Use cases: Impermissable AI and fundamental rights breaches

This briefing has been compiled to assist policymakers in the context of the EU's regulation on artificial intelligence. It outlines several cases studies across Europe where **artificial intelligence is being used in a way that compromises EU law and fundamental rights, and therefore requires a legal prohibition or ban**.

August 2020

Grave concerns remain as to how artificial intelligence (AI) will impact people, communities and society as a whole. Some AI systems have the ability to **exacerbate surveillance** and intrusion into our personal lives, reflect and **reinforce some of the deepest societal inequalities**, fundamentally alter the delivery of public and essential services, vastly undermine vital data protection legislation, suppress freedoms of expression and assembly, and disrupt the democratic process itself.

In European Digital Rights' explainer, EDRi details some of the implications of AI on fundamental rights. In EDRi's recommendations for a fundamental rights-based regulation on artificial intelligence, EDRi outlines the need for **clear legal limits on the uses of AI**, legal criteria for, democratic oversight, and the need for a **prohibition on impermissable uses of AI.**

EDRi recommends the European Commission draw red-lines for AI, in particular in these areas:

- Indiscriminate biometric surveillance and biometric capture and processing in public spaces, including public facial recognition;
- **use of AI to determine access to or delivery of essential public services (such as social security, policing, migration control);**
- uses of AI which purport to identify, analyse and assess emotion, mood, behaviour, and sensitive identity traits (such as race, disability) in the delivery of essential services;
- **predictive policing;**
- **use of AI systems at the border or in testing on marginalised groups, such as undocumented migrants;**
- autonomous lethal weapons and other uses which identify targets for lethal force (such as law and immigration enforcement);
- general purpose scoring of citizens or residents, otherwise referred to as unitary scoring or mass-scale citizen scoring.

Further information on EDRi's recommendation to the Commission on fundamental rights-based regulation on artificial intelligence: https://edri.org/wp-content/uploads/2020/06/AI_EDRiRecommendations.pdf

More information on biometric processing and capture in publicly accessible spaces can be found in EDRi's position paper on Biometric Mass Surveillance, where EDRi calls for an **immediate and indefinite ban** on biometric mass surveillance.

Table of Contents

I. Use of AI to determine access to or delivery of essential public services

DENMARK: Gladaxe system

In Denmark in 2018 three local authorities asked for exemption from data protection rules to run an experiment to trace children with special needs from a very early stage. The purpose was to trace children who were vulnerable due to social circumstances even before they showed actual symptoms of special needs. Based on previous use of statistics, the authorities decided to combine information about 'risk indicators', to determine neighbourhoods to be characterised as 'ghettos', based on an automated algorithmic assessment.

Indicators included unemployment levels, crime rates, educational attainment and other 'risk indicators', as well as whether the levels of first and second-generation migrants in the population is more than 50%. Individuals from neighbourhoods which meet these criteria are classified as 'ghettos'. The model used a points-based system, with parameters such as mental illness (3000 points), unemployment (500 points), missing a doctor's appointment (1000 points) or dentist's appointment (300 points). Divorce was also included in the risk estimation, which was then rolled out to all families with children.

These neighbourhoods are then subject to special measures, including higher punishments for crimes, putting children into public day care at an early age, lifting the protection of tenants in order to privatise public housing, tearing down entire building blocks and—indeed—applying the automated risk assessment system for families with children. This program poses **clear discrimination risks** and a lack of equal treatment on the basis of race, ethnicity and migration background.

Source: Algorithm Watch, 'Automating Society' (2019), https://algorithmwatch.org/en/automating-society-denmark/

UNITED KINGDOM: Harm Assessment Risk Tool ('HART')

Harm Assessment Risk Tool ('HART'), used by Durham Constabulary in the United Kingdom is based on a machine-learning algorithm to assess a suspect's risk of reoffending, using over thirty variables that characterise an individual's criminal history and socio-demographic background. The risk assessments conducted by HART are used by the local police to determine whether an individual should be charged, or diverted into a rehabilitation programme. HART's assessment can trigger a chain of events that can result in the deprivation of liberty, and/or a criminal conviction. Rather than basing such charging decisions on individual cases, HART **creates profiles** for entry into diversion programs on the **basis of sensitive and personal information**. **Clear examples of racial discrimination** in this system include the use of the 'Mosaic' code developed by a consumer credit reporting company, that categorised individuals into various groups according to *inter alia* ethnic origin, income, and education levels. Some socio-demographic categories used by Mosaic were highly racialised, including, for example, 'Asian Heritage', which stereotyped individuals of 'Asian' origin as being unemployed or having low-paid jobs, and living with extended families.

Source: Marion Oswald et al., 'Algorithmic risk assessment models: lessons from the Durham HART model and Experimental proportionality' Information & Communications Technology Law, Vol 27, Issue 2 (2018)

DENMARK: Tværspor research project

This automated risk assessment experiment in the field of social welfare is a project that measures chronically ill patients' behaviour in order to estimate when or how further efforts are necessary, namely whether patients should be admitted to hospital with severe conditions. The aim of this project is that it creates a tested model for assessing the individual patient's risk profile and for offering a cross-sectoral effort that can be extended to several clusters.

Source: Algorithm Watch, 'Automating Society' (2019), https://algorithmwatch.org/en/automating-society-denmark/; https://www.rm.dk/om-os/aktuelt/nyheder/nyheder-2017/april-17/ny-viden-om-patientadfard-skal-gore-sundhedsvasenet-mere-proaktivt/

NETHERLANDS: SyRI Case

SyRI is a risk profiling system used by the Dutch government, that linked and analysed large amounts of personal data of citizens, such as data on identity, labour, movable and immovable property, education, pension, business, income and assets, pension and debts. SyRI was used to prevent and combat abuse of social security provisions, tax and contribution fraud and non-compliance with labour laws.

The profiling of citizens by SyRI created risk reports: so-called "surprise addresses" with an increased risk of fraud. These people were registered, after which they could be subject to criminal and administrative investigations and sanctions. Every inhabitant of the Netherlands was 'suspected in advance' by the government's use of SyRI.

In 2014, a coalition of civil society organizations initiated strategic litigation on SyRI against the Dutch State. The manner in which the government used SyRI against its citizens and thus **processed large amounts of data was unprecedented, undemocratic and subject to serious human rights objections**.

