Consultation EU White paper on Artificial Intelligence

1. Introduction

On 19th February 2020, the European Commission published its White paper on Artificial Intelligence (AI). This White paper follows the European strategy for artificial intelligence presented in April 2018.

The White paper supports the use of artificial intelligence in Europe's (data) economy. Its approach is mainly economic and commercial. This is in line with the European Data Strategy.[1] That Strategy aims at creating:

> *"a single market for data, where data can flow freely within the EU and across sectors, for the benefit for all, where European rules, in particular privacy and data protection, as well as competition law are fully respected, and where the rules for access and use of data are fair, practical and clear."*

The White paper sets out the proposed key elements of a future legal framework regulating artificial intelligence. The legislative proposals shall be presented at the end of 2020 or in early 2021. Simultaneously with the publication of the White paper, the European Union invited the public to submit its comments on the White paper and on the suggestions made therein.

The Dutch section of the International Commission of Jurists (NJCM) hereby respectfully submits its comments and welcomes the initiative of the European Commission to publish a White paper on Artificial Intelligence and invite the public to comment on it.

2. NJCM

The NJCM, an association of jurists, was established in 1974 and forms the Dutch section of the International Commission of Jurists (ICJ). Since then it has become an influential organization for the protection of human rights in the Netherlands and in Dutch foreign policy. The NJCM has approximately 1,300 members. About 10 to 15 % of its members are actively involved within the organization on a voluntary basis, mostly through the working groups of the NJCM. These working groups monitor legal, social and political developments related to human rights, comment on legislative proposals to Parliament or to European institutions and report to international human rights organizations. The NJCM organises public events to enhance knowledge on human rights, especially under professionals but also the broader public. Since 2014, the NJCM has also conducted strategic litigation in human rights cases. In 2016 it started a clearinghouse to match NGOs with legal needs with pro bono lawyers.

[1] COM(2020) 66.

3. General comments on the approach taken

As stated in the introduction, the European Commission clearly takes an economic and commercial approach to the use of data and artificial intelligence. This approach is fueled by the estimation that the value of the "data economy" will be 5.8% of the EU's GDP in 2025 and that we will see a five fold growth of the global data volume between 2018 and 2025 (European Data Strategy). Against this backdrop, the White paper sets out the goal that Europe should "become a global leader in innovation in the data economy and its applications".

However, the use of artificial intelligence can seriously affect fundamental rights. A significant part of the data volume will concern personal data and certain AI based systems will have a profound effect on the private lives of citizens. On the one hand, the White paper, claims that it duly recognizes "the major impact that AI can have on our society and that, hence, a need exists to 'build trust' and that it is vital that European AI is grounded in our values and fundamental rights such as human dignity and privacy protection". On the other hand, the White paper does not link the suggested framework to existing mechanisms to mitigate the impact, such as human rights impact assessments.

Moreover, the White paper incorporates the maxim that there must be a 'free flow of data', and that 'improving access to and management of data is fundamental' (White paper p.8 section G). The use of artificial intelligence technology in the (digital) services we use in our everyday lives, may be beneficial, but can also be very harmful for citizens.

If at least part of the aim of the White paper is to generate legal norms that regulate government decisions, medical decisions, decisions about work or about the private lives of European citizens by, through or with the aid of AI systems, then this concerns of one of the most profound changes in the social contract between (governments) decision makers and citizens since the industrial revolution. It deserves our serious and very careful attention.

Involving all stakeholders

Artificial intelligence may affect all areas of social life, also those that are not subject to EU regulation. Moreover, the use of artificial intelligence can affect a large number of fundamental rights that are enshrined in national constitutions across Europe. In this respect, we would suggest a more careful approach to the use and regulation of artificial intelligence, and we encourage a broad dialogue to be undertaken on this topic. This dialogue should involve specialists of many different areas, including specialists on national constitutional orders of Member States, as well as human rights specialists. Moreover, the dialogue should involve democratically chosen representatives, such as the members of national parliaments. In this vein, we would welcome a significant expansion of the High-Level Expert Group wherein a dialogue were to be initiated with representatives of national parliaments.

