Paolo Cirio

Prohibir el reconocimiento facial en Europa

Ban facial recognition Europe

https://paolocirio.net/

Es artista conceptual, hacktivista y crítico cultural. Su producción ahonda en sistemas de información legales, económicos y culturales.

Studio@PaoloCirio.net

Ban Facial Recognition Europe

The first petition of over 50000 signatures

The petition for 1000000 signatures

- Legal research and petition
- Cases of violations in Europe
- Claims delivered to EU institutions
- Video statement by Paolo Cirio
- Press material of the campaign
- Twitter Ban Facial Recognition EU

The petition to ban facial recognition in Europe was created by Paolo Cirio in September 2020. His campaign collected over 50000 signatures. Later in 2021 this campaign merged with the platform to ban biometric surveillance *ReclaimYourFace* by EDRi and the petition on the European Citizen Initiative platform.

This petition introduces the campaign for the permanent ban of Facial Recognition used for identification and profiling in all of Europe. An initiative by the activist Paolo Cirio in alliance with La Quadrature du Net, We Sign It, and thanks to the research of European Digital Rights (EDRi).

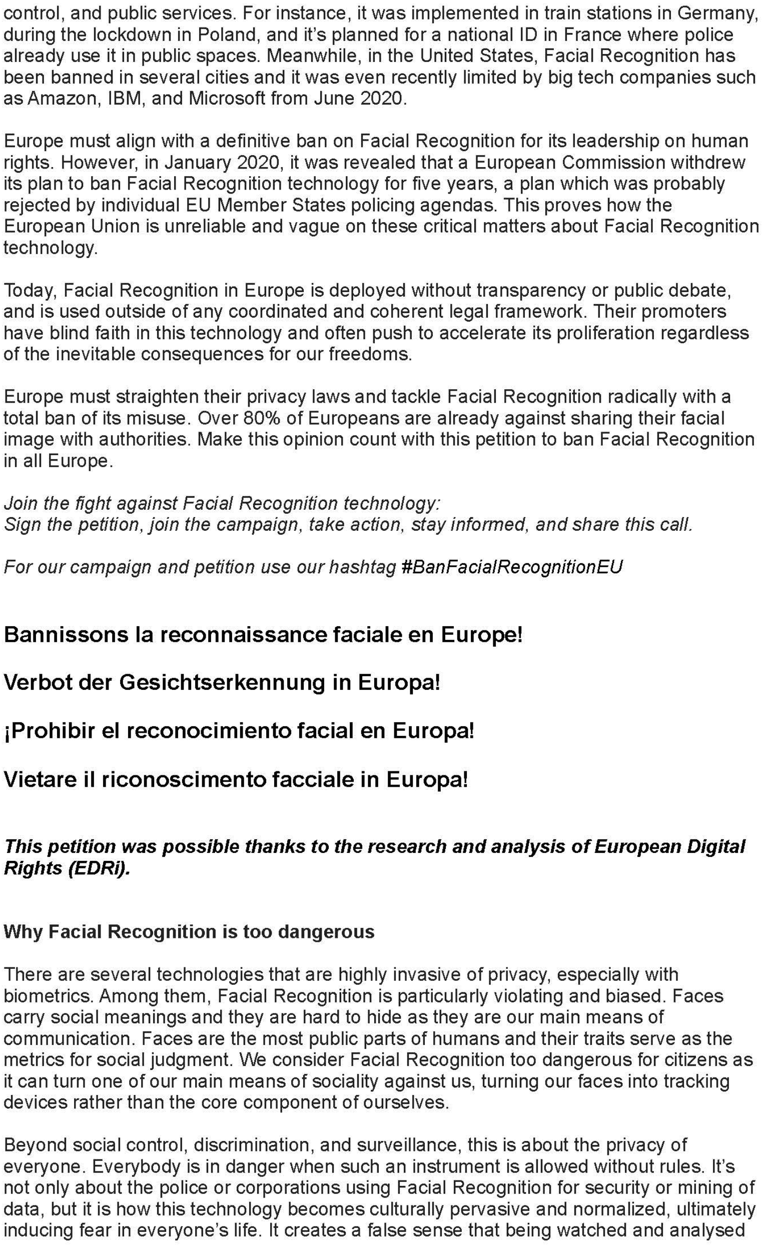
- Why Facial Recognition is too dangerous
- Facial Recognition needs to be banned
- What we need to ban Facial Recognition
- Cases and details of violations
- Legal claims and complaint

Automated Facial Recognition technology has already been rolled out in EU member states without public consultation. We demand the Members of the European Parliament and the European Commission to take seriously this enormous threat to human rights and our civil society and to legislate for the immediate and permanent ban on identification and profiling via Facial Recognition technology in all of Europe.

Facial Recognition is a particularly invasive technology. It's not only about the surveillance of activists, suspects, and minorities, but it is an invasion of privacy for everyone and an enormous danger to democratic freedoms, civil liberties, and free expression for the whole society.

Currently, police agencies and security departments of individual European states, in concert with the tech industry, lobby against the European institutions for the use of Facial Recognition technology. In response, this petition aims to challenge the objections made by individual member states on the banning of Facial Recognition and demands the European Commission to start infringement proceedings against Member States that are breaching EU laws already by using Facial Recognition.