On 5 February 2020, the District Court of The Hague ruled that SyRI was in violation of the European Convention on Human Rights. According to the Court, SyRI constituted a **disproportionate invasion of the private lives** of citizens. This did not only apply to people who were identified by SyRI as being at increased risk, but to everyone whose data was analysed by SyRI. According to the District Court, SyRI was **not transparent** and therefore not verifiable. The invasion of privacy was unforeseeable for citizens and they could not defend themselves against it. The Court also mentioned the actual risk of **discrimination and stigmatization** of citizens, based on **socio-economic status and possible migration background,** in so-called 'problematic neighbourhoods', where SyRI has already been deployed. According to the Court, the deployment of SyRI is accompanied by a risk of prejudice, but this risk cannot be controlled.

Source: https://pilpnjcm.nl/en/dossiers/profiling-and-syri/

POLAND: Random Allocation of Cases

In Poland, since the beginning of the 2018, the system of Random Allocation of Cases to Judges (also as "System") began to be used in all common courts to randomly assign judges to cases. The use of this System means that the **algorithm determines which judge will receive a specific case to be heard**. The Foundation, recognizing that the use of algorithms in the judiciary should be used extremely carefully, wanted to know the rules of its functioning.

In December 2017, the Foundation filed an application for access to public information to the Minister of Justice, and asked for access to an algorithm on the basis of which the Random Allocation of Cases System operates. The Minister **refused to provide information** covered by the Foundation's application and pointed out that the algorithm consists of technical information, is not public information within the meaning of the Polish Act on Access to Public Information, and therefore is not subject to disclosure. Then, in December 2017 the Foundation filed an action for failure to act of the Minister before the Court, considering that the algorithm that determines how individual judges are assigned to hear cases is public information and should be available to citizens.

Source: https://epf.org.pl/en/2019/07/09/do-you-know-what-your-algorithms-are-up-to/ ; https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/not-fully-transparent

SPAIN: BOSCO and Bono Social de Electricidad

The Bono Social de Electricidad is a discount on energy bills to at-risk individuals and families. The complexity of the application process and the lack of information from the administration were preventing disadvantaged groups from applying. Energy companies use BOSCO, a software created by the Spanish Ministry for Green Energy Transition, to decide who is entitled to the subsidy.

Both the government and the Council of Transparency and Good Governance denied Civio access to the code by arguing that sharing it would incur in a copyright violation. However, according to the Spanish Transparency Law and the regulation of intellectual property, work carried out in public administrations is not subjected to copyright.

Source: https://civio.es/novedades/2019/07/12/being-ruled-through-secret-source-code-or-algorithms-should-never-be-allowed-in-a-social-and-democratic-state-under-the-rule-of-law/

GERMANY: SCHUFA system

Germany's leading credit bureau, SCHUFA, can determine acceess to housing, as landlords may refuse to rent an apartment, banks may reject credit card applications and network providers will say 'no' to a new contract.

The scoring procedure of the private company SCHUFA is highly intransparent and not accessible to the public. According to the campaign OpenSCHUFA, Spiegel Online and BR who investigated this program, the determines the creditworthiness of 67 million Germans. The investigation has found a number of flaws, uncluding that this system **may reinforce discrimination** and that it has **violated the GDPR's data access provisions**.

Source: https://openschufa.de/english/

AUSTRIA: Employment Agency AMS

The Austrian employment Agency is using an algorithm to determine potential jon opportunities of unemployed people. In the recently published paper ("Algorithmic Profiling of Job Seekers in Austria: How Austerity Politics Are Made Effective"), the authors express strong concerns about the AMS algorithm.

The program will divide the unemployed into those with good, medium and bad job opportunities. People with good job market opportunities are those who are 66% likely to be able to find

employment for three months within seven months. Many variables are included in the assessment of the opportunities: for example, the place of residence of the job seeker, the previous career, the highest level of education completed, but also gender. When calculating short-term job opportunities, the individual variables mentioned have a different weight than in long-term assessment. Depending on how long someone has been unemployed, the weighting changes further.

As investigated by NGO Epicenter Works, there is not full transparency and so the impact assessment is not possible in some areas. However, the algorithm is shown to **explicitly discriminate on the ground of gender**. e.g. women with children are negatively weighted but men with children are not. In addition the system rates women 's job opportunities worse than those of men.

Source: https://algorithmwatch.org/en/story/austrias-employment-agency-ams-rolls-out-discriminatory-algorithm/

ESTONIA:

Following a reform of the work ability support system, machines and algorithms were used to automatically re-evaluate incapacity levels. Reportedly, the incomplete data in the e-health platform, coupled with a lack of in-person interviews, resulted in loss of social benefits for certain persons with disabilities and older persons with disabilities.

Source: "Governing the Game Changer – Impacts of artificial intelligence development on human rights, democracy and the rule of law".

II. Uses of AI to identify, analyse and assess emotion, mood and sensitive identity traits in the delivery of essential services

FRANCE: Behaviour prediction in Marseille

The City of Marseille is developing a system in testing phase to automatically alert the police to any "abnormal behavior" detected by its CCTV cameras. Invetsigated by La Quadrature du Net, the city revealed that the system is being designed to detect and analyse behaviors that may be considered "abnormal" in the public space (crowd starting to run, crowd linked to an event - accident, fight -, individual walking repeatedly in a space). In an internal memo dated October 29, the City nevertheless explains that "this tool is not functional to date." According to the same document, two other functions are "pending regulatory framework": a tool to reconstruct *a posteriori* "the journey of an individual from the archives of several cameras" and a sound detection module.

Such a system linking biometric capture and processing with the delivery of public services poses severe risks to fundamental rights, **data protection and often does not meet standards of justification in law, necessity or proportionality.**

FRANCE: Emotion recognition programs (several)

Two-I. Initial project: on trams in Nice (but not conducted due to backlash). Sold to Alain Behm (Mobil Security, a crow control gate which will be used in the 2024 French Olympics, and was used for the Environment Ministers' 2019 G7 in Metz). Sold to a casino (for identifying compulsive gamblers).

Partnership in Dubai to rank neighbourhoods according to "happiness levels", and try to bring the features conducive to happiness to the unhappy neighbourhoods.

Trial with volunteer patients in private hospitals in Metz, France.