Ethics and fundamental rights

The White paper seems to integrate an ethical approach to AI systems, as set out in the Ethics Guidelines for Trustworthy AI issued by the High-Level Expert Group. In these guidelines, fundamental rights have been used to come to the ethical principles. This is a positive step as this now provides an ethical and dogmatic framework. The White paper, however, aims at providing a concrete blueprint for a future legal framework. In this context, the White paper recognises that a number of human rights may be affected by AI systems. We welcome the position of the European Commission to protect the EU values and fundamental rights. Yet, in this step towards the adoption of legislative proposals, fundamental rights do provide more concrete and legally binding rules than ethical principles do. The Guidelines of the High-Level Expert Group are non-binding and a legal framework should comply with fundamental rights, that could be contested for a judge and be better explained. We notice that, as of yet, no human rights impact assessment has been carried out of the policy options that are envisaged. Since AI systems have the potential to severely impact fundamental rights, an extensive human rights impact assessment should be carried out in line with the Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union[2] and in line with international standards, such as the United Nations Guiding Principles on Business and Human Rights (UNGPs)[3]

4. The proposed legal framework

Against the backdrop of possible safety risks and risks relating to fundamental rights, as well as the desire to provide every AI developer with a clear cut and easily understandable regulatory framework, the White paper proposes to introduce a two pronged system of regulation. On the one hand, there should be a clearly defined ”high-risk” category and on the other hand a non-high risk category. AI systems that fall into the high-risk category need to conform to a number of standards. Non-high risk AI does not.

[2] Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union, COM(2010) 573, see also the Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments SEC(2011) 567. The European Court of Justice requires EU institutions to carefully consider the human rights impact of policy options and to choose the most proportionate option, e.g. ECJ, Joined Cases C-92/09 and C-93/09 of 9 November 2010 (Schecke and Eifert).

[3] UN Office of the High Commissioner for Human Rights “Guiding Principles on Business and Human Rights: Implementing the ‘Protect, Respect and Remedy’ Framework” (“UNGPs”), HR/PUB/11/04, 2011. See also the Commission Staff Working Document on Implementing the UN Guiding Principles on Business and Human Rights, SWD(2015) 144 final and the European Commission Sector Guides on Implementing the UN Guiding Principles on Business and Human Rights.

An AI system will fall into the category of high-risk, where it - cumulatively:

1) is used in a high-risk sector. Such high-risk sectors must still be defined. The White paper mentions that the list of high-risk sectors should be exhaustive and it provides as examples the healthcare, transport, energy sectors and parts of the public sector.

2) Is deemed a high-risk application within that sector. The White paper specifies that not all applications within a given high risk sector will pose a high-risk and suggests to assess the impact of a given application. The assessment could be based on the legal effects that are created by the application, a negative impact on rights of individuals or companies, risks of death or injury, severe material or immaterial damage, or on the fact that an application creates risks that subsequently cannot be avoided.

As a third category the White paper mentions AI applications that must be deemed high-risk as such. Examples that are given are AI applications that may affect employment equality and consumer rights - which is due to the EU acquis on these matters. Another category is remote biometric identification and other intrusive surveillance technologies.

In order to minimise the possible negative impact of high-risk AI applications, the White paper suggests that mandatory legal requirements are introduced for high-risk AI applications and that a prior conformity assessment should be carried out. The mandatory legal requirements consist of the following elements:

training data, e.g. sufficiently broad, representative and non-discriminatory data-sets, privacy protection;
data and record-keeping;
information to be provided to the public, e.g. information on the capacity and limitation of a given system, information for citizens if they are interacting with an AI application;
robustness and accuracy, e.g. reproducible outcomes, measures to deal with errors, adequate security measures and mitigating measures in place in case of security breaches;
human oversight, e.g. where social security is concerned, a decision should ultimately be carried out by a human agent; monitoring by a human agent during operation or designing systems

The White paper further mentions specific measures for remote biometric identification. It states as follows:

> *"It follows that, in accordance with the current EU data protection rules and the Charter of Fundamental Rights, AI can only be used for remote biometric identification purposes where such use is duly justified, proportionate and subject to adequate safeguards. In order to address possible societal concerns relating to the use of AI for such purposes in public places, and to avoid fragmentation in the internal market, the Commission will*

launch a broad European debate on the specific circumstances, if any, which might justify such use, and on common Safeguards."

