Global Campus
Europe

Policy Briefs
2020

Diego Naranjo

Your face rings a bell. How facial recognition poses a threat for human rights

Supported by

Table Of Contents

Your face rings a bell. How facial recognition poses a threat for human rights

Diego Naranjo

INTRODUCTION / EXECUTIVE SUMMARY

'The greatest danger still lies ahead, with the refinement of artificial intelligence capabilities, such as facial and pattern recognition.'[1] (Edward Snowden)

In 2013, Edward Snowden published historical revelations about mass surveillance by the National Security Agency (NSA) that caused an uproar on the political class, the media and the general population. The Snowden revelations brought to light the most invasive and extensive mass surveillance capabilities by a government known to date, one that we would have only expected to be reserved for the most tyrannical governments in a dystopian future. On the bright side, these revelations increased the awareness of privacy and data protection rights and accelerated the discussions on the General Data Protection Regulation[2] in the European Union (EU), strengthening the arguments of privacy and data protection activists. Moreover, the revelations also added new views on whether, in the race of the so-called 'war on terror', intelligence services had gone just too far.

Since then, public authorities in Europe and elsewhere[3] have expressed the need to reinforce privacy and data protection rights, and analyse the counterbalances of intelligence services with fundamental rights safeguards. Years after the Snowden revelations came out, stories started to appear in the media about the use of technologies in China that used invasive biometric[4] recognition pat-

[1] Ewen McAskill, 'Edward Snowden interview' (*The Guardian*, 13 September 2019) <https://www.theguardian.com/us-news/ng-interactive/2019/sep/13/edward-snowden-interview-whistleblowing-russia-ai-permanent-record> accessed 15 March 2020.

[2] Regulation (EU) 2016/679 (General Data Protection Regulation).

[3] Convention 108+ of the Council of Europe (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe ETS No 108)). This convention can be signed and ratified by countries from all around the world, and many countries are doing so: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>, accessed 6 June 2020.

[4] Biometrics data is defined as 'personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic [fingerprint] data'. Consolidated text: Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the

terns for apparent 'convenient' uses in ATMs[5] or, sometimes more bluntly, directly designed to suppress human rights and legal dissent.[6] The general tone of the news from the Western media regarding the use of face recognition systems and biometrics, especially if the news related to the deployment of social score systems in China, was of (understandable) alarm. The underlying idea that no one had to even mention is that something even remotely like that could not happen in advanced democracies.[7] Today, around 15 European countries[8] have deployed (in trial or full phase) facial recognition systems and other biometric technologies used for live remote identification in publicly accessible spaces.[9] When initially deployed, these systems escaped the attention of the media. But, around February 2019, the first scandals started to emerge in Europe[10] and the United States (US).[11] In the US several cities (Oakland, Berkeley, Somerville, Massachusetts, San Francisco and others[12]) banned such practices. In Europe, where generalised data protection, privacy laws and specialised human rights courts exist, the response was silence. The only exception to this radio silence happened, paradoxically, when these systems were under threat. When a leak of the European Commission (EC) Artificial Intelligence White Paper considered to launch a similar ban in the EU (only to be discarded a few lines later in the same document)[13] the topic became something worth discussing for a couple of weeks.

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 , Law Enforcement Directive art 3(13); 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 (General Data Protection Regulation) (General Data Protection Regulation (Regulation 2016/679) art 4(14); Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, Data Protection Regulation for EU institutions art 3(18).

[5] Charlotte Middlehurst, 'China unveils world's first facial recognition ATM' (*The Telegraph*, 1 June 2015) <https://www.telegraph.co.uk/news/worldnews/asia/china/11643314/China-unveils-worlds-first-facial-recognition-ATM.html> accessed 15 March 2020.

[6] Gilles Sabrie, 'Behind the Rise of China's Facial-Recognition Giants' (*Wired*, 9 March 2019) <https://www.wired.com/story/behind-rise-chinas-facial-recognition-giants/> accessed 15 March 2020.

[7] Darlene Storm, 'ACLU: Orwellian Citizen Score, China's credit score system, is a warning for Americans' (*Computer World*, 7 October 2015) <https://www.computerworld.com/article/2990203/aclu-orwellian-citizen-score-chinas-credit-score-system-is-a-warning-for-americans.html> accessed 15 March 2020.

[8] A map of existing face recognition systems can be accessed here: Electronic Privacy Information Center (EPIC), 'Ban Facial Surveillance' (*EPIC*) <https://epic.org/banfacesurveillance/> accessed 10 May 2020. The list might not be entirely up to date, due to the lack of transparency around the deployment of those systems.