Source: https://www.republicain-lorrain.fr/edition-de-metz-ville/2019/08/05/l-algorithme-de-two-i-mesurera-votre-douleur

FINLAND: DigitalMinds

DigitalMinds aims to eliminate the human participation in the recruiment process, in order to make the personality assessment process 'faster' and 'more reliable', according to the company. Since 2017 it has used public interfaces of social media (Twitter and Facebook) and email (Gmail and Microsoft Office 365) to analyse the entire corpus of an individuals' online presence. This results in a personality assessment that a prospective employer can use to assess a prospective employee. Measures that are tracked include how active individuals are online and how they react to posts/emails. Such techniques are sometimes complemented with automated video analysis to analyse personality in verbal communication.

Source: https://equineteurope.org/wp-content/uploads/2020/06/ai_report_digital.pdf

GERMANY: Affective Computing

Some companies and scientists present Affective Computing, the a**lgorithmic analysis of personality traits** also known as "artificial emotional intelligence", as an important new development. But the methods that are used are often dubious and present serious risks for **discrimination**.

Companies that use Precires's software **can select the characteristics their applicants** should have to be considered for a position. If a company uses characteristics based on their existing senior management staff – however they are measured – to create a profile for future managers, there is a **real risk that only people with comparable characteristics are hired or promoted**. Yet the company uses precisely these sorts of speech profile analyses of people in leadership positions to promote the company.

Source: https://algorithmwatch.org/en/story/speech-analysis-hr/

ITALY: Redditometro

The Italian Revenue Agency, using a tool called *Redditometro,* created profiles, which were based, amongst others, on assumed expenses made by taxpayers deduced, according to statistical parameters, from their allocation in specific family categories or geographical areas. This profiling tool was investigated by the Italian DPA, the *Garante*.

One of the main issues was the low quality of the data and the resulting high error rate based on unreliable inferences drawn from the data. On the basis of its investigation, the *Garante* prescribed that a taxpayer's real income could only be calculated from actual, documented expenses, and not deduced from statistically-based assumptions of levels of expenses.

Source: https://www.garanteprivacy.it/en/home/docweb/-/docweb-display/docweb/2765110

III. Predictive policing

NETHERLANDS: ProKid 12-SI

In the Netherlands, the government has used an algorithmic risk assessment tool, **ProKid 12- SI,** which purports to assess the risk of criminality of 12-year-old children since 2009. ProKid uses existing police data on these children, such as reports of where children have come into contact with the police, their addresses, information about their 'living environment', even including whether they are victims of violence, to identify them as being in one of four categories of 'risk' of committing crimes in future. The system **assesses children based on their relationships** with other people and their supposed risk levels, **meaning that individuals can be deemed higher risk by being linked to another individual with a high risk assessment,** such as a sibling or a friend. Parents' assessed risk can also impact a child's risk level. ProKid's algorithms **assess risks in relation to future actions** that the children have not yet carried out, and judges them on the basis of the actions of others close to them.

These risk assessments result in police 'registering' these children on their systems and monitoring them, and then referring them to youth 'care' services. ProKid frames children as potential perpetrators even when they are registered as victims of violence; which has serious implications on their presumption of innocence. As such, the ProKid 12-SI raises severe concerns relating to **rights of the child**, the **right to non-discrimination** based on a number of protected characteristics, the **presumption of innocence** and **data protection rights**.

Source: K La Fors-Owyczynik, 'Profiling 'Anomalies' and the Anomalies of Profiling: Digitalized Risk Assessments of Dutch Youth and the New European Data Protection Regime' (2016), https://link.springer.com/chapter/10.1007/978-3-319-48342-9_7)

DENMARK: Gladaxe system

See above (Use of AI systems to determine access to public services)

Source: Algorithm Watch, 'Automating Society' (2019), https://algorithmwatch.org/en/automating-society-denmark/

ITALY: KeyCrime

KeyCrime is predictive policing software based on an algorithm of criminal behaviour analysis. It was designed to automatically analyse criminal behaviour, help identify trends and suggest ways of thwarting future crimes.

Reportedly, the system can now sift through some 11,000 variables for each crime. These range from the obvious (time, location and appearance) to the less obvious (reconstructions of witnesses and suspects during subsequent interviews, and even the modus operandi of the criminal). Video feeds are included in the analysed data. The idea behind the software is to rationalise the use of the police force and automatically deploy officers exactly where they are needed.

Source: https://algorithmwatch.org/en/automating-society-italy/

SWITZERLAND: Precobs, Dyrias and ROS

Precobs: The Precobs system purports to predict where burglaries will occur from past data, based on the assumption that burglars often operate in small areas. The focus is on the detecting a cluster of burglaries, and directing police resources into those neighbourhoods.

Dyrias: The "dynamic system for the analysis of risk" program purports to predict the likelihood that a person will harm their intimate partner. Using police perceptions data, this algorithm outputs a likelihood score. 3,000 individuals were labeled "dangerous" in 2018 (but the label might not be derived from using Dyrias).

ROS: German-speaking cantons in Switzerland use ROS (an acronym for "Risikoorientierter Sanktionenvollzug" or risk-oriented execution of prison sentences) to label prisoners into categories when based on likelihood of recidivism. These classificatons generally cannot be changed and determine privileges and other decisions in the criminal justice system.

These programs **disproportionately target people from working class and other marginalised communities**, although there is a lack of data relating to race and ethnicity. According to Algorithm Watch, "[v]ery little public information exists on Precobs, Dyrias and ROS. The people impacted, who are overwhelmingly poor, rarely have the financial resources needed to question automated systems, as their lawyers usually focus on verifying the basic facts alleged by the prosecution."

Algorithm Watch, 'Automating Society' (2020), forthcoming,

https://algorithmwatch.org/en/story/swiss-predictive-policing/

UNITED KINGDOM Gangs Violence Matrix

The Gangs Matrix was launched the Metropolitan Police in 2012 as a database of suspected gang members in London. It purports to be a risk-management tool focused on preventing serious violence by identifying potential 'gang' members. However, according to a series of vague indicators, the database collects information of individuals who have never been involved with violent crime.

Even being a victim of a crime that the police link to a gang is viewed as an indicator of a likelihood of 'subsequently becoming drawn in to involvement in serious crime' and can result in the individual being placed on the Matrix.

The police also share the Matrix with other agencies, such as job centres, housing associations, and educational institutions, **leading to discrimination against individuals on the basis of their supposed gang affiliation**. Depending on the nature of the way this information is shared, this poses an opportunity for possible violations of the **right to privacy and may affect housing and employment rights on a discriminatory basis**. Those whose names are on the Matrix experience multiple stop and search encounters which seemingly lack any legal basis. Some report that police have stopped and searched them 200 times, others report up to as many as 1,000 times, with some reporting multiple stops everyday.