5. The proposed framework and the protection of fundamental rights

The proposed legal framework foresees impact assessments and a specific focus on the protection of fundamental rights in cases of high risk applications in high risk sectors, as well as for applications in a small number of specific areas. We wonder whether this approach is in line with the existing body of privacy law and human rights law.

Facial Recognition

Before we comment on the proposed framework, we would like to point out the lack of urgency regarding the use of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places.
The White Paper recognises that this use carries specific risks for fundamental rights. We're glad the EU report acknowledges that facial recognition, when deployed in public spaces, poses a threat to fundamental rights and to the GDPR. But it stops short of prescribing any hard limits, instead recommending 'broad European debate' on the topic. We note that new criteria around facial recognition are much weaker than the five-year ban on using such technology in public places, as was included in an amended version of the White Paper.
The White Paper mentioned that:

"In order to address possible societal concerns relating to the use of AI for such purposes in public places, and to avoid fragmentation in the internal market, the Commission will launch a broad European debate on the specific circumstances, if any, which might justify such use, and on common safeguards."

We believe a dialogue, as proposed, falls short in relation to the urgency of banning facial recognition. We therefore emphasise that it is urgent for the EC to take leadership on drawing red lines around facial recognition, particularly contending with the issue of concentrated power and the harms this technology presents to civil society.'

Firstly, we notice that the proposed framework does not seem to reflect the existing body of law concerning privacy, such as the GDPR, entirely. A recent analysis of the European Data Protection Board confirmed that the use of personal data as training data or the processing of personal data, through AI applications, falls within the ambit of the GDPR.[4] Consequently, the principle of transparency mandates that data subjects are informed in a meaningful manner, if and when their personal data is processed or used. The White paper indicates that additional

[4] Letter dated 29 January 2020 of the European Data Protection Board to Sophie in 't Veld, Member of the European Parliament (OUT2020-0004),

requirements may be called for to achieve the objectives pursued and therefore adequate information, about the use of high-risk AI systems, must be provided in a proactive manner. No such information needs to be provided in situations, where it is immediately obvious to citizens that they are interacting with AI systems. In our opinion and in accordance with the GDPR, information must always be provided, not only in cases of high risk categories.

The GDPR requires that a Data Protection Impact Assessment (DPIA) is carried out, when the processing of data is likely to result in a high risk. The Dutch Data Protection Authority has taken a similar stance, adding that a DPIA must also assess whether the means used are proportionate and necessary to achieve the purposes.[5] In line with the GDPR, the proposed framework solely mentions mandatory requirements for high risk applications in high risk sectors. In this context, we want to emphasize the need for a more fine tuned approach of the future regulatory framework, that contains mandatory human rights impact assessments and that does not exempt entire sectors from mandatory requirements by placing them in a low risk category.

Secondly, we want to point out that in addition to the right to privacy protection and the GDPR, the framework will need to ensure the respect for a variety of other human rights that may be (severely) affected by AI applications. In this respect, we would like to highlight a relevant recent case in The Netherlands (SyRI). In this case The Dutch Court judged an AI application used by the Dutch government to combat fraud. The Court concluded that this application is in violation with article 8 ECHR, the right to respect for private and family life. But first we want to explain the right to respect for private life and the protection of personal data and after the SyRI case, we will discuss the other rights.

5.1 Right to respect for private and family life & protection of personal data

- **Article 8 ECHR: Right to respect for private and family life**

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.

- **Article 7 EU Charter: Respect for private and family life**

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

- **Article 8 EU Charter: Protection of personal data**

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

[5] The Dutch Data Protection Authority, Toezicht op AI & algoritmes, p. 6, 7.

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.

Many AI applications collect and analyze the personal data of individuals. This interferes with the rights to private life and the right to data protection.[6] As already mentioned above, the GDPR provides clear guidance for the requirements regarding the processing of personal data. In addition, the case law of the European Court of Human Rights (ECtHR) is of key relevance. The ECtHR does not only recognize the negative obligation of article 8 ECHR, but also defines a positive obligation for states to protect the right to private life effectively even in the sphere of private relations of individuals amongst each other.[7] As such, the jurisprudence is of relevance to the legal framework that is proposed in the White paper.

