OSCE Makes Recommendations on Use of New Technologies for Border Management

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

Anna Pingen

On 5 October 2021, the Organization for Security and Co-operation in Europe (OSCE) released a new policy brief on Border Management and Human Rights. The policy brief aims at providing an overview of the what the implications of collecting and sharing information in the context of border management are and how the introduction or continued use of new technologies in the border space may affect human rights. It also provides recommendations to OSCE-participating States on how to respect and protect human rights when using new technologies to manage their borders.

AUTHOR

Anna Pingen
Researcher
Max Planck Institute for the Study of Crime, Security and Law

ISSN: 1862-6947
https://eucrim.eu

The brief calls to mind that, while States have a legitimate interest in controlling their borders and managing who enters their territory, border security must not come at the expense of human rights and fundamental freedoms. It is therefore necessary to put in place a robust legislative framework that both regulates the use of new technologies at borders and provides strong human rights safeguards.

The OSCE points out that the collection and automated processing of Advance Passenger Information (API) and Passenger Name Records (PNR) data by state authorities (via airlines) is a substantial interference with the right to privacy. Therefore, states need to clearly and convincingly demonstrate how the use of this data is limited to what is strictly needed in order to achieve a legitimate aim, such as the prevention, detection, and investigation of terrorist offences or other serious crimes. Furthermore, states need to minimize the amount of data being collected and minimize data retention periods. They should also strictly observe purpose limitations for data processing. The collection and processing of sensitive data like PNR should not be permitted.

As API and PNR data are used to identify terrorist suspects among travellers by means of comparison with relevant watchlists and databases, there can be wrongful identification that can impact freedom of movement. PNR data is also used for a general data analysis of the traveller as well as specific risk assessments of behaviour to detect potential suspicious patterns. This can lead to discriminatory profiling. Therefore, states need to put in place effective human rights safeguards to protect persons from being placed under wrongful suspicion for involvement in terrorism or other crimes, and states must refrain from discriminatory profiling on the basis of PNR data.

Regarding biometric data systems, the OSCE stressed that all systems operating with biometric data should be presumed high-risk technologies. They should undergo thorough and independent human rights impact assessments. States must also put in place clear human rights-based frameworks, which strictly regulate the use of biometric technology.

Especially refugees, asylum-seekers, and children crossing borders are at particular risk of human rights violations arising from the use of biometric data. In these cases, alongside privacy and data protection concerns, there are particular risks of infringements of absolute rights (the risk of refoulement; cruel, inhuman, and degrading treatment; or other infringements on human dignity). For persons in situations of heightened vulnerability, such as migrants and asylum-seekers, states must ensure that the principle of free and informed consent and the right to information are guaranteed whenever collection and processing of biometric data (e.g. fingerprints) takes place. For asylum seekers, the states should follow the well-established principle of not sharing the biometric data of asylum seeker with the country of origin. The OSCE sees a high risk in the use of biometric technology, such as facial recognition, which may reinforce bias and result in discrimination; the organization urges states to reconsider the use of such technology.

Regarding the use of algorithms, the OSCE points out that the technology is not a neutral technical tool that helps screen individuals and inform consequent decision-making in border control, since there is a risk of introducing bias to the algorithm through biased data sets. Therefore, algorithmic systems should undergo obligatory and regular audits in addition to "discrimination testing" by private companies as well as public bodies involved in the development and operation of such systems. Border guards working with such tools should also receive human rights and anti-discrimination training. It is also imperative that algorithmic decision-making tools remain under human control.

In order to avoid overbroad application of terrorism watchlists, the criteria for including individuals on such lists must be clearly defined, based on a narrow and precise definition of terrorist offences. Human rights safeguards must be integrated into all terrorism-related international and transnational co-operation agreements, including in relation to data sharing.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union