This has an impact on individuals' **rights to freedom from interference with their privacy** and their **freedom from arbitrary arrest** on an ethnically discriminatory basis. Matrixes like the gang matrix **violate the right to non-discimination** in that generally, racial, ethnic minorities are overrepresented, and vastly disproportionate to corresponding crime figures. As such, they are likely to **codify racialised policing practices alongside infringements on data protection rights**. 78 per cent of individuals on the Matrix are black, and an additional 9 per cent are from other ethnic minority groups, while the police's own figures show that only 27 per cent of those responsible for serious youth violence are black.

Source: Amnesty UK 'What is the Gangs Matrix?' https://www.amnesty.org.uk/london-trident-gangs-matrix-metropolitan-police

NETHERLANDS: Crime Anticipation System

In Amsterdam, the Crime Anticipation System is a place-based predictive policing tool which attempts to predict where **specific crimes**, such as burglary, muggings and assaults will take place within a two-week period. Amsterdam Police developed the system to predict more at-risk areas in a city, and improve efficient distribution of their workforce. The system uses machine learning to analyse three sources of data: socio-economic data from the Central Bureau of Statistics which includes people's age, incomes and the amount of social benefits in an area; historical crime data, originally gathered by the police, focusing on previous crimes, locations and known criminals; Geo-data from the Municipal Administration which consists of streets and addresses. The aim of the analysis is to grade different areas of Amsterdam into red, orange and yellow. **Areas graded red are considered high-risk and have increased police surveillance deployed to prevent predicted crimes from occurring.**

Amongst the indicators used by CAS to predict crimes in a particular area was the number of '**non-Western allochtones**' in the area – in other words, 'non-Western' individuals with at least one foreign-born parent. This **presupposes the existence of a correlation between ethnicity and crime**, and singles out a category of ethnicities to be of particular concern, given that the presence of 'Western', 'autochtone' individuals were not included in the indicators. Furthermore, given that 'Western' was defined somewhat subjectively (for example, including individuals of Japanese or Indonesian origin, and including all European nationalities, apart from Turkish), CAS incorporated highly questionable societal categorisations and biases.

Although not directed at individuals, place-based predictive policing systems still present a range of **data protection risks and a clear cases of discrimination on the grounds of ethnic origin.** In particular, the use of automated decision making systems to target policing to certain areas deemed 'high crime' can further overpolicing of certain communities and further embed existing bias and inequalities in policing data which already profile individuals from racial ethnic and religious minority communities, working class and other marginalised groups as posing a higher risk of committing crime.

Source: European Network Against Racism (2019). Data Driven Policing: Hardwiring Discriminatory Policing Practices in Europe: https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf; Oosterloo, S. at al. (2017) 'The Politics and Biases of the "Crime Anticipation System" of the Dutch Police'. Available at: http://ceur-ws.org/Vol-2103/paper_6.pdf

ITALY: Video surveillance and the prediction of 'abnormal behaviour'

In 2020, Hermes Center investigated the deployment of a so-called "innovative video surveillance" system in Tokamachi Park, Como. This advanced and potentially very intrusive system has been designed to perform facial recognition on all passers-by, **including predicting when they are "loitering" or "trespassing"**. Hermes Center obtained the Data Protection Impact Assessment (DPIA) for the system and discovered that it was poorly written; **did not risk-assess the enhanced fundamental rights issues** implicated by facial recognition compared to video surveillance; and showed a **lack of awareness for the fact that the system was already unlawful within the Italian legal framework**.

Subsequently, the Italian Data Protection Authority (DPA), the Garantie Privacy, struck down the system as having **no legal basis**, showing that the Como authorities had **wasted public money**.

Source: (investigated by Hermes Center) https://www.wired.it/internet/regole/2020/06/09/riconoscimento-facciale-como/

UNITED KINGDOM: Offender Group Reconviction Scale

The Offender Group Reconviction Score (OGRS) is a predictor of re-offending based on static risk such as age, gender and criminal history to calculate individual predictions. The tool is employed by probation and prison services across Europe and uses an algorithm to calculate the likelihood of reoffending (which is expressed as a percentage score).

The use of key variables such as age at first sanction (including warnings, (never) cautions, etc) and age at first conviction is likely to create **discriminatory effect on minority ethnic groups** namely, age at first sanction (including warnings, (never) cautions, etc) and age at first conviction. Given the effects of suspicion which result in increased levels of police stops, it is logical that the calculation of their risk of reconviction will be higher, not as a consequence of criminal activity, but as a consequence of the increased likelihood of being stopped by the police and law enforcement agencies.

Source: European Network Against Racism (2019). Data Driven Policing: Hardwiring Discriminatory Policing Practices in Europe: https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf; Research summary 07/09, OGRS 3: the revised Offender Group Reconviction Scale: https://core.ac.uk/download/pdf/1556521.pdf

BELGIUM: Zennevallei

The Zennevallei police zone will be working on a project on 'predictive policing' with Ghent University over the next two years. In 'predictive policing' it comes down to the fact that the police zone knows, on the basis of predictions, which location in the zone is a risk area for burglaries and other crimes.

This program will be developed by a doctoral student at Ghent University. First and foremost, she conducts a consultation round in which she collects 'big data' about all kinds of facts. That information goes much further than just a location and time, but also, for example, what the weather was like at the time. All that information will then be mapped.

A question has been tabled in the Belgian senate about this case. In the government's written response it was stated that 'The federal police also aims to improve their analytical capacity to move towards predictive policing.' Later, "my administration considers it important above all to properly build the basis of what will make the "predictive policing" ", Ie the data. **Too often, the data exploited are police statistics and only these. By doing so, we instill a bias in the system and we force the algorithms to reproduce prejudices and misinterpretations of the facts. Police statistics primarily reflect police activity. They do not reflect the criminal reality of a given territory.** "

Source: https://www.senate.be/www/?MIval=/Vragen/SVPrintNLFR&LEG=7&NR=591&LANG=nl

BELGIUM: iPolice

Predictive policing becomes possible thanks to the introduction of a new police computer system in 2020: iPolice. Ipolice uses databanks and algorithms help to identify times and spots when and where there is a heightened chance of criminal activity.

Belgian police are currently creating the tools and building the system. Data will then be introduced to allow links to be made. Data will be supplied by the police but also by outside agencies like the Met Office. Police spokesman Theyskens stresses that predictive policing is an aid and no magic ball. He argues that" Ethnic profiling will not be allowed! We have no intention to come to a Big Brother databank".

