

# Where's the gap?

---

MAPPING THE EXISTING  
REGULATORY LANDSCAPE FOR  
ARTIFICIAL INTELLIGENCE IN EUROPE

# If the EU wants to effectively regulate AI, a better understanding of initiatives that already tackle policy concerns is required. This paper provides a critical insight.

On the 19th February 2020, the European Commission published a highly awaited White Paper on Artificial Intelligence. This document ostensibly seeks to lay the basis for a future risk-based regulatory framework that would govern AI use in Europe. One of the core justifications for this future programme of work is the feeling that existing legislation - at both EU and national level - may be inadequate to cater for the introduction of AI technologies.

As a first step in this process, the Commission has launched a [public consultation](#) to establish whether the necessary components for 'an ecosystem of trust' are addressed by applicable EU legislation, or whether new rules for AI systems might be necessary (Section 2 of the public consultation). Namely, stakeholders are asked whether concerns around **safety, protection of fundamental rights, explainability, liability and accuracy** need to be further explored. This consultation will be open until 14th June 2020.


Simultaneously, a number of the European Parliament's Committees are working in parallel to draft non-legislative Own-Initiative Reports (INIs). These are meant to inform the European Parliament's, and in turn, the Commission's position on a regulatory AI framework. The Reports cover several aspects of artificial intelligence, from liability for faulty products, to ethical guidelines and intellectual property rights.


In addressing such issues, it is important not to overlook the significant work that is being undertaken - or has already been - to combat precisely these issues, both at the European and national levels. Indeed, Europe is already complementing its existing regulatory framework with amendments, standards, court cases and even new regulations to accommodate the use of AI, which should be factored into high-level strategies going forward.


To facilitate this 'big picture' thinking and potentially support various stakeholders in making decisions about the validity of the concerns raised by the Commission, we provide here a snapshot of illustrative examples that depict the various strands of policy initiatives that are currently being driven forward across Europe. The examples are categorised according to the policy areas that are outlined in the public consultation on the White Paper. This mapping exercise should enable practitioners, policymakers and companies alike to identify the potential policy and regulatory gaps, if any, that upcoming EU legislation could fill.





## Endangering safety


- 


The [EU Cybersecurity Act](#), which came into force in June 2019, simultaneously strengthened the EU regulator (the European Union Agency for Network and Information Security, ENISA) and **established an EU-wide cybersecurity certification framework**. Currently, certification is largely voluntary but it has been recognised that ‘critical’ products or activities may see this become mandatory.
- 

The European Telecommunications Standards Institute (ETSI) has led numerous work programmes over recent years to provide [industry standards in fields relating to connectivity and Internet of Things \(IoT\)](#), including network security, radio spectrum requirements, functional architectures and interface descriptions. ETSI has also produced more sector-specific standards that relate to IoT and AI, including for intelligent transport systems and eHealth. The standards body launched in October 2019 a new Industry Specification Group on Securing Artificial Intelligence (ISG SAI).
- 

The use of AI in medicine falls under the definition of ‘software’ in the new [Medical Device Regulation \(MDR\)](#), which was set to come into force in May 2020 prior to COVID-19 disruption. This will **place AI HealthTech systems within the scope of the pre-existing classification system** that has corresponding requirements to ensure safety.
- 

European aviation regulator, EASA, concluded a research project in March 2020 with the Swiss AI-autopilot development company Daedalean, which culminated in a report ([Concepts of Design Assurance for Neural Networks](#)) exploring the **challenges associated with use of neural networks in aviation**, and establishing a preliminary set of guidelines. The next step by EASA will be to “generalise, abstract and complement these initial guidelines, so as to outline a first set of applicable guidance for safety-critical machine learning applications”.
- 

According to the Netherlands’ 2019 [Experimental Law on Self-driving Vehicles](#), companies that wish to test self-driving vehicles must submit an application stating that **previous tests have ensured a minimum level of safety, environmental protection and reliability** of data communications.
- 

The Norwegian Ministry of Local Government and Modernisation’s [National Strategy for AI](#), published in January 2020, prioritised ensuring technical robustness of AI systems. As a result, the strategy launched a new programme of work by the Norwegian National Security Authority to build its expertise in **securing AI systems from cybersecurity threats**.
- 

Spanish Internet service providers have the **statutory duty to inform their customers about online risks for children** and available filtering technologies under [Spanish Law 32/2002](#) on Information Society Services and Electronic Commerce.