Several member states of Europe already use Facial Recognition for security, social



control, and public services. For instance, it was implemented in train stations in Germany, during the lockdown in Poland, and it's planned for a national ID in France where police already use it in public spaces. Meanwhile, in the United States, Facial Recognition has been banned in several cities and it was even recently limited by big tech companies such as Amazon, IBM, and Microsoft from June 2020.

Europe must align with a definitive ban on Facial Recognition for its leadership on human rights. However, in January 2020, it was revealed that a European Commission withdrew its plan to ban Facial Recognition technology for five years, a plan which was probably rejected by individual EU Member States policing agendas. This proves how the European Union is unreliable and vague on these critical matters about Facial Recognition technology.

Today, Facial Recognition in Europe is deployed without transparency or public debate, and is used outside of any coordinated and coherent legal framework. Their promoters have blind faith in this technology and often push to accelerate its proliferation regardless of the inevitable consequences for our freedoms.

Europe must straighten their privacy laws and tackle Facial Recognition radically with a total ban of its misuse. Over 80% of Europeans are already against sharing their facial image with authorities. Make this opinion count with this petition to ban Facial Recognition in all Europe.

Join the fight against Facial Recognition technology:
Sign the petition, join the campaign, take action, stay informed, and share this call.

For our campaign and petition use our hashtag #BanFacialRecognitionEU

Bannissons la reconnaissance faciale en Europe!

Verbot der Gesichtserkennung in Europa!

¡Prohibir el reconocimiento facial en Europa!

Vietare il riconoscimento facciale in Europa!

This petition was possible thanks to the research and analysis of European Digital Rights (EDRi).

Why Facial Recognition is too dangerous

There are several technologies that are highly invasive of privacy, especially with biometrics. Among them, Facial Recognition is particularly violating and biased. Faces carry social meanings and they are hard to hide as they are our main means of communication. Faces are the most public parts of humans and their traits serve as the metrics for social judgment. We consider Facial Recognition too dangerous for citizens as it can turn one of our main means of sociality against us, turning our faces into tracking devices rather than the core component of ourselves.

Beyond social control, discrimination, and surveillance, this is about the privacy of everyone. Everybody is in danger when such an instrument is allowed without rules. It's not only about the police or corporations using Facial Recognition for security or mining of data, but it is how this technology becomes culturally pervasive and normalized, ultimately inducing fear in everyone's life. It creates a false sense that being watched and analysed at all times is acceptable and creates societies filled with suspicion, abuse, and mistrust.

Facial Recognition technology is also worsened by “behavioural prediction” which claims of being able to classify a person’s emotions or intentions but fundamentally threatens human dignity and autonomy. Facial Recognition coupled with so-called artificial intelligence in the form of machine learning algorithms increase power imbalances, discrimination, racism, inequalities, and authoritarian societal control. There are too many high risks for any alleged “benefits” that the use of these technologies could ever conceivably bring.

Across Europe, governments, private companies, and also civilians seek the use of Facial Recognition. We already saw its use in workplaces, public spaces, schools, airports, houses, and in our own personal phones. These implementations of Facial Recognition often go beyond our consent, or we are often forced to consent, while the long-term consequences of storing biometric data and training artificial intelligence to analyse our faces might go beyond our control and the institutions we trust.

No argument can justify the deployment of such technologies. Civil, Commercial, and Governmental use of Facial Recognition devices for identification and categorisation of individuals must be strictly banned. Any Facial Recognition technology sold commercially or developed and used privately for this scope must be stopped.

Facial Recognition needs to be banned, not only regulated

Regulations are not enough and they would fail to tackle this technology because of the scale of its danger.

Facial Recognition infringes upon the right to dignity as it uses people’s own qualities, behaviours, emotions, or characteristics against them in ways that are not justified or proportionate to the EU’s fundamental rights or for individual national laws. For instance, current European regulations like the GDPR mainly cover citizens’ privacy in the commercial sector with several exceptions, however, it doesn’t sufficiently address the human rights that are in peril with Facial Recognition such as the right to dignity and equality.

Much like nuclear or chemical weapons, Facial Recognition poses a great threat to humanity. Its use for identification and profiling is certainly too dangerous to be used at all. It should be banned not only by the European Union but also globally by the United Nations.

There are false beliefs about Facial Recognition’s effectiveness and usefulness that justify its use within regulations. However, even for security, there are serious doubts if the police really need it or if it helps to provide better services. Private actors are gaining disproportionate power over the technology that has often been developed without accountability and transparency. Often, these technologies are sold to public authorities and law enforcement with little or no liability for their actions.

Beyond government and corporate surveillance, there are now huge amounts of public data on Internet websites, social media platforms, and open datasets that everyone can harvest or buy. Also, the infrastructures of the devices that capture images of faces are already ubiquitous with CCTV cameras, smartphones, and video scanners across our public and private lives. These conditions make Facial Recognition particularly dangerous among other technologies that can identify, track, and judge people.