Source: https://www.vrt.be/vrtnws/en/2018/08/30/police-to-use-algorithms-to-predict-crime/ ; https://issuu.com/fedpolbelgium/docs/18_ir03_full_fr_web

UNITED KINGDOM: National Data Analytics Solution (NDAS)

The National Data Analytics Solution ('NDAS') risk assessment tool uses statistical analysis and machine-learning to inform policing decisions, develop a list of individuals with a future likelihood to commit crimes, and to facilitate 'early interventions' where appropriate.

The sources of data that the system uses to conduct its risk assessments raise concerns that the system will be built to **profile individuals on the basis of very sensitive, personal information**, including stop and search data, data from social services, and the National Health Service. Where this data is used to indicate the likelihood of individuals' criminality, it will inevitably flag up people whose profiles fit those who are over-represented in that data as being higher risk, prima facie infringing on certain individuals **right to non-discrimination and equal treatment**. It is particularly worrying that an individual might be profiled for policing purposes on the basis of their health conditions or their access to essential services, such as welfare or benefits.

Source: Sarah Marsh, 'Ethics committee raises alarm over 'predictive policing' tool', The Guardian (20 April 2019) https://www.theguardian.com/uk-news/2019/apr/20/predictive-policing-tool-could-entrench-bias-ethics-committee-warns

UNITED KINGDOM: Origins Software

This tool deployed by the London Metroplitan Police Force purports to profile perpetrators and victims of crime. In official statements, designers of the software said the program is intended to redirect policing and other community policing services to "enable safer neighbourhood teams to better understand the communities they serve."

However, there has been clear linkages between the use of this software to create ethnicity based crime profiles based on racialised assumptions and stereotypes of criminal behaviour. The designer of the program wrote that it is likely that "different cultures do foster differences in behaviour among their members". This system was used since 2015 by the metropolitan police, amongst other police forces in the UK. Campaigners have warned of the links between racist stereotypes, algorithmic profiling, and overpolicing of racialised communities.

Source: https://www.theguardian.com/uk-news/2020/jul/27/met-police-use-software-ethnic-groups-specialise-profile?CMP=share_btn_tw

IV. Use of AI systems at the border, in migration control or in testing on marginalised groups

EUROPE: Common Identity Repository (CIR) and Visa Information System (VIS)

These systems are included insofar as they facilitate AI and other automated systems which profile, make decisions about, and potentially discriminate against migrants and other people on the move. These interoperable databases are used alongside predictive policing, security, migration control and anti-terrorism programs to profile already marginalised communities. Through these programmes, the EU "will significantly extend the collection and use of biometric and biographic data taken from visitors to the Schengen area."

Statewatch, reporting on the Visa Information System (VIS) notes that "Data will be gathered on travellers themselves **as well as their families**, education, occupation and criminal convictions. **Fingerprints and photographs will be taken from all travellers, including from millions of children from the age of six onwards**. This data will not just be used to assess an individual's application, but to **feed data mining and profiling algorithms.** It will be stored in **large-scale databases accessible to hundreds of thousands of individuals** working for hundreds of different public authorities."

"This system, the Common Identity Repository (CIR), is being introduced as part of the EU's complex 'interoperability' initiative and aims to facilitate an increase in police identity checks within the EU. It will only hold the data of non-EU citizens and, with only weak anti-discrimination safeguards in the legislation, raises the risk of **further entrenching racial profiling in police work**. [...] Furthermore, the last decade has seen numerous states across the EU turn their back on fundamental rights and democratic standards, with migrants frequently used as scapegoats for society's ills. In a climate of

increased xenophobia and social hostility to foreigners, it is extremely dangerous to assert that intrusive data-gathering will counterbalance a supposed threat posed by non-citizens."

Source: Statewatch Automated Suspicion: The EU's new travel surveillance initiatives (2020) available at: https://www.statewatch.org/automated-suspicion-the-eu-s-new-travel-surveillance-initiatives/

EUROPE: Military Drones at borders

Frontex, the European Border and Coast Guard Agency, has been testing unpiloted military-grade drones in the Mediterranean for the surveillance and interdiction of migrant vessels hoping to reach European shores to file asylum applications.

While 'smart-border' technologies have sometimes been called a more 'humane' alternative to physical barriers, using invasive surveillance technologies can push migration routes towards more dangerous terrains, potentially resulting in more deaths in the Mediterranean as more migrant boats are prevented from reaching the shores of Europe.

Source: Raluca Csernatoni, 'Constructing the EU's High-Tech Borders: FRONTEX and Dual-Use Drones for Border Management' (2018) 27 European Security 175.

EUROPE: Frontex scales up AI uses in border control

Frontex announces plans to scale up various projects involing the use of AI in migration control. These include: intuitive user interfaces and wearables supported by Artificial Intelligence and with Augmented Reality capabilities, 3D facial and iris verification technology for "real-on-the-move" border crossing experience, digital identity based on blockchain technology, highly accurate and cost effective handheld devices for drug and precursors detection on the field.

The projects in question include: ANDROMEDA, ARESIBO, BorderSens, COMPASS2020, D4FLY, MIRROR and PERCEPTIONS. These address a wide spectrum of technological capabilities critical for border security, including unmanned platforms, document fraud detection, situational awareness, artificial intelligence, augmented reality, integrated systems and identification of illicit drugs and their precursors.

Source: https://frontex.europa.eu/media-centre/news-release/frontex-helping-to-bring-innovation-to-future-border-control-VetIX5

HUNGARY, GREECE: iBorderCtrl

In airports in Hungary and Greece, a pilot project by a company called iBorderCtrl, funded by Horizon2020 in the EU for 4 million Euro, introduced AI-powered lie detectors at border checkpoints. The company alleged that people's faces would be monitored for signs of lying, and if the system becomes more 'skeptical' through a series of increasingly complicated questions, the person will be selected for further screening by a human officer.

Various groups including EDRi and Amnesty International have challenged the iBorderCTRL project, outlining the major fundamental rights abuses, **including discrimination, data protection and the infringement on the right to dignity.** Most notably, the Greek NGO Homo Digitalis, member of EDRi, filled a petition to the Greek Parliament, underlining the lack of transparency and calling for a full data protection impact assessment, echoed by Member of the European Parliament Patrick Breyer from the Green Party, who launched a legal challenge to the EU Commission's Research Agency refusal to disclose ethical assessments of the iBorderCTRL system.

