



Working for civil liberties in Europe since 1991

c/o MDR, 88 Fleet Street, London EC4Y 1DH

www.statewatch.org

office@statewatch.org

0203 691 5227

Registered UK charity no. 1154784 | Company no. 08480724

European Commission Rule of Law Report 2023

Submission from Statewatch

This submission to the European Commission's Rule of Law Report 2023 covers a number of issues that the questionnaire does not make it possible to address adequately. Our work and the work of other civil society organisations illustrates concerns that were not sufficiently, if at all, highlighted in the 2022 report, but should be taken into account in order to provide a holistic view of threats to the rule of law in the EU. Our submission examines rule of law issues at EU level, access to an effective remedy, the admissibility of evidence, surveillance and criminalisation of the press, the admissibility of evidence in criminal proceedings, and the transparency of public decision-making.

Rule of law issues at EU level

While the Rule of Law Report focuses on the actions and omissions of member state authorities, it is evident that there are also rule of law concerns at EU level, in particular as regards EU agencies Frontex and Europol. It is therefore vital that the 2022 rule of law report does not consider the failings of the member states in isolation. Frontex is deeply embroiled in ongoing violations of human rights at EU borders, an issue that is clearly related to a flagrant disregard for the rule of law, although this submission does not discuss the issue in further detail.

With regard to Europol, the agency was found to have been illegally processing vast quantities of personal data and was not particularly cooperative with an investigation into that practice by the EDPS. A resolution was reached, but the Council and Parliament then granted Europol the power to act contrary to the EDPS decision. The EDPS is thus suing the Council and Parliament and is [explicitly arguing](#) that the rule of law and the EDPS' independence are under threat.

In another case, Europol [received the personal data of a Dutch pacifist activist](#). As it appears from the investigation of the EDPS into the refusal of the activist's access request, the agency was instructed by the Dutch authorities to delete the personal data stored in their system and ignore the subject access request. In both these cases, member states sent personal data to Europol, which further processed the data, in violation of procedural and data protection safeguards. The latter case in particular raises the question of just how much data on political activists is held by Europol, and is an issue that should be the subject of further investigation.

The EDPS has also [denounced the Europol management board's failure to consult](#) with regard to the drafting of crucial implementing decisions, despite this being explicitly required

by the new Europol Regulation. This case, as the others concerning Europol, make clear that a lack of respect for the rule of law amongst member state authorities can all too easily make its way into EU institutions and agencies.

Access to an effective remedy

Organisations working in the area of digital rights such as [European Digital Rights](#), [NOYB](#), and [Access Now](#) have pointed out serious failings in the response by national data protection authorities complaints of privacy violation, in particular against 'big tech' companies. The work of those organisations indicates a lack of training of judges and lawyers in privacy, data protection and new technologies, with a disastrous impact on the right to access an effective remedy.

This is of particular importance in the context of the increase in digital policing programs targeting vulnerable population such as migrants and asylum seekers. In Greece, a police programme aiming to obtain the facial and fingerprint biometric data of migrants has been denounced by Human Rights Watch and Homo Digitalis as being inconsistent with laws on privacy and likely to increase discrimination. [Homo Digitalis' request to the Hellenic data protection authority for an opinion](#) on the programme has gone unanswered for almost three years.

The severity of these failings is made all the more clear by the fact the abuse of data rights is evidently routine and widespread: in 2022, data protection authorities have in some cases levied record fines against abusive data practices, as in the case of [Clearview AI](#). A class-action suit against [the Dutch secret services](#) was also an important victory.

Nevertheless, it is evident that [supervisory authorities simply do not have the adequate resources](#) to fulfil their roles effectively: over 80% of national data protection authorities say their budgets are insufficient, and 86% say they do not have enough staff. The EDPS reports similar problems. Given the ongoing introduction and development of extensive new databases and information systems both by member states and, in particular, at EU level, this lack of resources and personnel will inevitably lead to an inability to ensure that the law is enforced and new powers are not abused.

Admissibility of evidence

In 2020 the [French police hacked an encrypted message server, Encrochat](#), and obtained a large quantity of personal data. Those data have been shared, via Europol, with law enforcement authorities across Europe and have enabled the arrest of numerous criminals. However, the integrity of the data obtained cannot be verified by the authorities in executing states because of secrecy restrictions put in place by the French police. This causes a serious concern for the admissibility of evidence in court and, therefore, for a fair trial. Individuals are unable to know what data the indictment is based, nor the accuracy of that data. This makes it difficult, if not impossible, to contest in court, contrary to the principle of access to an effective remedy and equality of arms.

Courts in France and Germany have accepted the use of those evidence on account of the need to tackle serious criminality. The Berlin court of appeal has however asked preliminary questions to the CJEU underlining the importance of fair trial rights, in particular the ability to

challenge evidence. [In Italy a ruling of the supreme court](#) went in that direction by calling on prosecutors and police to disclose how messages were obtained from the Sky ECC network.

Surveillance and criminalisation of the press

Revelations about the use of spyware against journalists continued throughout the year. The Media Freedom Rapid Response that tracks, monitors and reacts to violations of press and media freedom in EU member states and candidate countries included a thematic analysis in their [yearly report](#). In 2022, the use of spyware and state surveillance of journalists was documented in Spain and in Greece. Several journalists reporting on the Catalan independence bid had their phone infected by the Pegasus software and suspect the Spanish authority to be at the origin of the hack.

Another lesser known spyware, Predator, has been detected in Greece on the phone of [a journalist working for international press](#). The investigation revealed that the Greek interior ministry was responsible for the surveillance. [The European Centre for Press and Media Freedom has also highlighted](#) how reporting on migration and refugee issues in Greece has become increasingly difficult, due to obstructions including “arbitrary arrest and detention, restriction of access to migration hotspots, surveillance, and harassment.” This follows [revelations from 2021](#) that multiple journalists covering migration and asylum were wiretapped by the Italian authorities, in total contravention of the freedom of the press.

Transparency of public decision making

Lighthouse Reports revealed in an [investigation last year that the Netherlands continued to use an algorithm known to falsely accuse families of benefit fraud](#). In 2021, a court ruled that the ‘mass profiling’ system (SyRI) was found to be in breach of EU law. One of the discriminatory risk characteristics used to profile people, the double nationality of parents, clearly illustrates how the programme was devised with racist assumptions at its core. After a social and political outcry that led to the resignation of the government, Lighthouse revealed that “the government had silently continued to deploy a slightly adapted SyRI in some of the country’s most vulnerable neighbourhoods.”

In another case concerning the Netherlands, the Public Interest Litigation Project revealed in a damning [report](#) that the Dutch police has recourse to a predictive policing algorithm targeting children from racialised communities. The Top 400 program in Amsterdam profiles and assesses young people to determine who is likely to commit a crime in the future. As a result of the program young adults were constantly monitored and followed by the police. Similar to the algorithmic technology described earlier, the data used were prejudiced on the racialised bias of decades of policing. The system is still in use in Amsterdam despite the scandal that followed the release of the testimonies of mothers in a [celebrated documentary](#).