[9] Some other uses which are not under this specific scope are also worrying, such as the use of facial recognition to evaluate access to rent subsidies. See José Gómez-Serranillos, 'RentCOVID-19: una tecnología de reconocimiento facial para revisar miles de solicitudes de ayudas al alquiler' (*Expansion*, 15 April 2020) <https://www.expansion.com/juridico/actualidad-tendencias/2020/04/13/5e94167f468aeb53128b45c6.html>, accessed 15 March 2020. However, these cases are not under the scope of this paper.

[10] Le Monde avec AFP, 'Nice va tester la reconnaissance faciale sur la voie publique' (*Le Monde*, 18 February 2019) <https://www.lemonde.fr/societe/article/2019/02/18/nice-va-tester-la-reconnaissance-faciale-sur-la-voie-publique_5425053_3224.html> accessed 15 March 2020.

[11] Kate Conger, Richard Fausset and Serge F Kovaleski, 'San Francisco Bans Facial Recognition Technology' (*The New York Times*, 14 May 2019) <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html> accessed 15 March 2020.

[12] Abdullah Hasan, '2019 Proved We Can Stop Face Recognition Surveillance' (*ACLU*, 17 January 2020) <https://www.aclu.org/news/privacy-technology/2019-was-the-year-we-proved-face-recognition-surveillance-isnt-inevitable/> accessed 15 March 2020.

[13] Samuel Stolton, 'LEAK: Commission considers facial recognition ban in AI "white paper"' (*Euractiv*, 17 January 2020) <https://www.euractiv.com/section/digital/news/leak-commission-considers-facial-recognition-ban-in-ai-white-paper/> accessed 15 March 2020.

The debate in the media in the EU has gone from initial discontent (especially for foreign practices) to silence. Initially, reporting on the use of facial recognition used the scenario of Hong Kong protestors being subject to face surveillance as a sign of Chinese lack of democratic values.[14] Smoothly, and without any transition or self-criticism about what they had reported days or weeks earlier regarding the use of the same technologies by Chinese authorities, barely any dissenting voices were audible from European media and policy makers regarding the deployment and public investment[15] in similar technologies in Europe. These double-standards (one for us, one for the rest) are symptoms of the normalisation of the shrinking of the civil space[16] in Europe and elsewhere. In times of widespread discontent and where legitimate dissent groups are being put in the category of extremist groups, from animal defence groups to environmentalist activists of Extinction Rebellion,[17] this is a concerning development of our system of values, laws and checks and balances. Under the current COVID-19 pandemic crisis, we risk moving to a dystopian COVID-1984 where emergency laws and abusive measures are put in place under the best of the intentions, and the worst of the unintended consequences.

In our increasingly interconnected societies it is of utmost importance and urgency that Europe prevents the deployment of remote face recognition and other biometric surveillance and identification technologies. Because of its potential threat specifically on freedoms of association and assembly, freedom of religion, rights to privacy and data protection and other fundamental rights, regional exemplary action in Europe banning these practices is urgent in order to avoid the normalisation of such practices across the entire continent, and from then for the rest of the world. Because, if Europe develops these practices, and they are not banned, oppressive regimes around the world will feel it to be legitimate to use them as well. If they are prompted to not do so because of potential threats to human rights, they could just point the finger back at Europe and say: If they use it, why not us?

PROBLEM DESCRIPTION

As of today, the US-based NGO Electronic Privacy Information Center (EPIC) has documented at least 15 face recognition systems deployed (in full or in a trial phase) in Europe.[18] Because of the lack of transparency of these systems, more of them might be in use or being planned. Opposition to those systems is clear from UN Special Rapporteurs,[19] data protection authorities[20] and the EU Fundamental Rights Agency (FRA), along

[14] An interesting piece is this one, where from criticising uses in Hong Kong goes to recognise the support of the use (of course for ‘serious crimes and terrorism’): Zak Doffman, ‘Hong Kong exposes both sides of China’s relentless facial recognition machine’ (*Forbes*, 26 August 2019) <https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/> accessed 15 March 2020.

[15] Privacy International, ‘MONITORYOU: the MilliONs beIng spenT by the eu on develOping surveillance tech to taRget YOU’ (*Privacy International*, 20 January 2020) <https://privacyinternational.org/node/3341> accessed 15 March 2020.

[16] Chris Stone, ‘Why the space for civic engagement is shrinking’ (*Open Society Foundations*, 21 December 2015) <https://www.opensocietyfoundations.org/voices/why-space-civic-engagement-shrinking> accessed 15 March 2020.

[17] Vikram Dodd and Jamie Grierson, ‘Non-violent groups on UK counter-terror list threaten legal action’ (*The Guardian*, 22 January 2020) <https://www.theguardian.com/environment/2020/jan/22/minister-denies-government-considers-extinction-rebellion-extremist> accessed 15 March 2020.

[18] EPIC (n 8).

