30 SEPTEMBER 2025
EUROPEAN ROUND TABLE CONFERENCE
THE MALTA CHAMBER - VALLETTA

ARTIFICIAL INTELLIGENCE: SUBJECT TO HUMAN RIGHTS PRINCIPLES

INTRODUCTION

While AI offers significant potential benefits, it also raises ethical and other concerns: including issues of privacy, confidentiality and bias.

Responsible development and deployment of AI is essential.

Developments in AI should be kept under watch to ensure compliance with the fundamental rights of the person.

Digital technologies create challenges as they can be used for wrong (or at least dubious) purposes.

ECHR - 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.

RATIONALE

The provisions of the Convention are part of the laws of Malta (Chapter 319).

Art 8 is there to protect the person against arbitrary action by public authorities.
There are also be positive obligations, being the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves.

A fair balance has to be struck between the competing interests of the person and of the State.

The case-law of the Strasbourg Court 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.

As declared by the ECtHR, 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.

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

National law must 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.

The Strasbourg Court has said that 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.
States have the responsibility to strike the right balance.

JUDGEMENTS

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 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 rights. 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

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.

CHARTER

We find provisions of similar content and quality in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union:

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.

The provisions of the Charter are part of Maltese Law by virtue of the Lisbon Treaty.

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.

DOMESTIC

JUDGEMENT

THE HAGUE DISTRICT COURT

05/02/2020

REF. C/09/550982/HA ZA 18/388

FACTS

A Risk Indication System (SyRI) was devised by the Dutch Government as a statutory instrument to prevent and combat fraud in social security and income-related schemes, tax and social security contributions and labour laws.

The technical infrastructure allowed that data be linked and analysed anonymously in a secure environment so that risk reports could be generated.

The legitimacy of the legislation sustaining SyRI was contested.

The system was devised to carry out different processing operations on personal data, collected large-scale data and generated risk notification about people likely to commit fraud : the "risk report".

The State argued that linking files and data analysis using algorithms could offer more possibilities to the public authorities to exchange data to combat fraud.

On the basis of this risk report, a legal or natural person was considered to be worth investigating in relation to possible fraud. With the deployment of SyRI, files at the disposal of government agencies are linked in a structured manner in order to be able to identify related abuses in specific areas.

In the case in point, a number of addresses in a particular district in a municipality were investigated.

THE JUDGEMENT

The Court ruled that SyRI violated Art 8 of the ECHR.

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 established that a specific person should be investigated for fraud.

What was questionable : the mutual exchange of personal data by administrative bodies, the provision of personal data to the Minister, and profiling.

The Court considered that the provisions of Convention have to interpreted in the light of the general principles of the Charter and the GDPR as these in some respects give further protection.

The Court considered that 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 person to whom the report was referring.

The data which was made subject to processing in SyRI were :

- data with which a work performed by a person can be determined.
- data showing that an administrative fine was imposed on a natural or legal person, or that another administrative measure had been taken.
- information enabling the identification of tax obligations of the person concerned.
- information intended to identify the ownership and use of movable and immovable property.
- information concerning grounds for exclusion from assistance or benefits.
- data making it possible to determine the (actual) place of residence or place of business of a natural or legal person.
- identification data: In the case of a natural person: name, address, postal address, date of birth, sex and administrative characteristics;
- In the case of a legal person: name, address, postal address, legal form, location and administrative characteristics.
- integration data: data which make it possible to determine whether a person is subject to integration obligations.
- compliance data: data that make it possible to record the compliance history of a natural or legal person with regard to legislation and regulations.
- education data: data with which the financial support for the funding of education can be determined.
- pension data: data regarding pension entitlements to be determined.

- reintegration data: data with which it can be determined whether reintegration obligations have been imposed on a person and whether these obligations are complied with.

- indebtedness data: data making it possible to determine the debts, if any, of a natural or legal person.

- benefits, allowances and grants data: data making it possible to establish the financial support of a natural or legal person.

- permits and exemptions, which are data making it possible to identify the activities for which a natural or legal person has requested or obtained consent.

- health insurance data, i.e. only the data with which it can be determined whether a person is insured under the Health Insurance Act.

THE ROLE OF THE MINISTER

The Minister determined whether a request for deployment of SyRI satisfied the conditions at law.

If a natural person or legal entity with an increased risk is not the subject of a risk report, his or her data will be destroyed within four weeks of completion of the analysis.

The Minister will destroy any remaining data not later than two years after the start of the SyRI project. The destruction will be recorded in an official report. The destruction order does not extend to the data in the risk notifications register. A retention period of two years after the registration of the risk report applies

THE PRIMARY CONSIDERATION

The District Court accepted the principle that new technologies can be used to prevent and combat fraud. There was also acceptance in principle that SyRI legislation is in the interest of economic welfare and therefore serves a legitimate purpose.

However, the State has 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.

Legislation must provide a sufficiently effective framework for the protection of the right to privacy, which includes the right to the protection of personal data, to enable all interests at stake to be considered in a transparent and verifiable manner.

Legislation should also allow any person to have a reasonable expectation that his or her private life will be sufficiently respected in the deployment of SyRI.

