AI & HUMAN RIGHTS: LAW & JUDGEMENTS

Presentation during the National AI Roundtable for Fundamental Rights Authorities and Bodies

16th September 2025

INTRODUCTION

Digital technologies create challenges as far as human rights and fundamental freedoms are concerned, as they can be used for wrong (or at least dubious) purposes.

ECHR

In Chapter 319 we find the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms (including Art 8) that Malta ratified and which have been transposed into domestic law. Protocol 12 of the Convention, which Malta has ratified, was not transposed into Chapter 319. This means that the provisions of Protocol 12 are not enforceable before the Maltese Courts. It is only the Strasbourg Court that has jurisdiction to hear and decide on cases that involve Protocol 12.

Art 8

1 Everyone has the right to respect for his private and family life, his home and his correspondence.

2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

THE RATIONALE

The essential object of Art 8 is to protect the person against arbitrary action by public authorities. There may also be positive obligations inherent in ensuring effective "respect" for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of persons between themselves. A fair balance has to be struck between the competing interests of the person and the community.

Case-law can be divided into five categories:

- Freedom from interference with physical integrity.
- Freedom from unwanted access to and collection of information.
- Freedom from serious environmental pollution.
- The right to be free to develop one`s identity.
- The right to live one`s life in the manner one`s choosing.

With regard to AI, one should pay particular attention to the second category.

Art 8 includes protection of the right to personal identity and to personal development. The right to personal identity is closely linked to the right to the protection of personal data. In case of data processing, the right touches upon the right to equal treatment, and the right to protection against discrimination, stereotyping and stigmatisation.

Although the right to protection of personal data is not enshrined as an independent right in the ECHR, judgements consider that in general the right to protection of personal data falls within the framework of Art 8.

Contracting States have an obligation to provide adequate protection against arbitrary behaviour, and define in sufficently clear terms the discretion (or margin of appreciation) granted to the competent authorities and the manner in which such discretion should be used.

Interference by the State must always be dictated by what is necessary in a democratic society. Therefore safeguards must be clearly defined, suitable to prevent abuse, and proportionate to achieve the intended objective. Any State claiming a pioneering role in the development of new technologies has a special responsibility to strike the right balance.

JUDGEMENTS

ECtHR

Fifth Chamber

8 February 2018

Ben Faiza v. France

The Court addressed the issue of AI-driven surveillance in a criminal investigation.

French police had secretly attached a GPS tracking device to the claimant`s to monitor his movements round the clock, and had also obtained his cell phone location data by mean of a court order to the mobile operator company.

The Court held that there was a breach of Art 8 with regard to the real-time GPS geolocation surveillance.

At the time, French law did not provide sufficient clarity or limits on the discretion of the authorities on the use of such a tracking device, making the intrusion into private life unlawful.

In contrast, the one-time retrieval of cell tower data was deemed lawful and necessary for investigating serious crime and therefore no breach was determined.

This judgement highlights the fact that the use of AI-enabled geolocation tools without a clear legal framework breaches privacy right. The continuous GPS monitoring was considered a highly intrusive measure requiring strict safeguards, which were absent in this case.

Grand Chamber

25 May 2021

Big Brother Watch and Others

v. United Kingdom

The Court examined the UK's bulk interception of communications following the Snowden revelations.

The Court found that the regime of mass surveillance of the UK Intelligence, Security and Cyber Agency (GCHQ), which involved automated filtering and analysis of vast amounts of online communications, violated Art 8.

The regime lacked "end-to-end" safeguards and oversight, allowing excessive data collection that was not "necessary in a democratic society."

Moreover, the Court found that the "interception programme" breached freedom of expression (Art 10) because it provided insufficient protection for confidential journalistic material.

The Court did note that bulk interception per se was not inherently unlawful provided robust safeguards are in place.

Grand Chamber

25 May 2021

Centrum för Rättvisa v. Sweden

The case related to Sweden's signals intelligence programme that allowed bulk collection of electronic communications.

The Court found a breach of Art 8 due to insufficient safeguards against abuse in the Swedish legislation.

The Court acknowledged that the legislation did meet some "quality of law" requirements, but identified three defects: (1) there was no clear rule requiring prompt destruction of intercepted data that proved irrelevant ; (2) there was no requirement to consider a person`s privacy before sharing intelligence with foreign partners, and (3) there was a lack of effective ex post facto review by an independent body.

Because of these flaws, the bulk data surveillance system failed to guard against arbitrary interference, and overstepped the State's margin of appreciation with the risk of arbitrary and abusive behaviour.

The use of far-reaching interception technology without robust safeguards violated Art 8.

First Chamber

11 January 2022

Ekimdzhiev and others v. Bulgaria

The Court carried out an examination of Bulgarian legislation on secret electronic surveillance and mobile data retention.

The Court found that the surveillance regime — including covert wiretapping and bulk communication data access — lacked effective safeguards against arbitrariness.

Systemic problems were identified: wide criteria for authorizing surveillance; inadequate oversight mechanisms, and insufficient rules on data storage, use, and destruction.

The Court considered that these deficiencies were evidence that the use of the special surveillance measures did not meet the "minimum safeguards" required by Art 8. In particular, the abusive potential of automated data-gathering tools (like indiscriminate SMS/telecom metadata collection) was not legally regulated and therefore posed an unacceptable risk to privacy.

First Chamber

4 July 2023

Glukhin v. Russia

This was the first Strasbourg Court ruling on facial recognition technology (FRT) used fo law enforcement purposes.