## Breach of fundamental rights



The EU's [General Data Protection Regulation](#) (GDPR, 2018) places **restrictions on data processing** in various situations, especially when it involves personal or identifiable data and/or when the resultant decisions have legal implications or 'significantly affects' the data subject. It specifically outlines some core principles for collecting and processing personal data, among them accuracy, integrity, confidentiality, lawfulness, fairness and transparency.



The [EU Charter of Fundamental Rights](#) brings together all the personal, civic, political, economic and social rights enjoyed by people within the EU, which shall be respected in the context of any legislative process and initiative. It is legally binding for all Member States and has been regularly updated to reflect changes in society - including scientific and technological developments. The Charter now **includes a 'third generation' of fundamental rights**, such as data protection, guarantees on bioethics and transparent administration.



The [2016 EU Police Directive](#) applies **central data protection tenets of the GDPR to police authorities** in the EU, including the requirement for a data protection officer, data protection impact assessments, and individuals' rights to seek amendment and correction. For instance, according to the directive, data that identifies sensitive personal characteristics (e.g. ethnicity, political affiliation, union membership) can be carried out only when and if strictly necessary - and in a safeguarded manner. The Directive requires by nature Member States to pass an implementing legislation.



The EU [Copyright Directive](#) prevents companies from "mining" text and data freely available online for commercial purposes, among others. As such, **copyright-protected data cannot be extracted as training data** for AI - with the aim of upholding copyrights. Article 17 of the Directive also **requires content-sharing online platforms to obtain licences from rights holders to publish copyrighted works**. Without the appropriate licence, platforms are liable for copyright infringement, unless these are able to demonstrate that they have made "best efforts" to obtain a licence, to "ensure the unavailability" of specific works on the platform if rights holders requested their removal, and to "prevent their future uploads". All EU Member States are required to amend their legislation to conform to the new Copyright Directive by June 2021, although some Member States continue to have concerns. So far, Luxembourg, Malta, Portugal and Poland have signaled "no activity" on the transposition process. The government of Poland has even asked the Court of Justice of the EU to annul Article 17, arguing that imposing the obligation to make such "best efforts" forces platforms to automatically verify (and in turn, filter) user-uploaded content. Meanwhile, in January 2020, the UK Government asserted that it had no plans to implement the Directive.



The Norwegian Ministry of Local Government and Modernisation pledged in its January 2020 [National Strategy on AI](#) to establish a new **advisory body and regulatory sandbox to examine the intersection between AI and data protection** under the remit of the Norwegian Data Protection Authority. The purpose of such a sandbox will be to ensure that businesses have a better understanding of the regulatory requirements placed on data protection, and that authorities gain a better understanding of new technological solutions and more easily identify potential risks and problems.



While acknowledging that the processing of biometric data through facial recognition without consent may contravene GDPR, Spanish police have implemented [‘appearance search’ AI software](#) which they argue is different in that it **detects facial traits, age, colours and shape in the same way that a police officer could do**, but can screen this footage with unprecedented speed. Results are compared with other video surveillance footage, but not with Government databases.



Portugal’s [Automation and the Future of Work](#) report (2017) describes the main **challenges caused by automation and its effects on salaries**, and suggests that public and private policies should aim at diminishing job losses and focus on adult learning and vocational education and training (VET). It further highlights the need for an adequate framework promoting business adaptability to the labour market’s changing needs and the adoption of new technologies and processes. In 2019, it was [announced](#) that the Government would seek to promote further research into the impacts of AI on society more broadly, going beyond employment, and looking at other areas such as democracy and fairness.



In 2018, Finland published a report on [“Work in the Age of Artificial Intelligence”](#) within the scope of its national AI programme. The report states that in order to **harness the potential of AI in the labour market**, society must invest in updating workers’ skills, facilitating workforce mobility and generating innovations that complement human labour - all the while respecting workers’ rights. AI could indeed also benefit employment in that it could help workers move on to roles that are a better match with their competence and free up less demanding jobs for the unemployed and those entering the labour market.



In its recent White Paper entitled [“Rome call for AI Ethics”](#), co-signed by IBM and Microsoft, the Vatican highlights **“impartiality” as a key principle to promote the ethical development** of Artificial Intelligence - thus one that respects fundamental human rights. “Impartiality” is defined as “not creating or acting according to bias, thus safeguarding fairness and human dignity.”