Today, Facial Recognition is already in our smartphones, passport controls at airports, and public spaces. Using Facial Recognition for local one-to-one face authentication to unlock a smartphone or to access a service looks far less intrusive than identifying an individual among many individuals in a public place. However, the development of the technology itself, the training of algorithms, and the storage of the biometric data held by private companies could, in the future, be used beyond the initial scope. Even when we give consent or use Facial Recognition in private, we risk that such data could cause future unintentional consequences such as leaks of biometric data, the sales of it to third parties, or the training of algorithms on our personal traits.

Therefore we reject both exceptions of using Facial Recognition in regards to innovation for the tech industry and for public security. We call for a total ban for all cases of Facial Recognition technologies regarding its use for any form of identification, correlation, and discrimination which would enable mass surveillance, hate crimes, ubiquitous stalking, and violations of personal dignity. It would still be possible for research, medical, and entertainment purposes under the conditions that no biometric data is stored or used to identify or classify individuals.

We argue that Facial Recognition is already illegal under EU law and must be banned in practice. Four European instruments already prohibit biometric mass surveillance: in the broadest sense, the European Convention on Human Rights and the EU Charter of Fundamental Rights, and more specifically, the Council of Europe Data Protection Convention, the General Data Protection Regulation (GDPR), and its sister instrument, the Law Enforcement Directive (LED). However, national data protection authorities (DPAs) have been inadequately resourced and politically disempowered by their member states, meaning that their efforts to enforce regulations have suffered, and actors in violation of the law have faced few incentives to comply.

That's why we need new laws to enforce a ban on Facial Recognition and not only weak regulations that can be interpreted and not enforced by the EU on its individual Member States and their MPs.

Identification and classification by Facial Recognition are too dangerous that it will never be necessary and proportionate since potential beneficial uses are not justified.

What we need to get Facial Recognition banned in EU

We need to take action at the European Parliament to draw attention to this issue in its Member States, as well as to put pressure on the European Commission to take enforcement action against the States that are currently violating EU fundamental rights and privacy laws. The total ban on identification and profiling via Facial Recognition technology shouldn't be just a directive but it must be a rigid ban to be enforceable throughout Europe without exceptions and expiration.

In the European Union there are already laws that regulate biometric mass surveillance, but they're not being applied. Protests, petitions, and strategic litigations can potentially be very effective in applying these existing laws and introducing a EU-wide ban.

On the streets and online, through protests and other forms of action, citizens and collectives across the world are teaming up to stop the fateful spread of Facial Recognition. Together, we are part of a wide movement resisting the advent of Face Recognition in all of Europe and globally.

Fight back and tell us if you see Facial Recognition used in schools, gated communities and buildings, IDs and badges, public services, lock devices, mobile applications, Internet platforms, and even if it's for entertainment or personal use or if it is used by the police, border control, law enforcement agencies, and investigators.

We ask the European Commission and the European Court of Justice to evaluate the cases we assembled about Facial Recognition programs in Europe for making these current and future uses illegal. If the European Commission, supported by the European Parliament, does not take the appropriate enforcement and legislative action to forbid such a technology, we plan to bring the cases to the European Court of Justice on the basis of current LED directives, GDPR regulations, Council of Europe Data Protection Convention, and national data protection laws, including European Convention on Human Rights and the EU Charter of Fundamental Rights.

Today, we express our collective refusal of these tools of social control by urging policymakers to ban them once and for all.

Cases and details - Facial Recognition in Europe

As of May 2020, at least 15 European countries have experimented with biometric technologies such as Facial Recognition in public spaces. At a minimum, there are activities happening in Czech Republic, Denmark, France, Germany, Greece, Hungary, Italy, the Netherlands, Poland, Romania, Serbia, Slovenia, Sweden, and Switzerland and the United Kingdom.

The following list of cases about the uses of Facial Recognition in Europe has been compiled by Paolo Cirio with his research and with the help of privacy policy experts and organizations such as La Quadrature du Net, and through the EDRi research paper for banning Biometric Surveillance:
https://edri.org/blog-ban-biometric-mass-surveillance/

This list demonstrates how the lack of a coherent legislation surrounding Facial Recognition is causing Member States of the EU to take individual initiatives, have lax oversight, and make actual use of such dangerous technology.

We demand greater public transparency of and accountability on the parties - whether public, private or collaborations between the two - who are deploying biometric processing, as well as data exchanges between law enforcement, border security, other public security agencies, including health, and national security agencies.

FRANCE

As of 2020
The French police already use Facial Recognition to identify people in public spaces. They use photos of people stored in the prior criminal records database TAJ (the "Traitement des antécédents judiciaires"). There are more than 18 million records of individuals in this database with more than 8 million photos. The use of Facial Recognition in this database in France has been allowed since 2012 and is currently being challenged in front of national courts.
https://www.laquadrature.net/2020/08/07/nous-attaquons-la-reconnaissance-faciale-dans-le-taj/
https://www.cnil.fr/fr/taj-traitement-dantecedents-judiciaires

October 2019
France is poised to become the first European country to use Facial Recognition technology to give citizens a digital identity - whether they want it or not. Saying that he wants to make the state more efficient, President Emmanuel Macron is pushing through plans to roll out an ID program based on Facial Recognition called Alicem as part of his government.
https://www.bloomberg.com/news/articles/2019-10-03/french-liberte-tested-by-nationwide-facial-recognition-id-plan