[19] EU Fundamental Rights Agency (FRA), ‘Facial recognition technology: fundamental rights considerations in the context of law enforcement’ (FRA 2020) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf> accessed 15 March 2020; Patrick Williams and Eric Kind, ‘Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe’ (European Network Against Racism (ENAR) 2019) <https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf> 16 accessed 15 March 2020; European Commission, ‘On Artificial Intelligence - A European approach to excellence and trust’ (COM(2020) 65 final 19 February 2020) <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 15 March 2020.

[20] According to the FRA eight out of ten people are against sharing their facial image with authorities. Source: FRA, (3

with civil rights groups. All of them have raised concerns about the use of facial recognition systems and other biometric technologies used for live remote identification in publicly accessible spaces. By not reacting quickly and strongly to this threat, we risk normalising mass surveillance and providing an example for the rest of the world that would get away using these same technologies to attack human rights defenders.

RATIONALE FOR ACTION

At the time of writing of this paper, at least 15 European states have implemented in trial or full implementation forms face recognition systems. It is not clear what the legal basis is in European or national law for the deployment of those systems, as well as whether data protection impact assessments were done before deploying them.[21] The population, which in the EU is clearly in opposition to the deployment of these measures,[22] is mostly unaware of the reach of the deployment of facial recognition systems that are already in place.

Some of the few institutional voices in the EU that have raised concerns about these systems are the European Data Protection Supervisor (EDPS),[23] the French Data Protection Authority CNIL[24] and, more timidly, the EC in their Artificial Intelligence (AI) White Paper.[25] Despite these voices and the publication of a detailed FRA Focus Paper on this topic,[26] little (if anything) seems to make state authorities concerned and consider pausing or cancelling current practices, not to mention abort the deployment of new biometric systems. Given the current lack of institutional action to ban such practices (from national governments and European institutions), it is of utmost importance for human rights defenders to act now, as the lack of action could lead to mainstreaming mass surveillance in our already digitally controlled societies.

POLICY OPTIONS AND RECOMMENDATIONS

We are at a crossroad regarding the use of these technologies. Decades ago, video surveillance/closed-circuit television (CCTV) cameras were implemented ferociously all over the world with the alleged goal of deterring (poverty-related or violent) crimes. Despite criticism from human rights groups, cameras were deployed just because the technology was available and no comprehensive law would stop them. Now those same systems can be re-programmed[27] to allow those cameras to go one step beyond from the mere capturing and recording of images to live recognition of individuals, their 'feelings' or other patterns that may be considered 'useful' for law enforcement purposes or any other goals.

The use of face recognition and other biometrics live recognition systems do not only affect the fundamental rights to data protection and privacy. FRA has described[28] some of the risks associated with the use of such systems such as

March 2020) <https://twitter.com/EURightsAgency/status/1234804039449239553>, accessed 15 March 2020.

[21] The face recognition system in the Brussels National Airport started functioning in 2016 without previously preparing a data protection impact assessment, for example.

[22] FRA (n 20).

[23] Wojciech Wiewiórowski, European Data Protection Supervisor (EDPS), 'AI and Facial Recognition: Challenges and Opportunities' (*EDPS*, 21 February 2020) <https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en> accessed 15 March 2020.

[24] Commission Nationale de l'Informatique et des Liberté (CNIL), 'Reconnaissance faciale : pour un débat à la hauteur des enjeux' (*CNIL*, 15 November 2019) <https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux> accessed 15 March 2020.

[25] European Commission (n 18).

[26] FRA (n 19).

[27] Williams and Kind (n 19).

[28] FRA (n 19) 20: 'People may feel uncomfortable going to public places under surveillance. They may change their behaviour, withdrawing from social life, not visiting central places under surveillance, avoiding train stations or declining to attend cultural, social or sports events.'

its chilling effects, inadequate response from untrained police officers and discrimination.

The assessment of three UN Special Rapporteurs is not to be ignored, although that seems to be the case in the current absence of any meaningful debate at the European and national levels. The UN Special Rapporteur on Freedom of Association and Assembly Clément Voule expressed in his 2019 Report presented before the UN General Assembly that '[t]he use of surveillance techniques for the indiscriminate and untargeted surveillance of those exercising their right to peaceful assembly and association, in both physical and digital spaces, should be prohibited'.[29] The necessity and proportionality of such systems has also been put in question by the UN Special Rapporteur on the Right to Privacy Joseph Cannataci[30] and similar concerns have been raised about the impact on human rights defenders, journalists, politicians and UN investigators by UN Special Rapporteur on Freedom of Expression David Kaye.[31]

These converging opinions are not surprising. The use of face recognition systems disproportionately impacts and limits fundamental rights and, more generally, threatens the way we understand democracy. This includes how social relationships and interactions will occur (from strikes to women marches to migrant rights meetings), what the limitations for law enforcement and intelligence services in democratic societies should be, and what freedom of speech means in over-controlled environments.