Source: https://edri.org/immigration-iris-scanning-and-iborderctrl/; https://www.amnesty.org/en/latest/news/2019/03/automated-technologies-and-the-future-of-fortress-europe/; https://www.homodigitalis.gr/en/posts/3044 with full text of petition here https://www.homodigitalis.gr/wp-content/uploads/2018/11/05.11_HomoDigitalis_Petition_iBorderCtrl.pdf

Further research into iBorderCTRL and similar systems at EU borders has emphasised the "profound human rights ramifications and real impacts on human lives" in the use of biometric and other border technologies, such as **the EU's iBorderCTRL**, on vulnerable and/or marginalised groups such as refugees and people on the move. The project emphasises the significant **human rights threats posed by the discriminatory outcomes that can arise when culturally-specific actions or behaviours are interpreted by an algorithm**, as well as the **privacy and security threats to asylum seekers** by the use of these technologies at borders. The work foregrounds the lived experiences of people on the move, as these perspectives are often left out of policy conversations on these far reaching technological experiments, including the **coercive collection of biometric information in humanitarian settings such as refugee camps.** The project also examines the **responsibility of various actors, including state entities, the private sector, and international organizations such as UN agencies in sharing of data about refugees without appropriate safeguards**.

Sources:

(1)https://www.nytimes.com/2020/04/15/opinion/coronavirus-surveillance-privacy-rights.html

(2)https://edri.org/the-human-rights-impacts-of-migration-control-technologies/

(3)https://edri.org/accountable-migration-tech-transparency-governance-and-oversight/

(4)https://www.cigionline.org/articles/privatization-migration-control

(5)https://www.researchgate.net/publication/337780154_Technology_on_the_margins_AI_and_global_migration_management_from_a_human_rights_perspective

UNITED KINGDOM: UK Home Office Visa Algorithms

In 2019 the Joint Council for the Welfare of Immigrants (JCWI) and the Foxglove legal team, have launched a legal case challenging the discriminatory nature of the secretive visa algorithms used by the UK Home Office in what they are calling a 'digitally hostile environment.'

In the submission to the UK High Court which has granted judicial review, the group alleged that the algorithms has created three separate streams or channels for applications, including a so-called fast-lane that could lead to "speedy boarding for white people" to enter the country. The case alleges that **applications from people whose nationalities may be flagged under various categories receive a higher risk rating**, becoming subjected to far more intensive scrutiny by Home Office officials, taking longer to reach a decision and were much more likely to be refused. The case alleges that this type of risk streaming results in **racial discrimination** and therefore breaches the 2010 Equality Act.

On the 7th August 2020, the Home Secretary Priti Patel announced the intention to end the use of the streaming algorithm. The government has pledged a full review of the system, including for issues of 'unconscious bias' and discrimination.

Source: https://www.theguardian.com/uk-news/2020/jun/18/home-office-legal-challenge-digital-hostile-environment ; https://eachother.org.uk/digital-hostile-environment/; https://www.foxglove.org.uk/news/home-office-says-it-will-abandon-its-racist-visa-algorithm-nbsp-after-we-sued-them

SLOVENIA: BORDER AI

The Delo newspaper report stated that the police have acquired information about almost 800,000 airline passengers (so-called Passenger Name Records, PNR) since October 2017. An algorithmic system tagged 8,928 passengers who were then thoroughly inspected before entering the country. The police stated that 40 per cent of those passengers were tagged as "not suspicious" and will not be reported next time they come to the border. Airline companies provided the data.

A police spokesperson explained they are not using algorithmic decision-making systems in this process. The system automatically matches a passenger to "other police data" such as criminal files. If a match is positive, a border police officer is informed and required to manually verify the information before inspecting a passenger. The police system also flags passengers who are using "unusual or illogical flights".

The Slovenian Human Rights Ombudsman and the Information Commissioner stated that such a system is not constitutional and filed a formal complaint in 2017. [The Information Commissioner claimed that the adopted changes of the amended law on the duties and powers of the police, which gave the police the power to gather the PNR, have legalised some **excessive and inadmissible** measures for gathering personal data **without sufficient protection of citizens that have not been accused or suspected of any wrongdoings**, e.g. terrorism or organised crime. They argued that all passengers should not be routinely scanned at the airport just because they are entering the state or landing during the transfer. The Human Rights Ombudsman supported their claims and the Slovenian Constitutional Court will therefore be required to rule on the constitutionality of the latest revision of the law on the duties and powers of the police.

Source: https://algorithmwatch.org/en/automating-society-slovenia/

GREECE: SPIRIT Project

Greece and other EU borders: social media-scraping SPIRIT project funded by Horizon2020 does experiments with genuine end-users (investigation by Homo Digitalis)

The example of the Horizon 2020-funded SPIRIT project reinforces the lack of fundamental rights compliance, transparency and accountability in a social media scraping use-case. 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 Szcytno (PL). According to the website, the project aims to use tools such as face extraction and matching, to **correlate information from social media data,** which **constitutes a form of mass surveillance,** and to continuously initiate complex associative searches over all sources relevant to criminal investigation. According to freedom of information requests, **trials are planned for 2020 and 2021, including with genuine end users (i.e. potentially vulnerable migrants at EU borders) - despite the project purportedly being only an experiment.**

Source: https://www.asktheeu.org/en/request/7495/response/25180/attach/2/REA%20reply%20confirmatory%20signed.pdf?cookie_passthrough=1

V. Biometric Surveillance

ITALY: SARI facial recognition

Facial recognition system threatens fundamental rights and fails to demonstrate lawful basis (investigated by Hermes Center)

In 2017, Hermes Center reported on the Italian Ministry of Interior's purchase of a facial recognition system called "SARI". They found that according to the Ministry's contract, the system would be used in both "Enterprise" (at rest) and "Real-Time" (live) modes, **including at "public demonstrations"**, which could lead to a **chilling effect on freedom of expression and assembly**, supported by a **mass database of 10 million images.** At the time of purchase, a lawyer confirmed that **Italy had "no warranty provision that specifies the ways and limits of capture and related database management**". Hermes Center's investigation also found a lack of transparency/information, and a contractual requirement to use an algorithm approved by the NIST committee despite the committee not having tested any algorithms for accuracy of video sequencing, creating a risk of mistaken identity. (1)