July 2019

The Provence-Alpes-Côte d’Azur (PACA) regional authority asked France’s data protection authority, the CNIL, for permission to use a Facial Recognition system to manage entry at Ampère high-school in Marseille. This “trial” was intended to be a year-long experiment and was also carried out at another school in the same region (the Lycée les Eucalyptus in Nice). This use was designed to increase the security of both students and staff and to quicken the time it takes for students to enter the school premises. These attempts of using Facial Recognition in the two French schools were stopped by a lawsuit in 2020.
https://ai-regulation.com/first-decision-ever-of-a-french-court-applying-gdpr-to-facial-recognition/

Since 2012
“PARAFE” is a program for automated border gates already installed in various stations and airports in France. The gates use Facial Recognition technology to verify the user's identity against the data stored in the chip in their biometric passport. The program was developed by the French company Thales.
https://en.wikipedia.org/wiki/PARAFE
https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/smart-gates-paris

GERMANY

January 2020
Germany’s Interior Minister, Horst Seehofer, planned to use automatic Facial Recognition at 134 railway stations and 14 airports, according to a news report published on 3 January 2020. This provoked an outrage in the German media, leading to the plans being put on hold.

August 2017 - July 2018
The interior ministry tested Facial Recognition cameras at the Berlin-Südkreuz train station. The result was that 80% of the people were correctly identified. After the 2018 tests, Interior Minister Seehofer said that Facial Recognition systems would “make police work even more efficient, thus improving security for citizens”.
https://www.euractiv.com/section/data-protection/news/german-ministers-plan-to-expand-automatic-facial-recognition-meets-fierce-criticism/

POLAND

March 2020
Poland’s mandatory Facial Recognition-based app was used to enforce quarantine. It sent the police to the home of anyone that fails to share a selfie on the app within 20 minutes of an alert.
https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/

SCOTLAND

February 2020
Police in Scotland said it hoped to use live Facial Recognition software by 2026, but later put the plans on hold. The technology can scan crowds of people and cross-reference faces with police databases.
https://www.bbc.com/news/uk-scotland-51449166

SWEDEN

August 2019
Facial Recognition was in use by high-school students in Sweden to keep track of attendance in the Skelleftea municipality. The trial, which took place in autumn 2018, had

been so successful that the local authority was considering extending it. However, Sweden judges and data protection authorities blocked the experimentation of Facial Recognition in schools.
https://www.bbc.com/news/technology-49489154

GREECE

March 2020
The Greek watchdog filed a request for opinion to the Greek DPA regarding a so-called "smart policing" contract of the HP. This contract aims at developing smart devices with integrated software enabling facial recognition and automated fingerprint identification of individuals during police stops. The Hellenic Police signed a €4 million contract in the spring of 2019 with Intracom Telecom, a global telecommunication systems and solutions vendor, for a smart policing project. No data protection impact assessment was taken out before the contract was signed, nor was the relevant data protection authority contacted.
https://edri.org/our-work/facial-recognition-homo-digitalis-calls-on-greek-dpa-to-speak-up/
https://algorithmwatch.org/en/story/greek-police-live-facial-recognition

NETHERLANDS

As of 2020
The Dutch police maintain a facial recognition database that currently offers information on 1.4 million individuals. Facial recognition uses are introduced in the public space under the guise of a pilot or, especially in smart city contexts, "Living Lab", sidestepping regulatory requirements and frustrating civic engagement.
https://www.vice.com/nl/article/8xzydz/gezichtsherkenning-op-de-nederlandse-straten-moeten-we-dat-willen

In the Netherlands, the use of facial recognition is on the rise in public spaces. Its use is already documented in supermarkets, at the airport and at soccer stadiums:
https://www.rtlnieuws.nl/nieuws/nederland/artikel/4941596/gezichtsherkenning-biometrie-alphen-jumbo-privacy
https://www.amsterdam.nl/wonen-leefomgeving/innovatie/de-digitale-stad/digitale-perimeter/
https://www.volkskrant.nl/kijkverder/v/2020/de-stand-van-gezichtsherkenning-in-nederland~v91028

CZECH REPUBLIC

November 2019
Prague police have asked the municipality for a green light to activate automatic facial recognition cameras at six locations. The media recently nformed that in the autumn of 2020 police representatives announced that they had bought top recognition software from Cogniware.
https://english.radio.cz/prague-police-seek-okay-test-facial-recognition-camera-system-raising-privacy-8114937

November 2019
The Czech data protection authority has ruled that processing of data using facial recognition technology on a construction site was legal in very specific circumstances. The inspection authority of the Office for Personal Data Protection carried out an inspection investigating processing of personal data related to the use of facial recognition technology (FaceID) for identifying workers present on construction site.
https://www.lexology.com/library/detail.aspx?g=63ba2d65-9b5c-41e4-b83a-1948d644d319