In its jurisprudence, the ECtHR has set standards that have to be met in order for an interference by an AI application to be justified. The interference must be based on (domestic) law and it has to be compatible with the rule of law, which is explicitly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8 ECHR.[8] The relevant law must be accessible to the person concerned and foreseeable as to its effects.[9]

In the case that an AI application is used by law enforcement as surveillance measure the Court sets a higher standard to the foreseeability: Foreseeability in the special context of secret measures of surveillance, such as the interception of communications, does not mean that an individual should be able to foresee, when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. According to the ECtHR domestic law must thus be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures.[10]

Furthermore, the ECtHR requires that the measures taken strike a fair balance between the aim of interference and the right to private life.They must be proportionate and conform to the principle of subsidiarity. An important element in the fair balance is that adequate and effective guarantees against abuse of power are in place.[11] It is important that if the data is used by state

[6] ECHR 27 June 2017, ECLI:CE:ECHR:2017:0627JUD000093113 (*Satakunnan MarkkinapÖrssi oy and Satamedia oy/Finland),* p. 134, 'The Court reiterates that the storing of information, relating to an individual's private life in a secret register, and such information, come within the scope of Article 8 § 1.The fact that information is already in the public domain will not necessarily remove the protection of Article 8 of the Convention.'
[7] ECHR 10 May 2011, ECLI:CE:ECHR:2011:0510JUD004800908 (*Mosley/ The United Kingdom),* para. 106.
[8] ECHR 4 December 2015, ECLI:CE:ECHR:2015:1204JUD004714306 (*Roman Zakharov/Russia*), para. 228.
[9] *Ibid.*, para. 229.
[10] *Ibid*. Note that this is reflected in the principle of transparency under the GDPR
[11] *Ibid.*, para. 231.

authorities for mass surveillance, that an independent and impartial body, like a judge, is able to control when surveillance starts, how it is carried out and how it ends.[12] The ECtHR stresses that it is also very important for an individual to have an effective remedy.[13] A consequence of this right for an effective remedy is that decisions taken or assisted by AI applications must be explainable and that the mechanisms upon which the decisions are based are transparent. As AI applications are likely to have a great impact on the life of an individual, it is of utmost importance that individuals can effectively challenge decisions taken by or assisted by AI applications.

In the White Paper the European Commission recognises that AI applications can affect the right of privacy. We want to set out that the use of AI applications by state authorities for surveillance have to meet stricter requirements than in other cases. In the White Paper this is not described.

5.1.1 The Dutch SyRI decision

In this paragraph we will elaborate on a Dutch court case in which the application of an AI system, used by the government, violated the rights of citizens. This was one of the first European court cases about an AI application used by a government.[14] The case concerned an AI application used by the Dutch government to prevent and combat fraud in the area of social security (and income-dependent schemes, taxes and social security, and labour laws). The system was called SyRI (Dutch: Systeem Risico Indicatie) and was able to link a large number of government data-sets and analyse them anonymously in a secure environment, so that risk reports could be generated. The government did not provide any information as to which data sets had been combined and as to the functioning of the algorithm. Also, the system could be used for multiple purposes, but no impact assessment was carried out before the system was used for a specific purpose.

In one occasion, the system was specifically used to target and analyse the data of all residents in low income areas, such as certain districts of Rotterdam. Data of the citizens of this area were analyzed by the algorithm to find discrepancies. If the data met the risk profile, these citizens popped out of the system. The NJCM, together with a number of other claimants, started legal proceedings against this use of the system and the law that the system was based upon. In this judgment of 5 February 2020 the District Court of the Hague stated:

> "*that the Netherlands as a party to the ECHR has a special responsibility when applying new technologies to strike the right balance between the benefits the use of such technologies brings as regards preventing and combating fraud on the one hand, and the potential interference with the exercise of the right to respect for private life through*

[12] *Ibid.*, para. 233.
[13] *Ibid.*, para. 234.
[14] District Court The Hague, 5 February 2020, ECLI:NL:RBDHA:2020:1878 (SyRI), para. 6.95.