Further investigations by Hermes Center in 2019, including using freedom of information (FOI) requests, found **inconsistencies in the details provided by authorities** about the system, including the size of the database and when the system entered into use, as well as **a disproportionate use of the system against migrants and foreigners**. The Italian data protection authority (Garante Privacy) is still investigating the Real-Time mode of SARI, although FOI requests show that **the Ministry of the Interior has since stopped replying to the DPA**. (2)

Sources:

(1)https://medium.com/@ORARiccardo/italian-police-has-acquired-a-facial-recognition-system-a54016211ff2

(2)https://www.wired.it/attualita/tech/2019/04/03/sari-riconoscimento-facciale-stranieri/

GREECE: 'Smart' policing

Smart policing project suspected of violating data protection rights; Hellenic police fail to provide information to the contrary (investigated by Homo Digitalis)

In 2019, the Hellenic Police signed a €4 million contract with Intracom Telecom, for a smart policing project, majority funded by the European Commission's ISF fund. Based on the provisions of the Directive 2016/680 (LED) and the Greek Law 4624/2019 implementing it, Homo Digitalis asked the Minister of Citizen's Protection whether or not the Hellenic Police had consulted the Hellenic Data Protection Authority (DPA) on this matter and/or conducted a related Data Protection Impact Assessment (DPIA) and what the applicable safeguards are, as well as to clarify the legal provisions that allow for such data processing activities by the Hellenic Police.

In February 2020, the Hellenic Police replied but **neither confirmed nor denied that a prior consultation with the Hellenic DPA took place or that a DPIA was conducted**. Moreover, Homo Digitalis claims that **the Hellenic Police did not adequately reply about the applicable safeguards and the legal regime that justifies such data processing activities**.

With this request, Homo Digitalis claims that the processing of biometric data, such as the data described in the contract, is allowed only when three criteria are met: 1. it is authorised by Union or Member State law, 2. it is strictly necessary, and 3. it is subject to appropriate safeguards for the rights and freedoms of the individual concerned. None of the above mentioned criteria is applicable in this case. Specifically, **there are no special legal provisions in place allowing for the collection of such biometric data during police stops by the Hellenic police**. Moreover, the use of these devices **cannot be justified as strictly necessary since the identification of an individual is adequately achieved by the current procedure used**. Nevertheless, such processing activities are using new technologies, and are very likely to result in a high risk to the rights and freedoms of the data subjects. Therefore, the Hellenic Police is obliged to carry out, prior to the processing, a data protection impact assessment and to consult the Hellenic DPA.

Source: https://edri.org/facial-recognition-homo-digitalis-calls-on-greek-dpa-to-speak-up/

UK: Covert facial recognition

Covert, unlawful public-private partnership in King's Cross covered up by police (investigated by Privacy International)

In 2018, civil society organisations in the UK discovered that **a secretive facial recognition system in London's Kings Cross was the result of a 2-year partnership between the Metropolitan Police and the private owner of the site**. They found evidence of the police **unlawfully sharing images of people with a private company**, and a **failure to define what a "wanted" or suspicious person would be under law**. The Police also **dishonestly denied knowledge of the system** until investigations revealed their confirmed involvement. (1)

Further civil society reports showed that UK's deployments of biometric surveillance systems were **wrong in 9 out of 10 cases**. (2) There are additionally examples of people in the UK being stopped for covering their face in public in order to avoid the systems, undermining the idea that passers-by can be considered to consent to being surveilled by the system. (3)

Sources:

(1)https://privacyinternational.org/case-study/3973/kings-cross-has-been-watching-you-and-police-helped

(2)https://www.theguardian.com/uk-news/2018/may/15/uk-police-use-of-facial-recognition-technology-failure

(3)https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html

SERBIA, UGANDA: Government surveillance

Huawei enters into opaque and undemocratic government surveillance partnerships (investigated by Privacy International and SHARE Foundation)

EDRi members Privacy International (PI), SHARE Foundation and PI's partner in Uganda, Unwanted Witness, have been following the use of Huawei facial recognition technologies in undemocratic ways. In Serbia, the Ministry of Interior have **refused to answer freedom of information (FOI) requests** about the **deployment of 1000 cameras across Belgrade**, and have also **failed to meet their legal obligation to perform a data protection impact assessment (DPIA)**. SHARE Foundation have found evidence that footage from these cameras has at times been **leaked to the public** and at other times **gone 'missing' when it has been needed**. (1) Early reports from protests in Belgrade in July 2020 also suggest that the facial recognition systems may have been used to identify and prosecute lawful protesters.

In Uganda, the facial recognition surveillance contract between the government and Huawei has been kept secret, with **evidence that it has already been used to spy on political opponents**. There are plans to expand the system and connect it to other forms of sensitive data, which is very concerning given the lack of transparency and the fears of human rights violations. (2)

Sources:

(1)https://privacyinternational.org/case-study/3967/thousands-cameras-citizen-response-mass-

biometric-surveillance

(2)https://privacyinternational.org/case-study/3969/huawei-infiltration-uganda

ARGENTINA: Public facial recognition

Professor mistakenly stopped as a result of flawed facial recognition technology is arbitrarily detained by police (investigated by EDRi)

In 2019, a professor and small business owner called Leo Colombo in Buenos Aires, Argentina was wrongfully incriminated by a facial recognition system which had matched him to a police **database that mistakenly identified him** as a suspected robber. (1) Despite the police knowing that he was not their suspect, their **lack of control over the system** meant that they had to take Leo to the police station for a **long, distressing and wasteful process.** Whilst it was eventually resolved for Leo, **a fellow citizen with darker skin faced the same issue, and was imprisoned for 7 days** as a result of suspected technological reinforcement of unconscious bias and the reluctance of humans to override algorithms. These are socio-technological phenomena which are evidenced in a growing body of academic research. (2)

While this example occurred in Argentina, the fundamental issues (**police inability to override machine decisions**; the **power and influence of private companies to control systems and set parameters**; **abuse of data and databases**; **false arrests**; and more) are just as relevant in the EU.

Sources:

(1) https://edri.org/dangerous-by-design-a-cautionary-tale-about-facial-recognition/

(2) For example, see McGregor, L., Murray, D. & Vivian Ng. (2019). 'International Human Rights Law as a Framework for Algorithmic Accountability'. *The International and Comparative Law Quarterly,* 68(2), 309-343.