ITALY

June 2020
The municipality of Como, Italy, purchased a facial recognition system, which was bought, installed, and tested for months with little transparency and despite the lack of a clear legal framework. The experiment in the city of Como was stopped by a measure of the Italian Data Protection Authority thanks also to a timely journalistic investigation. Yet, other cities have already announced the installation of similar technologies, such as Turin and Udine.
https://privacyinternational.org/case-study/4166/how-facial-recognition-spreading-italy-case-como
https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/

November 2017
Italian police has acquired a facial recognition system. The Ministry of the Interior commissioned Parsec 3.26 to provide software for the "Automatic Image Recognition System (SARI)" which, if we want to be more precise, is a system for facial recognition. The SARI system acquired by the scientific police has proved to be immediately biased and covered by a veil of extreme secrecy.
https://medium.com/@ORARiccardo/italian-police-has-acquired-a-facial-recognition-system-a54016211ff2
https://www.wired.it/attualita/tech/2019/04/03/sari-riconoscimento-facciale-stranieri/

EUROPEAN EXPORT

Amnesty International found that three companies based in France, Sweden and the Netherlands sold digital surveillance systems, such as facial recognition technology and network cameras, to key players of the Chinese mass surveillance apparatus. In some cases, the export was directly for use in China's indiscriminate mass surveillance programs, with the risk of being used against Uyghurs and other predominantly Muslim ethnic groups throughout the country.
https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-human-rights-abusers/

EUROPEAN BORDERS

The SPIRIT is a European funded project to scrape social media images of faces to build a database for Facial Recognition analysis. Five law enforcement-related stakeholders participate in this research project: the Hellenic Police (GR), the West Midlands Police (UK), the Police and Crime Commissioner for Thames Valley (UK), the Serbian Ministry of Interior (RS), and the Police Academy in Szczytno (PL). According to the sparse and nontransparent website, the project aims to use tools, such as face extraction and matching, to correlate information from social media data similar to the model of the U.S. company Clearview AI. According to freedom of information requests, trials were planned for 2020 and 2021.

The iBorderCtrl is a European funded research project on the Hungarian, Greek, and Latvian borders. The project planned to use automated analysis of biometric data to predict evidence of deception among those looking to enter the European Union as "lie detectors" for refugees. The project came to an end in August 2019.
https://edri.org/blog-ban-biometric-mass-surveillance/

The Prum System is an EU-wide initiative connecting DNA, fingerprint, and vehicle registration databases for mutual searching. Ten European member states, led by Austria, call to expand the Prum System and create a network of national police facial recognition databases and interconnect such databases to every member of state with networks of police facial databases spanning the whole of Europe and the U.S.
https://theintercept.com/2020/02/21/eu-facial-recognition-database/

The “EU security-industrial complex” leads to the promotion, defense, and use of “securitisation” technologies. The agencies Europol and Frontex already use advanced biometric technology to survey borders and profile travellers.
https://edri.org/blog-ban-biometric-mass-surveillance/

Foreign countries and companies in Europe

The scraping of social media and the brokerage of datasets goes beyond borders, with companies and state actors interested in harvesting, scanning images, and building databases of biometric data of European citizens.

This is already happening with Clearview AI, an American company that scrapes images from social networks, and with FindFace, a face recognition technology developed by the Russian company NtechLab.

https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
https://www.forbes.com/sites/thomasbrewster/2020/01/29/findface-rolls-out-huge-facial-recognition-surveillance-in-moscow-russia/

The use of these tools goes beyond Europe with foreign entities that are allowed to use Facial Recognition technology on European citizens. Amazon, Facebook, Google, and Apple also assemble huge databases of biometric facial data of European citizens and use it to train their artificial intelligence without transparency and accountability. Products such as Ring of Amazon, Apple Face ID, Google Lens, and Facebook facial recognition features should be forbidden to use on all European citizens.

LEGAL COMPLAINT

Complaint submitted in February 2021 by the campaign for the permanent ban of Facial Recognition used for identification and profiling in all of Europe.

The complaint package is composed of the following:
- The claims of violations (list of articles and regulations in EU)
- The evidence of violations (list of cases of FR uses in EU)
- The evidence of the will of the people (50,000 signatures)

This legal complaint is delivered to the European Data Protection Supervisor (EDPS) for asking them to exercise their mandate by ensuring that the European Commission and EU institutions are upholding their data protection obligations. This package is also sent to the European Commission to take enforcement action against the States that are currently violating EU fundamental rights and to the European Parliament to debate and pass a resolution supporting the ban of Facial Recognition.

Uses of Facial Recognition technology in Europe led to abuses of fundamental rights, lack of accountability, and misspending of public funds for several years. European institutions are responsible for not enacting a clear legal framework concerning Facial Recognition technology and not enforcing actions for violations of existing regulations.

LEGAL CLAIMS

The listed cases of use of Facial Recognition in EU must be considered in violation of articles in the Charter of Fundamental Rights of the EU, the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), European Data Protection Board Guidlines, European Convention on Human Rights, and the Council of Europe Data Protection Convention.

- Directive (EU) 2016/680
The Police and Criminal Justice Authorities Directive, also known as Law Enforcement Directive (LED), defines the processing of personal data by authorities dealing with criminal offences and evidence by police. Facial Recognition uses are violating fundamental rights in the Article 10 of this Directive, which states that every biometric data used in order to identify individuals is only possible “where strictly necessary” and “subject to appropriate safeguards for the rights and freedoms of the data subject”.