Civil society has been vocal as well against the use of biometric surveillance systems. The Electronic Frontier Foundation (EFF)[32] in the US, Liberty[33] and Privacy International[34] in the UK, SHARE Foundation in Serbia[35] and European Digital Rights (EDRi)[36] in the EU, among many others,[37] have all denounced the arbitrary and abusive use of such systems and their impact on human rights. The US case is somewhat surprising in the sense that, despite the absence of general data protection legislation at the federal level, several cities and states have already banned facial recognition.[38] Meanwhile, in Europe, the situation is terribly quiet. The EC has gone from considering (and immediately dis-

[29] Special Rapporteur on the rights to freedom of peaceful assembly and of association, 'Report on the rights to freedom of peaceful assembly and of association: The Digital Age' (17 May 2019) A/HRC/41/41 15 <https://undocs.org/A/HRC/41/41> accessed 15 March 2020.

[30] Chris Burt, 'UN privacy rapporteur criticizes accuracy and proportionality of Wales police use of facial recognition' (*Biometric Update.com*, 3 July 2018) <https://www.biometricupdate.com/201807/un-privacy-rapporteur-criticizes-accuracy-and-proportionality-of-wales-police-use-of-facial-recognition> accessed 15 March 2020.

[31] United Nations Human Rights, Office of the High Commissioner, 'UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools' (*OHCHR*, 25 June 2019) <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736> accessed 15 March 2020.

[32] Electronic Frontier Foundation (EFF), 'Biometrics: Facial Recognition' (*EFF*) <https://www.eff.org/document/biometrics-facial-recognition> accessed 15 March 2020.

[33] Liberty, 'Resist facial recognition' (*Liberty*) <https://www.libertyhumanrights.org.uk/resist-facial-recognition>, accessed 15 March 2020.

[34] Privacy International, 'Facial Recognition' (*Privacy International*) <https://privacyinternational.org/learning-topics/facial-recognition> accessed 15 March 2020.

[35] Share Foundation, 'New surveillance cameras in Belgrade: location and human rights impact analysis – "withheld"' (*Share*, 29 March 2019) <https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/> accessed 15 March 2020.

[36] Ella Jakubowska, 'Facial recognition and fundamental rights 101' (*EDRi*, 4 December 2019) <https://edri.org/facial-recognition-and-fundamental-rights-101/> accessed 15 March 2020.

[37] La Quadrature du Net, 'Joint Letter from 80 organisations: Ban Security and Surveillance Facial Recognition' (*La Quadrature du Net*, 19 December 2019) <https://www.laquadrature.net/en/2019/12/19/joint-letter-from-80-organisations-ban-security-and-surveillance-facial-recognition/> accessed 15 March 2020.

[38] See the interactive map at Ban Facial Recognition, <https://www.banfacialrecognition.com/map/>. More information on the US cases can be found at Electronic Privacy Information Center (EPIC), 'State Facial Recognition Policy' (*EPIC*) <https://epic.org/state-policy/facialrecognition/>, accessed 15 March 2020.

carding)[39] a ban on facial recognition to asking for a 'debate'[40] on the use of these technologies. Outside the EU, Belgrade is deploying face recognition with Chinese technology using 1,000 cameras[41] while Chinese police officers support the local police on the ground.[42]

The inaction of authorities in Europe is worrisome for two reasons: first, and as it has already been stated in this paper, the permissive attitude on the use of biometric mass surveillance technologies cannot but accelerate the deployment of these technologies, building towards a 'normalisation' of technologies that not such a long time ago, when used in China, were used to depict the worst aspects of modern-day totalitarianism. Second, Europe is setting a terrible precedent for autocratic regimes that may buy these technologies and use them to crack legal dissent and point out to Europe and its criminalisation of dissent (under the disguise of criminalising only 'extremist groups'[43]) if accused of wrongdoing by governments.

Given this situation, we suggest European policy-makers to implement the following recommendations:

Stop current uses of surveillance biometric systems

According to article 52.1 of the EU Charter of Fundamental Rights[44] (the Charter) limitations to fundamental rights are '[s]ubject to the principle of proportionality' and they can be made only 'if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others'. Currently no comprehensive information is available about the justification (necessity, proportionality and sometimes even adequate legal basis[45]) of these systems. Therefore, member states must stop the use of existing facial recognition systems and other biometric technologies used for live remote identification in publicly accessible spaces (whether in trial or fully operational phases), dismantle them and block the deployment of new systems until their alignment with EU primary law, namely the Charter, is ensured. At the same time, cities (especially, but not only, those signatories of the Declaration of Cities for Digital Rights[46]) as the institutions which are closer to citizens and themselves sometimes with the capabilities to install or remove such systems, need to take a brave step forward to defend their citizens from these pervasive systems of mass surveillance deployed in their territories. Local and regional authorities, within their competences, should also enact laws or update existing ones to prohibit the use of these technologies and dismantle such systems when they are deployed under their competences. Finally, we advocate that once the specific legal instruments are in place that municipalities make such steps public by declaring the geographical area they govern as 'biometrics-free'.