The claimant had staged a peaceful one-man protest in the Moscow metro. The Police used FRT on CCTV footage and live cameras to identify, track, and arrest him for failing to notify authorities of the demonstration.

The Court held that the use of AI-driven facial recognition breached Art 8 (supra) and Art 10 (the right to freedom of expression).

The Court considered that processing a person`s biometric data in the context of a peaceful protest was particularly intrusive and that the deployment of facial recognition against a person who was in lawful exercise of his rights was incompatible with the ideals and values of a democratic society governed by the rule of law.

The judgement laid emphasis on the need for detailed rules and strong safeguards when employing FRT, especially live real-time use, to prevent abuse or arbitrary targeting. The State`s failure to ensure such safeguards was in breach of the Convention. List of any judgements given by the Court of Justice of the European Union on AI vis-a-vis the Charter of Fundamental Rights

RAISON D`ETRE

Although the existence of intelligence services with powers of secret surveillance are tolerated under the Convention, the practice of such services must prove necessary to safeguard democratic institutions. Any interference must be proportionate to the aims pursued, and supported by relevant and sufficient reasons. Indiscriminate collection of information by State officials about persons without their consent does interfere with their private life.

THE CHARTER

The provisions of the Charter of Fundamental Rights and Freedoms of the European Union became part of Maltese Law by virtue of Malta`s ratification of the Lisbon Treaty of the EU.

Art 7

Everyone has the right to respect for his or her private and family life, home and communications.

Art 8

1 Everyone has the right to the protection of personal data concerning him or her.

2 Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

Art 47

The right to a fair trial

CJEU

Grand Chamber

21 June 2022

Ligue des droits humains

(PNR Passenger Data Case)

The matter related to the use of AI type techniques under the Passenger Name Record Directive.

The Court ruled that because AI methods often rely on opaque statistical inference processes, they can obstruct persons` rights to understand decisions and obtain effective judicial remedies as required by Art 47 of the Charter.

PRELIMINARY REFERENCES

PENDING

Art 47

Yettel Bulgaria EAD

25 Nov 2024

Bulgarian Court wanted to know how the AI Act (Reg. 2024/1689) and consumer law interact with automated billing decisions.

No ruling yet

RULING

Fourth Chamber

13 January 2025

Random case-allocation system in judicial proceedings in Poland.

In particular, whether opaque ICT/algorithmic allocation undermines a “tribunal established by law” and fair trial.

The ruling was in the sense that EU law precludes national provisions that categorically prevent appellate courts from reviewing irregular reallocation of a case, particularly when such reallocation breaches national rules governing random allocation of cases within courts and the appellate review is expressly forbidden.

When a case is reallocated improperly and runs counter to national procedural law, the national courts must be able to review that irregularity.

A blanket rule that bars appellate courts from reviewing procedural irregularities violates the principles of judicial independence and effective judicial protection under EU law.

FOREIGN DOMESTIC

THE NETHERLANDS

5 February 2020

DISTRICT COURT - THE HAGUE

C/09/550982/HA ZA 18/388

The Dutch Government devised a statutory Risk Indication System (SyRI) to prevent and combat fraud primarily (but not only) in social security. The system was designed to allow data to be linked and analysed anonymously in a secure environment so that risk reports could be generated. The legislation sustaining SyRI was contested.

The case focused not just on data processing operations in the deployment of the SyRI and its technical safeguards, but also on other issues including: the mutual exchange of personal data by administrative bodies and the provision of personal data to Government.

The State argued that new technologies, including digital interventions linking files and data analysis using algorithms could offer more possibilities to the public authorities to exchange data to combat fraud.

The Court ruled that SyRI violated Art 8 of the Convention. The risk model, the indicators and the data that were actually processed were neither public nor known to those involved, and had a significant effect on the private life of the persons to whom the report referred.

The Court considered the lawfulness of the interference within the context of the right to privacy, and found that SyRI legislation did not satisfy the condition of “necessary in a democratic society”. The risk reports had significant consequences on persons` lives in the sense that they indicate that a specific person is worthy of investigation related to fraud.

SyRI legislation did not cater for an information obligation on the data subjects whose data were processed to enable them to know that their data was the object of processing. Nor did the legislation provide for an obligation to inform data subjects, individually where appropriate, of the fact that a risk notification has been made.

Although the Court accepted the principle that new technologies could be used to prevent and combat fraud and that in principle SyRI legislation had a legitimate purpose, the the development of new technologies had also to take into account the right to the protection of personal data.

Legislation had to provide a framework sufficient to protect the right to privacy, which includes the protection of personal data, in order to enable all interests at stake to be considered in a transparent and verifiable manner.

Legislation has also to allow any person to have a reasonable expectation that his/her private life would be respected in terms of Art 8 of the Convention, meaning that in the application of new technologies, the State has a particular responsibility to strike the right balance between, on the one hand, the benefits associated with the use of technologies to prevent and combat fraud and, on the other hand, the interference that this may cause in the exercise of the right to respect for private life.

The Court found that the SyRI legislation did not meet that requirement and decided against the Government.

CONCLUSION

Because AI refers to the simulation of human intelligence processes, it is essential to approach the development and deployment of AI technologies with a human rights perspective.

Innovation is good provided no compromises are accepted to the detriment of human rights. A strongly human rights compliant and respectful AI has to reach out in order to achieve a reasonable balance that puts aside risks to the well being of persons.

To protect better human rights standards in practice, we require good law. AI is no exception to the rule of law. AI cannot be used to favour discriminatory practices. Nor can it become capable of making decisions that negatively affect the lives of people.