- General Data Protection Regulation
In the General Data Protection Regulation (GDPR) violations with Facial Recognition concern the Article 9 with the idea that the processing of biometric data for identification is forbidden. Also Article 6 is violated when there aren’t the conditions under which personal data can be legally processed, one such requirement being that the data subject has given their explicit consent.

- EDPB Guidelines 3/2019
The European Data Protection Board (EDPB) on 29 January 2020 adopted guidelines on the processing of personal data through video devices which has a dedicated section on special categories such as biometric data. The scope of application is GDPR, thus the guidelines generally apply to companies and authorities other than law enforcement and intelligence services. An instance of violation with Facial Recognition is with the point 66 of the guidelines: "the data controller should always try to minimize the risk of capturing footage revealing other sensitive data regardless of the aim."

The human rights violations concerning privacy apply with the use facial recognition and the following institutions define them:

- European Convention on Human Rights:
Article 8, “It provides a right to respect for one's private and family life, his home and his correspondence”.

- Council of Europe Data Protection Convention:
Principles 108, about "the collection and processing of biometric data”.

- European Court of Human Rights:
Article 12, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."

- Charter of Fundamental Rights:
Article 11, "Freedom of assembly and association" The notion of anonymity is a prerequisite to join a political protest in public spaces.

Beyond privacy and surveillance, facial recognition infringes human dignity and enables social discrimination, therefore more violations of fundamental rights would apply to this legal complaint.

This legal complaint is addressed to the following institutions:
European Data Protection Supervisor, European Data Protection Board, European Union Agency for Fundamental Rights, Council of Europe, European Commission, European Parliament.

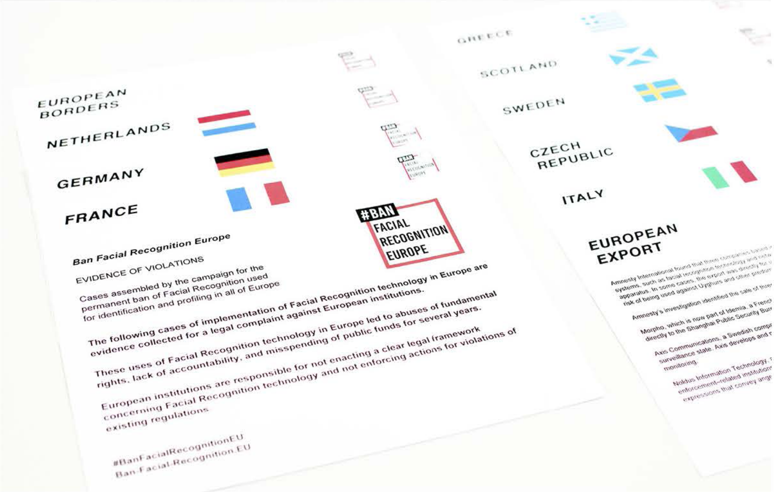
BAN FACIAL RECOGNITION EUROPE BANNER

#BAN
FACIAL
RECOGNITION
EUROPE
GREECE
SCOTLAND
SWEDEN
CZECH REPUBLIC
ITALY
EUROPEAN EXPORT

#BAN
FACIAL
RECOGNITION
EUROPE
EUROPEAN BORDERS
NETHERLANDS
GERMANY
FRANCE
Ban Facial Recognition Europe
EVIDENCE OF VIOLATIONS
Cases assembled by the campaign for the permanent ban of Facial Recognition used for identification and profiling in all of Europe
The following cases of implementation of Facial Recognition technology in Europe are evidence collected for a legal complaint against European institutions.
These uses of Facial Recognition technology in Europe led to abuses of fundamental rights, lack of accountability, and misspending of public funds for several years.
European institutions are responsible for not enacting a clear legal framework concerning Facial Recognition technology and not enforcing actions for violations of existing regulations.
#BanFacialRecognitionEU
Ban-Facial-Recognition.EU
GREECE
SCOTLAND
SWEDEN
CZECH REPUBLIC
ITALY
EUROPEAN EXPORT

#BAN
FACIAL
RECOGNITION
EUROPE
#BAN
FACIAL
RECOGNITION
EUROPE

#BAN
FACIAL
RECOGNITION
EUROPE



EUROPEAN BORDERS

NETHERLANDS

GERMANY

FRANCE

Ban Facial Recognition Europe

EVIDENCE OF VIOLATIONS

Cases assembled by the campaign for the permanent ban of Facial Recognition used for identification and profiling in all of Europe

The following cases of implementation of Facial Recognition technology in Europe are evidence collected for a legal complaint against European institutions.

These uses of Facial Recognition technology in Europe led to abuses of fundamental rights, lack of accountability, and misspending of public funds for several years.