Prepare and publish a comprehensive analysis of all existing biometric systems

FRA has expressed that, with the exception of some of the member states they researched, '[o]nly limited information is currently available on the possible use or tests of live facial recognition technologies in other EU Member States'.[47] It is of utmost importance to follow up on the work

[39] Hasan (n 12).

[40] CNIL (n 24).

[41] Share Foundation, 'Serbia: Unlawful facial recognition video surveillance in Belgrade' (*EDRi*, 4 December 2019) <https://edri.org/serbia-unlawful-facial-recognition-video-surveillance-in-belgrade/> accessed 15 March 2020.

[42] Ivana Sekularac, 'Chinese police officers join Serbian colleagues on the beat in Belgrade' (*Reuters*, 23 September 2019) <https://www.reuters.com/article/us-serbia-china-patrols/chinese-police-officers-join-serbian-colleagues-on-the-beat-in-belgrade-idUSKBN1W81B0> accessed 15 March 2020.

[43] FRA (n 19).

[44] Charter of Fundamental Rights of the European Union (2000/C 364/01).

[45] Regarding lack of legal basis, see FRA (n18) 12, 13 for cases in Germany and UK, respectively.

[46] Cities for Digital Rights <https://citiesfordigitalrights.org/>, accessed 15 March 2020.

[47] FRA (n 19) 13.

already done by FRA and make sure that all of these biometric/facial recognition systems are mapped and analysed to the extent of understanding their legal basis (if any), impact on fundamental rights, legal safeguards (data protection impact assessments, etc…) present when implementing the different systems and which companies are developing and implementing the different systems (and potential connections to people in power who 'coincidentally' promote similar policies).

The public-private partnerships are not a minor issue in this discussion. The existence of what Statewatch has called a 'EU security-industrial complex'[48] may lead (as civil society groups have suggested in the case of Passenger Name Record (PNR) systems[49]) to the promotion, defence and (ab)use of 'securitisation' technologies, from CCTV cameras to 'lie detectors'[50] for refugees. By uncovering the fact that some securitisation public policies are promoted by private interests we will be able as a society to take better decisions as whether these policies are in the public interest, or only in the private interest.

Because of this, and simultaneously to the ban, the EC should require the FRA to prepare this comprehensive analysis of all existing and planned facial recognition systems and other biometric technologies used for live remote identification in publicly accessible spaces used in all EU member states. Based on the information derived from this research the EC should decide on any next steps forward, including launching of infringement procedures in case member states continue deploying and using systems which are in breach of the Charter.

Enact legislation banning the use of these technologies and stop funding them

In addition to this, and in order to improve legal clarity and to avoid a whack-a-mole game where systems are deployed and cancelled taking advantage of the lack of clear guidance from policy-makers, the EC should take steps to prepare legislation that leads to the ban on the use of facial recognition systems and other biometric technologies used for live remote identification in publicly accessible spaces. The EC, as the Guardian of the Treaties (including the Charter), should push forward a ban on the deployment and use of recognition systems and other biometric technologies used for live remote identification in publicly accessible spaces and the dismantlement of existing ones in member states until the analysis of their necessity and proportionality shows its adequacy with EU law.

The EC showed some interest in the first leak of the Artificial Intelligence White Paper,[51] although the same document that proposed the ban as an option later discarded the ban as the one the EC should take forward. In the actual white paper published in March 2020, the EC only timidly suggested to 'launch a broad European debate on the specific circumstances, if any, which might justify such use [of technologies used for remote biometric identification], and on common safeguards'.[52]

Finally, the second recommendation we make is for public institutions to immediately stop funding research projects that have a surveillance, biometrics or facial recognition component. Euractiv[53] reported that:

[48] Statewatch, 'Market Forces: the development of the EU security-industrial complex' (*Statewatch*, 2009) <http://www.statewatch.org/marketforces/index.htm> accessed 15 March 2020.

[49] Estelle Massé and Joe McNamee, 'The curious tale of the French prime minister, PNR and peculiar patterns' (*Euractiv*, 4 October 2016) <https://www.euractiv.com/section/justice-home-affairs/opinion/checked-for-tuesthe-curious-tale-of-the-french-prime-minister-pnr-and-peculiar-patterns/> accessed 15 March 2020.

[50] Tara Deschamps, 'Computer says "no"' (*University of Toronto Magazine*, 2 October 2019) <https://magazine.utoronto.ca/people/alumni-donors/computer-says-no-petra-molnar-ai-immigration-decisions/> accessed 15 March 2020.