> *such use on the other hand. From the viewpoint of protection of the right to respect for private life, which includes the protection of personal data, legislation must offer a sufficiently effective framework which allows the weighing of all interests in question in a transparent and verifiable manner."* [15]

The Court thus confirms that every state authority has a special responsibility to safeguard the right to respect of private life, when it is regulating new technologies. From this ruling, we could derive a special responsibility for the European Commission to safeguard the right to respect of private life. Moreover, a legal framework must strike a fair balance between the use of technologies that invade private life and the right to private life, as set out in art. 8 ECHR and it must entail a mechanism to balance the interests of all parties concerned.

The Court ruled that SyRI was serving a legitimate purpose (preventing the misuse of public funds). But the system and legislation, it was based upon, lacked a fair balance and SyRI violated the right to private life. Specifically the Court was of the opinion:

> *"that the SyRI legislation contains insufficient safeguards to protect the right to respect for private life in relation to the risk indicators and the risk model which can be used in a concrete SyRI project. Without insight into the risk indicators and the risk model, or at least without further legal safeguards to compensate for this lack of insight, the SyRI legislation provides insufficient points of reference for the conclusion that by using SyRI the interference with the right to respect for private life is always proportionate and therefore necessary."*

This confirms that transparency is a key requirement for an application in order not to fall foul of article 8 ECHR. In fact, the Court also applied the GDPR principles of transparency and purpose limitation and found that SyRI did not obey these principles. This provided an additional reason for the court to find that SyRI violated article 8 ECHR.

Finally, the Court confirmed that SyRI created potential discriminatory effects. It held:

> "*SyRI has only been applied to so-labelled 'problem districts', as confirmed by the State at the hearing. This in and of itself need not imply that such use is disproportionate or otherwise contrary to Article 8 paragraph 2 ECHR in all cases. However, given the large amounts of data that qualify for processing in SyRI, including special personal data, and the circumstance that risk profiles are used, there is in fact a risk that SyRI inadvertently creates links based on bias, such as a lower socio-economic status or an immigration background."*[16]

The use of SyRI in the so called 'problem districts' thus entailed a serious risk of discrimination.

---

[15] *Ibid.*, para. 6.6.
[16] *Ibid.*, para. 6.93.

5.2 Non-discrimination

- **Article 14 ECHR: Prohibition of discrimination**

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

- **Article 21 EU Charter: Non-discrimination**

1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

2. Within the scope of application of the Treaty establishing the European Community and of the Treaty on European Union, and without prejudice to the special provisions of those Treaties, any discrimination on grounds of nationality shall be prohibited.

As stated in the White paper, every social and economic activity has an inherent risk of bias and discrimination. This holds true for AI applications, as they can be based upon (training) data, that contains stereotypes or prejudices. Such algorithms may then produce a myriad of decisions that are based upon these stereotypes and prejudices which can lead to (serious) discrimination.[17] Thus, as stated in the White paper, bias in AI can have a much larger effect without the social control that normally occurs. Due to the opaque nature of many algorithms, it is difficult to discover if an algorithm is discriminatory, because of the lack of transparency of the used data.

Also in the case that the (training) data does not contain stereotypes and prejudices, algorithms can be discriminatory. The use of the algorithm can affect a specific group of people. Like in the Dutch case mentioned above. The algorithm is used to combat fraud of social insurances. This will affect for a great deal people with a low income that are dependent on social insurances. And it has only been applied to so-labelled ‘problem districts’.This can lead to bias and a serious risk of discrimination.

We welcome that the White paper explicitly recognizes the potential of AI applications to produce discriminatory effects. However, we want to point out that the lack of a human rights impact assessment and the sectoral approach that is taken in the proposed framework (low risk and high risk sectors) might not adequately take account of the discriminatory risk of AI applications in a range of different low risk sectors.

[17] M.J. Vetzo, J.H. Gerards en R. Nehmelman, *Algoritmes en grondrechten*, Boom Juridisch, Den Haag 2018, page 139,140.

5.4 Freedom of expression

- **Article 11 EU Charter, Freedom of expression and information**

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected.