European institutions are responsible for not enacting a clear legal framework concerning Facial Recognition technology and not enforcing actions for violations of existing regulations

#BanFacialRecognitionEU
Ban-Facial-Recognition.EU

GREECE

SCOTLAND

SWEDEN

CZECH REPUBLIC

ITALY

EUROPEAN EXPORT

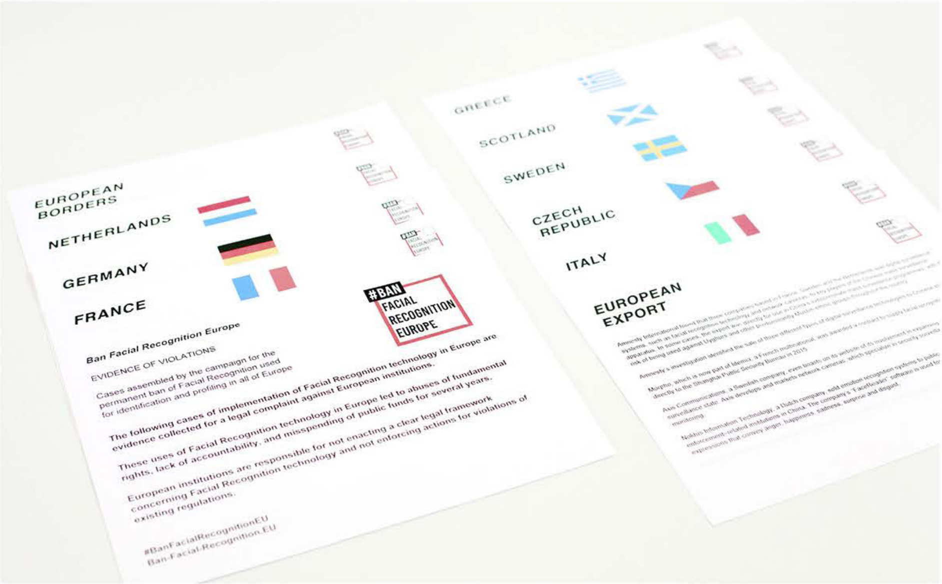
Amnesty International found that three companies based
systems, such as facial recognition technology and netw
apparatus. In some cases, the export was directly for u
risk of being used against Uyghurs and other predom

Amnesty's investigation identified the sale of thre

Morpho, which is now part of Idemia, a French
directly to the Shanghai Public Security Bur

Axis Communications, a Swedish compa
surveillance state. Axis develops and r
monitoring.

Noldus Information Technology,
enforcement-related institution
expressions that convey ange



EUROPEAN BORDERS

NETHERLANDS

GERMANY

FRANCE

#BAN FACIAL RECOGNITION EUROPE

Ban Facial Recognition Europe

EVIDENCE OF VIOLATIONS

Cases assembled by the campaign for the permanent ban of Facial Recognition used for identification and profiling in all of Europe

The following cases of implementation of Facial Recognition technology in Europe are evidence collected for a legal complaint against European institutions.

These uses of Facial Recognition technology in Europe led to abuses of fundamental rights, lack of accountability, and misspending of public funds for several years.

European institutions are responsible for not enacting a clear legal framework concerning Facial Recognition technology and not enforcing actions for violations of existing regulations.

#BanFacialRecognitionEU
Ban-Facial-Recognition.EU

GREECE

SCOTLAND

SWEDEN

CZECH REPUBLIC

ITALY

EUROPEAN EXPORT

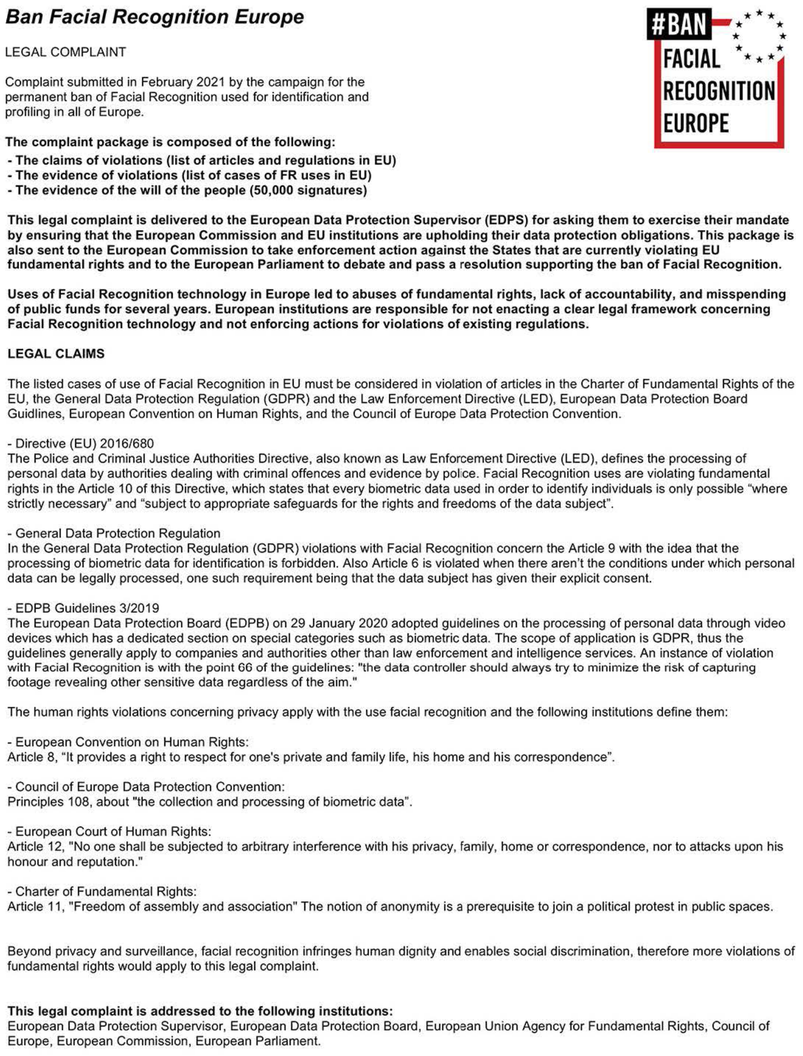
Amnesty International found that three companies based in France, Sweden and the Netherlands sold digital surveillance systems, such as facial recognition technology and network cameras, to key players of the Chinese mass surveillance apparatus. In some cases, the export was directly for use in China's indiscriminate mass surveillance programmes, with the risk of being used against Uyghurs and other predominantly Muslim ethnic groups throughout the country.