[51] Hasan (n 12).

[52] CNIL (n 24).

[53] Daniel Leufer and Fieke Jansen, 'The EU is funding dystopian Artificial Intelligence projects' (*Euractiv*, 22 January 2020) <https://www.euractiv.com/section/digital/opinion/the-eu-is-funding-dystopian-artificial-intelligence-projects/> accessed 15 March 2020.

> the [European] Commission is investing in the development of AI systems through funding programs such as Horizon 2020, which will have invested nearly €80 billion of funding over 7 years (2014 to 2020), with a significant portion of that going to so-called 'artificial intelligence' projects.

This includes the problematic iBorderCTRL.[54] Funding projects that could help develop biometric systems used for mass surveillance should be reviewed in view of the implications that the public investment in such technologies could have for fundamental rights.

CONCLUSIONS

Facial recognition systems and other biometric technologies used for live remote identification in publicly accessible spaces are probably the current most invasive systems of mass surveillance in European societies. Their risks are well documented and cities and states (outside Europe) have taken strong steps to deter their uses. Increasing research is being done on these biometric systems, but little (if anything) is getting the attention of data protection supervisors, national human rights institutions and policy makers. While these systems have been banned in cities and states in the US, the EC seems to be unwilling, at least in their first months in office, to take immediate action probably in order to avoid upsetting too soon the member states who are developing these systems.

As it happened with CCTV cameras, these systems will be deployed for the most noble reasons (prevention and detection of serious crimes, finding missing children...) without the evidence showing the necessity, proportionality and even the efficiency of those biometric systems to achieve the ends they are supposedly aiming at. If there is no concrete action to ban the use of these systems in publicly accessible spaces, we will be seeing more of these systems in Europe and across the world (sometimes, conveniently, re-purposing CCTV cameras for the new application). The argument will be around 'efficiency' or 'usefulness' of the new technologies. However, efficiency or usefulness are not valid legal basis, even when proved (which regarding these systems is not the case). In this sense, analogue conclusions on the use of face surveillance could be taken from the analysis that EDRi states regarding the use of data retention:

> Because of the scale and the means put into this issue, it must be part of the Rule of Law and must respect fundamental rights. Relying only on efficiency would mean ignoring other democratic issues and could potentially, in extreme cases, lead to harms done to citizens.[55]

Given the risks posed by facial recognition systems and other biometric technologies used for live remote identification in publicly accessible spaces for our most basic fundamental rights, from dignity to privacy to freedom of assembly, policy-makers need to take urgent action before the systems are further deployed, developed and normalised in our streets, shopping centres, train stations and parks. The risks for increasing power imbalances, discrimination, racism, inequalities and general societal control are too high for the alleged 'benefits' these technologies could bring.

[54] European Commission CORDIS, 'Intelligent Portable Border Control System' (*CORDIS*) <https://cordis.europa.eu/project/id/700626>, accessed 15 March 2020.

[55] Laureline Lemoine, 'Data Retention: "National security" is not a blank cheque' (*EDRi*, 29 January 2020) <https://edri.org/data-retention-national-security-is-not-a-blank-cheque/> accessed 13 April 2020.

REFERENCES

Access Now, 'Why ID' <https://www.accessnow.org/whyid-letter/> accessed 10 May 2020

Ban Facial Recognition <https://www.banfacialrecognition.com/map/>

Burt C, 'UN privacy rapporteur criticizes accuracy and proportionality of Wales police use of facial recognition' (*Biometric Update.com*, 3 July 2018) <https://www.biometricupdate.com/201807/un-privacy-rapporteur-criticizes-accuracy-and-proportionality-of-wales-police-use-of-facial-recognition> accessed 15 March 2020

Cities for Digital Rights <https://citiesfordigitalrights.org/>

Commission Nationale de l'Informatique et des Liberté (CNIL), 'Reconnaissance faciale : pour un débat à la hauteur des enjeux' (*CNIL*, 15 November 2019) <https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux> accessed 15 March 2020

Conger K, Fausset R and Kovaleski SF, 'San Francisco Bans Facial Recognition Technology' (*The New York Times*, 14 May 2019) <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html> accessed 15 March 2020

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe ETS No 108)

Data Protection Regulation for EU institutions (Regulation 2018/1725)

Deschamps T, 'Computer says "no"' (*University of Toronto Magazine*, 2 October 2019) <https://magazine.utoronto.ca/people/alumni-donors/computer-says-no-petra-molnar-ai-immigration-decisions/> accessed 15 March 2020

Dodd V and Grierson J, 'Non-violent groups on UK counter-terror list threaten legal action' (*The Guardian*, 22 January 2020) <https://www.theguardian.com/environment/2020/jan/22/minister-denies-government-considers-extinction-rebellion-extremist> accessed 15 March 2020