AI applications are used by online intermediaries to prioritise information for their users and to perform content moderation, as is described in the White paper. Content moderation by online intermediaries is often done so that the online content meets the terms of service or in order to filter copyright violations. Content moderation and filtering, however entails the risk that false positives lead to the removal of perfectly legal content. In that sense algorithms are inaccurate.[18] Moreover, it is difficult to set clear standards for the definition of for example hate speech, fake news or terrorist content.[19] In order to be on the safe side, intermediaries may tend to filter and thus block more content than is necessary. Another problem will arise with the prioritising and filtering of the information that is available online. By using AI applications, it is possible that information is willingly or unwillingly left out of searches or feeds or that other information is prioritised in a manner that creates a bias in viewers/users.[20] This can mean that information from e.g. minorities does not reach the greater public. This will have an impact on the right of expression and information of these groups. The articles they post will be read less, because they are left out of searches or because their article pops out as the fifth or sixth choice.

We recognize that a fine balance has to be struck between the regulation of the use of AI in online media - which may be an intrusion into freedom of expression of media providers - and the regulation of AI in social media due to the positive obligation deriving from freedom of expression to protect the equal access of media to everyone (not being blocked by filtering) or to protect democratic processes (combatting filter bubbles and fake news).

5.5. Rights to a fair trial

- **Article 47 EU Charter, Right to an effective remedy and to a fair trial**

Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

[18] M.J. Vetzo, J.H. Gerards en R. Nehmelman, *Algoritmes en grondrechten*, Boom Juridisch, Den Haag 2018, page 157.
[19] Acces now, *Human rights in the age of Artificial intelligence*, page 22.
[20] M.J. Vetzo, J.H. Gerards en R. Nehmelman, *Algoritmes en grondrechten*, Boom Juridisch, Den Haag 2018, page 155-156.

Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.

Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

The growing use of AI applications may also affect our justice system. In that context the White paper says:

" *Certain AI algorithms, when exploited for predicting criminal recidivism, can display gender and racial bias, demonstrating different recidivism prediction probability for women vs. men or for nationals vs. foreigners."*

In the United States, for example, Afro-American defendants were falsely labeled with a high risk of recidive and given higher bail conditions, kept longer in pre-trial detention and sentenced to longer imprisonment.[21]

Another problem is that judges will increasingly rely on algorithms, which compare earlier judgments and sentences and their differences and similarities. Similar cases will be assessed more equally and so decided more by algorithms. Judges leaning more on intransparent AI applications can endanger the impartiality and independence of judges.[22]

Moreover, decisions made by AI applications lack social control. In some cases breaking the law can be justified. For example, it will probably be justified to pass a red light to avoid a collision with a truck on the loose. A police officer can make this distinction, a red light camera will ticket all drivers that pass the red light.[23] In this respect, the White Paper mentions human oversight. Yet, the above discussed SyRI case, as well as recent examples of ethnic profiling by the Dutch border police show that human oversight can only serve as a remedy, where AI decisions are explainable, the personnel is authorised to reverse decisions, there are no policing targets to be met and the relevant personnel is highly trained and fully aware of the potential fundamental rights violations, that can be caused by the specific use of an AI application.

Finally, AI applications can have a negative effect on the equality of arms. Algorithms and decision making, based on algorithms, are usually intransparent, due to their complexity. This means that persons affected, like suspects, might lack the means to verify how a given decision was taken. This can lead to an unequal position of all parties involved, particularly in criminal

[21] Acces now, *Human rights in the age of Artificial intelligence*, page 19.
[22] M.J. Vetzo, J.H. Gerards en R. Nehmelman, *Algoritmes en grondrechten*, Boom Juridisch, Den Haag 2018. Page 168-169.
[23] Acces now, *Human rights in the age of Artificial intelligence,* page 19.

cases, because a government could have a technological advance.[24] Yet, from a human rights perspective, it is essential that all grounds for a decision are clearly communicated, as the consequences of decisions in criminal justice or social security are of the most severe nature (deprivation of liberty, loss of livelihood or housing) and a meaningful defence is contingent upon knowing all grounds for a given decision.

The Dutch SyRI case, set out above, serves as a clear reminder that the use of opaque algorithms in a social security (or criminal justice setting for that matter) may affect a number of human rights.

5.6. Freedom of movement

- **Article 45 EU Charter, Freedom of movement and of residence**

1. Every citizen of the Union has the right to move and reside freely within the territory of the Member States.

2. Freedom of movement and residence may be granted, in accordance with the Treaties, to nationals of third countries legally resident in the territory of a Member State.