FRANCE: School facial recognition

France: court rules that facial recognition in schools violates data protection rights (investigated by La Quadrature Du Net)

In 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 for managing entry at Ampère high school in Marseille. This "trial" was intended to be a year-long experiment and was also being carried out at another school in the region (the Lycée les Eucalyptus in Nice) and was said to be held on the basis of students' and parents' consent. The intention of the system was to facilitate the job of the schools' security agents, helping them to spot identity theft and to prevent access of unauthorised persons to the school. This was designed to increase the security of students and staff and to speed up the time it took for students to enter the school premises.

As the CNIL emphasised, **a school facial recognition system is not necessary when there is the less intrusive alternative of using identity badges**. Furthermore, this use of facial recognition is **disproportionate** as it brings in a **large-scale, intrusive data surveillance program against minors** simply for the objective of school entry. (1)

Under the GDPR, there are **legal requirements for consent and for the minimisation of data**. As confirmed by the CNIL and the Marseille regional Court, the Ampère facial recognition trial significantly **violated both of these criteria**, gathering data when it was unjustified, and being fundamentally unable to obtain legitimate consent due to the power dynamics between the public authority and students. Across EU law, young people are given enhanced protections (cf. Article 8 GDPR re information society services). Under GDPR, biometric data is considered highly sensitive (Article 9(1)). The **biometric data of minors therefore requires the highest level of protections**, which Ampère did not meet. (2) (3)

Sources:

(1) https://www.cnil.fr/fr/experimenta-tion-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

(2) https://www.edps.europa.eu/sites/edp/files/publication/20-01-28_edps_quick-guide_en.pdf

(3) https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf

GLOBAL: dignity, trauma, bias, function creep

Various locations: facial recognition is violating rights to dignity, non-discrimination, due process, data protection and privacy (examples collected by Privacy International)

- "Researchers scraped videos of transgender vloggers off YouTube without their knowledge [or consent] to train facial recognition software" (2017)

- "Study: Emotion-reading facial recognition displays racial bias" (2019)
    - In this study, the faces of black men were consistently interpreted as displaying more negative emotions / anger than white men by a facial recognition algorithm.
- "Study: Facial recognition research erases trans and nonbinary people" (2019)
- "Facial recognition systems display inherent bias" (2016)
    - This includes a facial recognition algorithm labeling "non-white people as "gorillas", "animals", or "apes"" and telling "Asian users their eyes were closed when taking photographs".
- "Amazon's facial recognition software, Rekognition, incorrectly matched 28 US lawmakers to [criminal] mugshots" (2018)
- "One Ring to watch them all" (2020)
    - This piece reveals that Amazon have been training law enforcement to **circumvent investigatory warrants** by using their Ring technology, despite the fact that the technology **consistently targets black people**. There is evidence that this technology is now being used in the UK.

Further examples (collected by EDRi):

- **Increasing evidence of facial recognition leading to traumatic wrongful arrests**
    - Black man in US wrongfully arrested due to facial recognition system, highlighting serious failure of due process and investigatory standards by police. https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html
- **Lack of evidence that biometric surveillance works, challenging its grounds of necessity and proportionality**
    - "Many studies have shown that – despite claims by law enforcement and private companies – there is no link between surveillance and crime prevention. Even when studies have concluded that "at best" CCTV may help deter petty crime in parking garages, this has only been with exceptionally narrow, well-controlled use, and without the need for facial recognition." (https://edri.org/the-many-faces-of-facial-recognition-in-the-eu/)
    - "Take for example iBorderCtrl, a Horizon 2020-funded project that aims to create an automated border security system to detect deception based on facial recognition technology and the measurement of micro-expressions. In short, the EU spent €4.5 million on a project that 'detects' whether a visitor to the continent is lying or not by asking them 13 questions in front of a webcam. [...] The historical practice of lie detection is lacking in substantial scientific evidence and the AI technologies being used here to analyse micro expressions are just as questionable. [...] To make matters worse, the Commission is ignoring the transparency criteria outlined in the Ethics Guidelines by refusing to publish

certain documents, including an ethics assessment, "on the grounds that the ethics report and PR strategy are "commercial information" of the companies involved and of "commercial value"." (https://www.euractiv.com/section/digital/opinion/the-eu-is-funding-dystopian-artificial-intelligence-projects/)

- **Significant evidence of function creep and combining databases**
  - Assistant Professor at Leiden University reports on the increasing use of social media and other data in border assessments, including algorithms which systematically "assign higher risk ratings to ethnic minorities" (https://www.politico.eu/article/future-passports-biometric-risk-profiles-the-codes-we-carry/)
  - EDRi member CCC have collected information relating to the use of facial recognition by police to analyse images and videos collected during the G20 meeting in Hamburg by the police, by public transport authorities and by various third parties through a reporting platform. The Hamburg data protection authority ordered the police to delete the 17 terabytes of data that they analysed, but the police ignored the order and then took the data protection authority to court (https://netzpolitik.org/2019/datenschuetzer-scheitert-an-loeschung-biometrischer-g20-datenbank/)

- **Examples of unlawful or problematic uses stopped by national data protection authorities (DPAs)**
  - Sweden (2019) – Swedish DPA finds school facial recognition unlawful, issues fine (https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en)
  - France (2019) – French DPA finds two school facial recognition systems unnecessary and disproportionate (https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position)
  - UK (2019) – UK DPA finds use of covert facial recognition by private/public partnership "deeply concerning" (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/)
  - UK (2019) – UK DPA tells law enforcement to "slow down and justify" the use of facial recognition in public spaces (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/live-facial-recognition-technology-police-forces-need-to-slow-down-and-justify-its-use/)
  - Poland (2020) – Polish school fined for defacto mandatory fingerprint scanning system for distributing school lunches (https://uodo.gov.pl/en/553/1102)
  - Sweden (2020) – Swedish DPA launches investigation into Clearview AI (https://www.datainspektionen.se/nyheter/datainspektionen-inleder-tillsyn-med-anledning-av-clearview-ai/)

- As of July 2020, the Hamburg data protection authority is also considering opening an investigation against Clearview AI, according to investigations by CCC.
- As of July 2020, CCC have also started investigations into PimEyes, a Polish company with similar functionality to Clearview AI, for clear breaches of the GDPR. CCC have submitted a complaint to the Hamburg data protection authority.

For more information on EDRi's work across artificial intelligence and fundamental rights, please contact Sarah Chander, Senior Policy Officer, at sarah.chander@edri.org

For more information on EDRi's work on biometrics and fundamental rights, please contact Ella Jakubowska, Policy and Campaigns Officer, at ella.jakubowska@edri.org