Doffman Z, 'Hong Kong exposes both sides of China's relentless facial recognition machine' (*Forbes*, 26 August 2019) <https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/> accessed 15 March 2020

Electronic Frontier Foundation (EFF), 'Biometrics: Facial Recognition' (*EFF*) <https://www.eff.org/document/biometrics-facial-recognition> accessed 15 March 2020

Electronic Privacy Information Center, 'Ban Facial Surveillance' (*EPIC*) <https://epic.org/banfacesurveillance/> accessed 10 May 2020

— 'State Facial Recognition Policy' (*EPIC*) <https://epic.org/state-policy/facialrecognition/>

European Commission, 'On Artificial Intelligence - A European approach to excellence and trust' (COM(2020) 65 final 19 February 2020) <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf> accessed 15 March 2020

European Commission CORDIS, 'Intelligent Portable Border Control System' (*CORDIS*) <https://cordis.europa.eu/project/id/700626>

Fundamental Rights Agency (FRA), 'Facial recognition technology: fundamental rights considerations in the context of law enforcement' (FRA 2019) <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf> accessed 15 March 2020

— (3 March 2020) <https://twitter.com/EURightsAgency/status/1234804039449239553>

General Data Protection Regulation (Regulation 2016/679)

Gómez-Serranillos J, 'RentCOVID-19: una tecnología de reconocimiento facial para revisar miles de solicitudes de ayudas al alquiler' (*Expansion*, 15 April 2020) <https://www.expansion.com/juridico/actualidad-tendencias/2020/04/13/5e94167f468aeb53128b45c6.html>

Hasan A, '2019 Proved We Can Stop Face Recognition Surveillance' (*ACLU*, 17 January 2020) <https://www.aclu.org/news/privacy-technology/2019-was-the-year-we-proved-face-recognition-surveillance-isnt-inevitable/> accessed 15 March 2020

Jakubowska E, 'Facial recognition and fundamental rights 101' (*EDRi*, 4 December 2019) <https://edri.org/facial-recognition-and-fundamental-rights-101/> accessed 15 March 2020

Kaye D, 'The surveillance industry is assisting state suppression. It must be stopped' (*The Guardian*, 26 November 2019) <https://www.theguardian.com/commentisfree/2019/nov/26/surveillance-industry-suppression-spyware> accessed 10 May 2020

La Quadrature du Net, 'Joint Letter from 80 organisations: Ban Security and Surveillance Facial Recognition' (*La Quadrature du Net*, 19 December 2019) <https://www.laquadrature.net/en/2019/12/19/joint-letter-from-80-organisations-ban-security-and-surveillance-facial-recognition/> accessed 15 March 2020

Law Enforcement Directive 2016/680

Le Monde avec AFP, 'Nice va tester la reconnaissance faciale sur la voie publique' (*Le Monde*, 18 February 2019) <https://www.lemonde.fr/societe/article/2019/02/18/nice-va-tester-la-reconnaissance-faciale-sur-la-voie-publique_5425053_3224.html> accessed 15 March 2020

Lemoine L, 'Data Retention: "National security" is not a blank cheque' (*EDRi*, 29 January 2020) <https://edri.org/data-retention-national-security-is-not-a-blank-cheque/> accessed 13 April 2020

Leufer D and Jansen F, 'The EU is funding dystopian Artificial Intelligence projects' (*Euractiv*, 22 January 2020) <https://www.euractiv.com/section/digital/opinion/the-eu-is-funding-dystopian-artificial-intelligence-projects/> accessed 15 March 2020

Liberty, 'Resist facial recognition' (*Liberty*) <https://www.libertyhumanrights.org.uk/resist-facial-recognition>

Massé E and McNamee J, 'The curious tale of the French prime minister, PNR and peculiar patterns' (*Euractiv*, 4 October 2016) <https://www.euractiv.com/section/justice-home-affairs/opinion/checked-for-tuesthe-curious-tale-of-the-french-prime-minister-pnr-and-peculiar-patterns/> accessed 15 March 2020

McAskill E, 'Edward Snowden interview' (*The Guardian*, 13 September 2019) <https://www.theguardian.com/us-news/ng-interactive/2019/sep/13/edward-snowden-interview-whistleblowing-russia-ai-permanent-record> accessed 15 March 2020

Middlehurst C, 'China unveils world's first facial recognition ATM' (*The Telegraph*, 1 June 2015) <https://www.telegraph.co.uk/news/worldnews/asia/china/11643314/China-unveils-worlds-first-facial-recognition-ATM.html> accessed 15 March 2020

Molnar P and Gill L, 'Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Immigration and Refugee System' (International Human Rights Program (Faculty of Law, University of Toronto) and the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto) 2018) <https://ihrp.law.utoronto.ca/sites/default/files/media/IHRP-Automated-Systems-Report-Web.pdf> accessed 10 May 2020