To strengthen the external borders and internal security of the EU, the European Commission has made several proposals to upgrade and expand European border and security information systems. The two interoperability proposals concern also existing centralised systems, like SIS, which allows competent authorities e.g. to enter and consult alerts on third-country nationals for the purpose of refusing their entry or stay in the Schengen area. SIS will also contain databases for fingerprints, palm prints, facial images and DNA concerning, for example missing persons, persons involved in terrorism-related activities or migrants to tackle irregular migration.[25]

Article 24 paragraph 1 of REGULATION (EU) 2018/1861 mentions the conditions for entering alerts for refusal of entry and stay in SIS:

" (a) the Member State has concluded, based on an individual assessment which includes an assessment of the personal circumstances of the third-country national concerned and the consequences of refusing him or her entry and stay, that the presence of that third-country national on its territory poses a threat to public policy, to public security or to national security, and the Member State has consequently adopted a judicial or administrative decision in accordance with its national law to refuse entry and stay and issued a national alert for refusal of entry and stay; or
(b) the Member State has issued an entry ban in accordance with procedures respecting Directive 2008/115/EC in respect of a third-country national."

[24] M.J. Vetzo, J.H. Gerards en R. Nehmelman, *Algoritmes en grondrechten*, Boom Juridisch, Den Haag 2018, page 170-171.
[25] https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/628267/EPRS_BRI(2018)628267_EN.pdf, page 2.

It is a good thing that member states can work together to reinforce the external borders and internal security of the EU. Member States can e.g. exchange information about third-country nationals, refused in their country. If this individual wants to travel to another Member State, he will also be refused in that country, based on the information they received from the first country. But countries will not make their own decision. Errors in the information shared in these systems can be a serious violation of the freedom of movement.

5.7. Right to free elections

- **Article 3, protocol no. 1 to the ECHR**

The High Contracting Parties undertake to hold free elections at reasonable intervals by secret ballot, under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature.

In 2016, Carole Cadwalladr, a journalist at The Guardian, found out that a company called Cambridge Analytica, used millions of profiles of Facebook to send them selected advertisements related to the Brexit referendum. With algorithms and big data this company targeted voters and found out what they thought and what their fears were. With AI it is possible to screen all profiles available on the internet and to know what people's preferences are, which political opinion they have. In this case, with this information, they could influence the voters with personal directed advertisements. They used this information to influence their choices and send them advertisements, in favour of Brexit, sometimes also with fake news. AI applications played a huge role in the Brexit referendum.[26] This same tactic was also used in the elections of the US. In the article of Carole Cadwalladr and Emma Graham-Harrison[27], the whistleblower sets out how they targeted public voters in the US to send them personal political advertisements.

These examples show how the role of AI applications in creating and spreading fake news and selected advertisements can lead to a real threat to the rights of free elections.

5.8. Right to work

- **Article 30 EU Charter, Protection in the event of unjustified dismissal**

Every worker has the right to protection against unjustified dismissal, in accordance with Union law and national laws and practices.

---

[26] Facebook's role in Brexit -- and the threat to democracy and https://www.volkskrant.nl/nieuws-achtergrond/werd-brexit-referendum-beinvloed-13-duizend-twitterbots-verspreidden-pro-brexit-boodschappen~bfffbdd8/

[27] Carole Gawalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach', The Guardian 17/03/2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

- **Article 31 EU Charter, Fair and just working conditions**

1. Every worker has the right to working conditions which respect his or her health, safety and dignity.

2. Every worker has the right to limitation of maximum working hours, to daily and weekly rest periods and to an annual period of paid leave.

AI applications can be used to find adequate candidates for a vacancy, but companies can also use AI to observe if employees meet the standards set by the employer.[28] These data can be used by the employer to see which employees are the most productive. In theory employers can even force their employees to wear smart devices to monitor their activities.[29] The monitoring of private communication on the workplace can constitute an interference with the respect for private life.[30] Amazon, for example, uses AI to keep an eye on the productivity of its employees. Employees with a low productivity will be fired.[31] This can be a risk for the rights concerning work.

6. NJCM's Comments on the proposed framework

As shown above in the previous section, AI applications may impact the fundamental rights of European citizens in many ways. The White paper rightly recognises this in section 5. Yet, the White paper sets out to present a rather detailed blueprint for the future legal framework of the matter, before any human rights impact assessment has been carried out. Hence, we recommend that the European Commission, before issuing any legislative proposals, carries out a thorough human rights impact assessment as mentioned in Commission Communication COM(2010) 573.