The Court found that the SyRI legislation did not meet that requirement.

OTHER CONSIDERATIONS

Transparency requires that information should be accessible and comprehensible.

SyRI legislation did not cater for an information obligation on data subjects whose data were processed in order that those persons could reasonably be expected to know that their data was the object of processing.

Nor did the legislation in question provide for an obligation to inform data subjects individually, where appropriate, of the fact that a risk notification has been made.

There was objective difficulty for a person to defend himself against a risk report that concerns him/her.

Likewise, it is difficult to see how a data subject whose data have been processed in SyRI, but who did not result in a risk report, can be aware that his or her data have been processed on correct grounds.

The fact that data did not lead to a risk notification does not detract from the required transparency with regard to that processing. The right to respect for private life also implies that a data subject must be given a reasonable opportunity to follow his or her data.

The judgement is res judicata because the Government did not appeal.

DOMESTIC FALLOUT

The judgement effectively dismantled SyRI.

Although the law remained on the statute book, in practice it was a dead letter.

The political consequences were significant.

Despite declared intentions by the Dutch Government to improve algorithmic transparency and oversight, and despite that plans were announced for a national algorithm register where public institutions had to list and describe their automated decision systems together human-rights impact assessments, the situation did not improve substantially until the Childcare Benefits scandal came to the fore and to public attention.

The political consequences were remarkable.

Many innocent families were targeted more often than not through the adoption of discriminatory criteria. Parents were unfairly labelled and forced to repay large sums. Many were financially ruined.

The outrage was serious because governance culture had shifted towards suspicion and surveillance of welfare recipients, with insufficient regard for rights.

Following a parliamentary inquiry, the Dutch Government (Rutte III) resigned in January 2021 after taking collective responsibility. A €500m fund was set up to compensate the families.

INTERNATIONAL RESPONSE

The sensitive and delicate questions raised in the Netherlands sent shockwaves across the Continent.

THE COUNCIL OF EUROPE

The CoE considered the SyRI outcome as a validation of the Convention's role in the digital age: Art 8 being the defence against unfettered state algorithms.

The CoE did not stop there.

The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, was adopted in 2024.

The Convention aims to ensure that activities within the lifecycle of artificial intelligence systems, although conducive to technological progress and innovation, are fully consistent with human rights, democracy and the rule of law.

The Convention opened for signature on the 5 September 2024 even for countries outside the European Continent.

So far the list of signatories has been very encouraging.

The fundamental principles of the Convention include the protection of human dignity, individual autonomy, equality, non-discrimination, privacy, personal data, transparency and oversight, accountability, safe innovation and reliability.

Simply for the purpose of submitting a complete picture, I have to point out that positions have beens put forward in the "The Washington Post" this year to underline the view that AI's fast-moving nature often outpaces regulatory efforts including the CoE Framework Convention. The opinion expressed is that the high-level provisions do not address cutting-edge "frontier" AI capabilities directly, and full implementation will be slow. Experts warn that AI treaties could become outdated almost as soon as they are drafted simply because AI innovation is sprinting ahead of the deliberate consensus-driven pace of global lawmaking.

THE EUROPEAN UNION

As part of its digital strategy, the EU embarked on regulating the development and use of AI. In April 2021, the European Commission proposed the first EU AI law that established a risk-based classification system.

In June 2024 the Artificial Intelligence Act was adopted. After its entry into force, the Act established deadlines : 6 months for "Prohibited AI Systems" ; 24 months and 36 months for "High Risk AI systems" as defined respectively in Annex III and Annex I of the Act ; and and 12 months for "General Purpose". The Act will be fully in force in 2026.

I must point out that MDIA, MCA and DPC each in its jurisdiction and competence are doing their fair share.

The Ombudsman is there as well to oversee their administrative operations.

THE PATH AHEAD

International legal instruments alone are not enough. There is a need for strong investment in awareness strategies and education projects that assist the public in learning not only about the operations of AI, but also its impact on everyday life, stressing on the importance of providing transparent and comprehensible information that is accessible not just to experts but also to the public in general. In addition people should reasonably be advised how their data are being processed.

Because AI refers to the simulation of human intelligence processes by computer systems, it is essential to approach the development and deployment of AI technologies with a human rights perspective. Reaching a reasonable balance requires collaboration between governments, technology developers, civil society organizations, and other stakeholders.

One should strive strongly in favour of a human rights compliant and respectful AI that supports human development. There is nothing inherently wrong with the tech world owning technology, but there is something inherently worrying when developments negatively impact opn the lives of people.

What solutions can we suggest so that the technology is in the service of human well-being ?

1 the invocation of the language of ethics

and

2 the language of human rights

Ethics is an inherently subjective issue. But using ethics to tame of technology could be a way forward.

Human rights must be put at the centre not to displace ethics but to promote further protection. To protect better human rights standards in practice, we require good law both as far as principles are concerned and in the way that law is written in order to avoid loopholes.

The need for innovation is good provided no compromises are accepted to the detriment of human rights. A strong human rights compliant and respectful is a must for the future.

We have to start thinking, speaking and promoting for everyday use algorithmic accountability and transparency. Thank you.