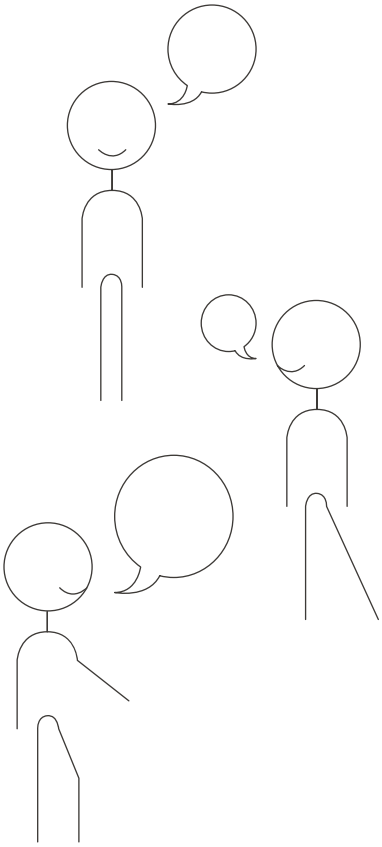
When badly used, facial recognition technologies can jeopardise human dignity because of their intrusive nature, as well as violate the right to be free of discrimination, and infringe on freedom of speech and association or the right to a good administration[31]. Hence, the technical performance of FRTs is not a sufficient criterion to justify the necessity and proportionality of their use. It is thus essential to design safeguards that go beyond mere technical criteria — like an algorithm's level of precision — in order to guarantee the protection of citizens' fundamental rights and freedoms.

During the seminar, some participants suggested that these safeguards could come in the form of independent regulatory bodies tasked with evaluating the quality of facial recognition devices (before and after their deployment), putting in place control mechanisms and authorisation procedures, and regulating biometric data collection and processing. It was also mentioned that, considering how sensitive these technologies are and the variety of use cases, it is necessary to analyse them before they are rolled out, and on a case-by-case basis. Among the different arguments, there is the idea that such a risk-assessment framework would make it possible to go further than the data protection impact assessments (DPIA) imposed in the GDPR. In a way, the approach that the European Commission put forward in its proposed regulation on AI follows this direction. Indeed, European executives suggest that AI-powered remote biometric identification systems should undergo an *ex-ante* conformity assessment conducted by a certified organisation.

Still, there is no consensus at the moment regarding which organisation should be responsible for these evaluations and how they should proceed. It should be noted, however, that to be efficient, these organisations should be independent, unbiased and should edict clear and unambiguous advice that may not be subject to differing interpretations.



31 European Union Agency for Fundamental Rights, "Facial recognition technology: fundamental rights considerations in the context of law enforcement", 21 November 2019, 34 pp.: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law



The regulation of facial recognition technologies must take into account their collective impact on society

Using facial recognition technologies impacts all aspects of society, hence the necessity of thinking about their supervision beyond individual consequences that generally revolve around the issue of personal data protection. In order to involve citizens more in the decision-making process in the United Kingdom, a public consultation was launched by the Ada Lovelace Institute, an independent research centre that has been working on biometric technologies and facial recognition technologies. According to a study led by the institute in September 2019, 55 % of the citizens who responded want restrictions on the use of FRTs by police forces[32], and an important part of society distinguishes legitimate use cases from others deemed illegitimate, such as using these technologies in transportation or schools. In the wake of these observations, the Ada Lovelace Institute created the Citizen's Biometric Council[33], a deliberative body made of around fifty citizens representative of British society. After many debates with various experts, the members of this council proposed a series of measures aiming at rendering the use of biometric technologies "trustworthy": a more comprehensive framework, independent authorities to provide oversight, and ensuring the respect of minimum standards regarding the deployment of these technologies[34].

This example shows that sharing information with citizens and making them a part of the debate allows for enlightened choices for society. Informing the public thus appears to be a priority as well as putting in place deliberative processes where FRT industry players can exchange views with researchers, representatives from civil society, regulators and citizens.

32 Ada Lovelace Institute, "Beyond face value: public attitudes to facial recognition technology", September 2019, 23 pp.: https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/

33 See the presentation of the "Citizens' Biometrics Council" on the website of the Ada Lovelace Institute: https://www.adalovelaceinstitute.org/project/citizens-biometrics-council/

34 Ada Lovelace Institute, "The Citizens' Biometrics Council — Recommendations and findings of a public deliberation on biometrics technology, policy and governance", March 2021, p. 3: https://www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Citizens_Biometrics_Council_final_report.pdf

Towards an open debate featuring multiple stakeholders

The comparative study of France and the United Kingdom around the deployment and regulation of facial recognition technologies reveals different uses in both countries, which are derived from political, social, cultural and legal differences. It appears clear that the regulation of these technologies should not only take into account their technical efficiency, but also their ability to comply with citizens' fundamental rights and freedoms. In this respect, a case-by-case evaluation by an independent authority could be part of the solution. As the European Commission just issued a proposal aimed at framing various uses of AI — which authorises several use cases of FRTs —, the moment has come to build a coherent and collective vision of the way they should be regulated.

—

Authors

Jessica Galissaire, Studies Manager, Renaissance Numérique

Audrée Latinaud, Project Assistant, Renaissance Numérique

—

Proofreading

Jennyfer Chrétien, Executive Director, Renaissance Numérique

Pol-Euan Lacombe, Project Assistant, Renaissance Numérique

Guillaume Morat, Senior Associate, Pinsent Masons

—

Renaissance Numérique thanks the British Embassy in Paris and Pinsent Masons Law Firm for their support in organising the seminar "Facial Recognition Technologies: Comparative views from across the Channel" on 11 February 2021.

The think tank also thanks all those who participated in this seminar and contributed to the reflexions contained in this note, particularly Tom Barry, Minister Counsellor for European and International Affairs at the British Embassy in Paris, Théodore Christakis, Professor (Dr.) of International and European Law and Chair 'Legal and Regulatory Implications of Artificial Intelligence' at Grenobles Alpes University, Benedict Dellot, Manager for AI surveillance at the Centre for Data Ethics & Innovation, Claire Edwards, Partner at Pinsent Masons, Stephanie Hare, Independent researcher specialised in tech, Irina Orssich, Team Leader on AI in the "AI & Digital Industry" Directorate of the European Commission's DG CNECT, Hetan Shah, Co-chair of the Ada Lovelace Institute, and Camille Vaziaga, Public Affairs Manager for France at Microsoft.