Privacy International, 'MONITORYOU: the MilliONs beIng spenT by the eu on develOping surveillance tech to taRget YOU' (*Privacy International*, 20 January 2020) <https://privacyinternational.org/node/3341> accessed 15 March 2020

— 'This UK Government-Funded AI Programme Wants to Make "Face Recognition Ubiquitous". (But Sure, We're Probably Being Paranoid About Face Surveillance)' (*Privacy International*, 3 March 2020) <https://privacyinternational.org/node/3389> accessed 10 May 2020

— 'Facial Recognition' (*Privacy International*) <https://privacyinternational.org/learning-topics/facial-recognition> accessed 15 March 2020

Sabrie G, 'Behind the Rise of China's Facial-Recognition Giants' (*Wired*, 9 March 2019) <https://www.wired.com/story/behind-rise-chinas-facial-recognition-giants/> accessed 15 March 2020

Sekularac I, 'Chinese police officers join Serbian colleagues on the beat in Belgrade' (*Reuters*, 23 September 2019) <https://www.reuters.com/article/us-serbia-china-patrols/chinese-police-officers-join-serbian-colleagues-on-the-beat-in-belgrade-idUSKBN1W81B0> accessed 15 March 2020

Share Foundation, 'New surveillance cameras in Belgrade: location and human rights impact analysis – "withheld"' (*Share*, 29 March 2019) <https://www.sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/> accessed 15 March 2020

— 'Serbia: Unlawful facial recognition video surveillance in Belgrade' (*EDRi*, 4 December 2019) <https://edri.org/serbia-unlawful-facial-recogni-

tion-video-surveillance-in-belgrade/> accessed 15 March 2020

Special Rapporteur on the rights to freedom of peaceful assembly and of association, 'Report on the rights to freedom of peaceful assembly and of association: The Digital Age' (17 May 2019) A/HRC/41/41 15 <https://undocs.org/A/HRC/41/41> accessed 15 March 2020

Statewatch, 'Market Forces: the development of the EU security-industrial complex' (*Statewatch*, 2009) <http://www.statewatch.org/marketforces/index.htm> accessed 15 March 2020

Stolton S, 'LEAK: Commission considers facial recognition ban in AI "white paper"' (*Euractiv*, 17 January 2020) <https://www.euractiv.com/section/digital/news/leak-commission-considers-facial-recognition-ban-in-ai-white-paper/> accessed 15 March 2020

Stone C, 'Why the space for civic engagement is shrinking' (*Open Society Foundations*, 21 December 2015) <https://www.opensocietyfoundations.org/voices/why-space-civic-engagement-shrinking> accessed 15 March 2020

Storm D, 'ACLU: Orwellian Citizen Score, China's credit score system, is a warning for Americans' (*Computer World*, 7 October 2015) <https://www.computerworld.com/article/2990203/aclu-orwellian-citizen-score-chinas-credit-score-system-is-a-warning-for-americans.html> accessed 15 March 2020

The Public Voice, 'Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance Endorsements' (*The Public Voice*) <https://thepublicvoice.org/ban-facial-recognition/endorsement/> accessed 10 May 2020

United Nations Human Rights, Office of the High Commissioner, 'UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools' (*OHCHR*, 25 June 2019) <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736> accessed 15 March 2020

Wiewiórowski W, European Data Protection Supervisor (EDPS), 'AI and Facial Recognition: Challenges and Opportunities' (*EDPS*, 21 February 2020) <https://edps.europa.eu/press-publications/press-news/blog/ai-and-facial-recognition-challenges-and-opportunities_en> accessed 15 March 2020

Williams P and Kind E, 'Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe' (European Network Against Racism (ENAR) 2019) <https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf> accessed 15 March 2020

Global Campus
of Human Rights

Monastery of San Nicolò
Riviera San Nicolò, 26
I-30126 Venice Lido (Italy)

gchumanrights.org

Global Campus of Human Rights

The Global Campus of Human Rights is a unique network of more than one hundred participating universities around the world, seeking to advance human rights and democracy through regional and global cooperation for education and research. This global network is promoted through seven Regional Programmes which are based in Venice for Europe, in Sarajevo/Bologna for South East Europe, in Yerevan for the Caucasus, in Pretoria for Africa, in Bangkok for Asia-Pacific, in Buenos Aires for Latin America and the Caribbean, and in Beirut for the Arab World.

The Global Campus Policy Observatory

The Observatory is a 'virtual hub' which comprehends a team of seven researches from the regional programmes to produce, publish and publicly present seven different policy analyses in form of policy briefs, with the aim of making of each regional programme a solid focal point for policy expert advisory in human rights issues.

This document has been produced with the financial assistance of the European Union and as part of the Global Campus of Human Rights. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or of Global Campus of Human Rights.