Amnesty's investigation identified the sale of three different types of digital surveillance technologies to Chinese

Morpho, which is now part of Idemia, a French multinational, was awarded a contract to supply facial recogni directly to the Shanghai Public Security Bureau in 2015.

Axis Communications, a Swedish company, even boasts on its website of its involvement in expanding surveillance state. Axis develops and markets network cameras, which specialize in security surveilla monitoring.

Noldus Information Technology, a Dutch company, sold emotion recognition systems to public enforcement-related institutions in China. The company's "FaceReader" software is used fo expressions that convey anger, happiness, sadness, surprise and disgust.



Ban Facial Recognition Europe

LEGAL COMPLAINT

Complaint submitted in February 2021 by the campaign for the permanent ban of Facial Recognition used for identification and profiling in all of Europe.

#BAN
FACIAL
RECOGNITION
EUROPE

The complaint package is composed of the following:

- The claims of violations (list of articles and regulations in EU)
- The evidence of violations (list of cases of FR uses in EU)
- The evidence of the will of the people (50,000 signatures)

This legal complaint is delivered to the European Data Protection Supervisor (EDPS) for asking them to exercise their mandate by ensuring that the European Commission and EU institutions are upholding their data protection obligations. This package is also sent to the European Commission to take enforcement action against the States that are currently violating EU fundamental rights and to the European Parliament to debate and pass a resolution supporting the ban of Facial Recognition.

Uses of Facial Recognition technology in Europe led to abuses of fundamental rights, lack of accountability, and misspending of public funds for several years. European institutions are responsible for not enacting a clear legal framework concerning Facial Recognition technology and not enforcing actions for violations of existing regulations.

LEGAL CLAIMS

The listed cases of use of Facial Recognition in EU must be considered in violation of articles in the Charter of Fundamental Rights of the EU, the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), European Data Protection Board Guidlines, European Convention on Human Rights, and the Council of Europe Data Protection Convention.

- Directive (EU) 2016/680
The Police and Criminal Justice Authorities Directive, also known as Law Enforcement Directive (LED), defines the processing of personal data by authorities dealing with criminal offences and evidence by police. Facial Recognition uses are violating fundamental rights in the Article 10 of this Directive, which states that every biometric data used in order to identify individuals is only possible “where strictly necessary” and “subject to appropriate safeguards for the rights and freedoms of the data subject”.

- General Data Protection Regulation
In the General Data Protection Regulation (GDPR) violations with Facial Recognition concern the Article 9 with the idea that the processing of biometric data for identification is forbidden. Also Article 6 is violated when there aren’t the conditions under which personal data can be legally processed, one such requirement being that the data subject has given their explicit consent.

- EDPB Guidelines 3/2019
The European Data Protection Board (EDPB) on 29 January 2020 adopted guidelines on the processing of personal data through video devices which has a dedicated section on special categories such as biometric data. The scope of application is GDPR, thus the guidelines generally apply to companies and authorities other than law enforcement and intelligence services. An instance of violation with Facial Recognition is with the point 66 of the guidelines: "the data controller should always try to minimize the risk of capturing footage revealing other sensitive data regardless of the aim."

The human rights violations concerning privacy apply with the use facial recognition and the following institutions define them:

- European Convention on Human Rights:
Article 8, “It provides a right to respect for one's private and family life, his home and his correspondence”.

- Council of Europe Data Protection Convention:
Principles 108, about "the collection and processing of biometric data”.

- European Court of Human Rights:
Article 12, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation."

- Charter of Fundamental Rights:
Article 11, "Freedom of assembly and association" The notion of anonymity is a prerequisite to join a political protest in public spaces.

Beyond privacy and surveillance, facial recognition infringes human dignity and enables social discrimination, therefore more violations of fundamental rights would apply to this legal complaint.

This legal complaint is addressed to the following institutions:
European Data Protection Supervisor, European Data Protection Board, European Union Agency for Fundamental Rights, Council of Europe, European Commission, European Parliament.