Moreover, it is likely that the proposed high *versus* low risk approach does not lead to an adequate protection of fundamental rights. To name a few reasons:

- Firstly, an AI application that is of high risk to fundamental rights, may be used in a low risk sector, e.g. a sports application that processes and shares medical data. Moreover, it lies within the nature of many AI applications to generate cross-sector effects. For instance, behavioural data collected in social media (entertainment sector) may be used to predict behaviour and such predictions may be (and are) in use for a variety of sectors, some of which are, in a fundamental rights context, high-risk applications (political advertising) and some which may not be (advertising for consumer goods).

- Secondly, it will be impractical or impossible to provide generic criteria for low-risk applications within a high-risk sector. For instance, the White paper provides as an example the scheduling system of a hospital. Yet, if such a system were to integrate the

[28] https://www.theguardian.com/technology/2019/apr/07/uk-businesses-using-artifical-intelligence-to-monitor-staff-activity
[29] Van Est & Gerritsen 2017, p. 24
[30] EHRM (GK) 5 september 2017, nr. 61496/08, ECLI:CE:ECHR:2017:0905JUD006149608 (Bărbulescu t. Roemenië), EHRC 2018/3 m.nt. B.P. ter Haar, JAR 2017/259 m.nt. C.M. Jakimovicz
[31] Amazon Uses AI To Fire Unproductive Employees

(automatic) 'optimization' of medical resources and waiting times for medical procedures (trading off financial interests with health), as may very well be possible, the scheduling system would take decisions that do generate a medical impact and hence a scheduling system may be of high-risk to the fundamental rights of patients (right to health, right to life) and would need to be assessed. For example, the scheduling system may take the decision when an operation is planned and how long this operation will last. There could be circumstances that a patient has a poorer health and the doctor needs more time for the surgery. The scheduling system cannot take these circumstances into consideration like a doctor.

- Thirdly, only a concrete impact assessment in a concrete case can determine whether an AI application is of high risk. Risks cannot be determined beforehand by defining low risk sectors that are exempt from the impact assessment that is necessary to protect human rights. In such an assessment, it must be determined whether an impairment is proportionate, if the application respects the principle of subsidiarity, and if, in case an AI application takes or influences decisions that impact human rights, AI (assisted) decisions can be reviewed by a judge (no opaque (black box) decisions), and if the principles of transparency, purpose limitation and data minimisation are observed.[32] In this respect we also point to the United Nations Guiding Principles on Business and Human Rights (UNGPs)[33] and OECD Guidelines for Multinational Enterprises.[34] These standards assign companies the responsibility to avoid harm and respect human rights and remedy abuses when they occur. They require businesses to conduct human rights impact assessments (HRIA's) and require them to "know and show" that they respect human rights with respect to their own activities, and the activities directly linked to their products and services and operations. We believe that an essential component of a future legal framework is to require businesses, who deploy products or services based on AI, to establish operational-level and non-judicial grievance mechanisms for the identification, and where relevant remediation of impacts on any stakeholder.[35]

In that vein, we suggest that the Commission reconsiders the sectoral approach to regulating AI applications as well as the list of mandatory legal requirements. In our view, the impact assessment and the mandatory legal requirements that are proposed for high-risk AI should be taken into account also outside the context of high-risk sectors. Moreover, we suggest that a genuine human rights impact assessment is carried out next to the mandatory DPIA as mentioned in the GDPR. At last, we propose that the well defined principles of privacy regulation of transparency, purpose limitation and data minimisation are fully taken into account in the legislation as well as in any impact assessment.

---

[32] See e.g. the SyRI case mentioned above, ECLI:NL:RBDHA:2020:1878.
[33] UN Office of the High Commissioner for Human Rights "Guiding Principles on Business and Human Rights: Implementing the 'Protect, Respect and Remedy' Framework" ("UNGPs"), HR/PUB/11/04, 2011.
[34] OECD Guidelines on Multinational Enterprises, 2011.
[35] These mechanisms should comply with UNGP Guiding Principle 31 terms to ensure their effectiveness.