In 2019, the Netherlands published a [“Strategic Action Plan for Artificial Intelligence”](#) where the government outlines its plans to accelerate the development of AI, while safeguarding “public values” and fundamental rights. Among these is human dignity and autonomy, for instance vis-a-vis the danger of dehumanization and the influence of AI on making choices. In this context, the Ministry of Social Affairs and Development is looking into ways to **monitor/target AI-led discrimination in recruitment and selection processes by employers**, such as age biases.



## Leading to discriminatory outcomes



The European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) is currently drafting a non-legislative [Own-Initiative Report \(INI\) on the use of Artificial Intelligence in criminal law](#) and its use by the police and judicial authorities in criminal matters. The Own-Initiative Report, which aims to inform the Parliament's position on a EU-wide regulatory framework for AI, will look into different questions related to the use of Artificial Intelligence in this context, such as benefits and risks of this new technology, predictive policing, facial recognition, as well as the ethical and fundamental rights implications.



In its [Strategic Action Plan for Artificial Intelligence](#), the government of the Netherlands indicates that the national Royal Library of The Netherlands is increasingly **making data available as training material for AI to mitigate bias** to state-of-the-art algorithms. The library has the expertise to assess training material's bias that can in turn lead to discriminatory AI applications. To this end, the public library has developed an "assessment framework" to evaluate the "quality of AI" on the basis of seven principles: accessibility, inclusiveness, supervision, transparency, neutrality, safety and compliance.



In 2018, the United Kingdom's Centre for Data Ethics and Innovation (CDEI) was asked by the Government to explore the potential for bias in algorithmic decision-making. Last year, the CDEI published an interim report of its [Review into Bias in Algorithmic Decision-Making](#), focused on exploring bias in four sectors: policing, financial services, recruitment and local government. The Review seeks to **identify and mitigate bias, by tackling the inputted data, tools and techniques, and governance**, which could inform specific legislation going forward. The CDEI is expected to publish its final report and recommendations to the Government before the end of 2020.



France's 2016 [Loi pour une République Numérique](#) (Digital Republic Act) introduced a provision on individuals' right to know the **explanation behind the decisions made by public sector bodies about individuals**, particularly where the decision is "taken on the basis of an algorithmic treatment". Given the obligations included in the EU's Better Enforcement Directive, this is likely to be extended to the decisions made by private actors as well.



## Explainability of rationale for AI decisions



The European Union's [Better Enforcement Directive](#) (Directive 2019/2161, part of the New Deal for Consumers) adds a new obligation for traders to **inform consumers when the price is personalised** on the basis of automated decision-making. This obligation will be applicable from 28 May 2022. The Better Enforcement Directive also amends [Directive 2005/29/EC](#) on unfair commercial practices from 2005, complementing it with a digital angle. This updated consumer protection legislation aims at tightening transparency requirements for businesses.



The United Kingdom's Information Commissioner's Office (ICO) and the Alan Turing Institute (ATI) - the national institute for data science and artificial intelligence - have recently launched their guidance, "[Explaining decisions made with AI](#)", to help businesses explain the processes, services and decisions delivered or assisted by AI to the individuals affected by them. Going forward, businesses could face financial penalties if they are unable to explain such processes and decisions, as [warned](#) by the ICO's Executive Director for Technology Policy and Innovation last year.



In its [Strategic Action Plan for Artificial Intelligence](#), the Dutch government has committed to establishing a "transparency lab" for government organisations to exchange knowledge and support in the areas of transparency, explainability and accountability. The government will conduct research into the legal aspects of decision-making algorithms and AI applications in the administration of justice, among others. The government is also investing in research into the responsible use of AI as well as the transparency and explainability of algorithms (through its [VWData programme](#)). The Plan stipulates that AI applications with a high impact on people or society "should be controllable": through "technical transparency" (transparent training data, models and source codes), and/or through explainability of the AI system (either the system as a whole or specific results). Companies and governments have a **legal responsibility to provide sufficient insight into the AI applications** that they use, and the associated procedures.



In 2018, Luxembourg's financial watchdog published a [White Paper on the Opportunities, Risks and Recommendations of Artificial Intelligence for the Financial Sector](#). The White Paper states that institutions should implement measures to ensure the **explainability of their artificial intelligence and machine learning systems** from the design phase. The regulator claims that explanations can help to get a functional understanding of the behaviour of machine learning systems and check whether bias is incorporated, which may in turn lead to substantial errors or discrimination.



## Liability and compensation for victims

- 

The European Parliament’s Legal Affairs (JURI) Committee has drafted a non-legislative Own-Initiative Report (INI) on ‘[Civil liability regime for artificial intelligence](#)’. The Report argues that the “**deployer**” of an AI system **should be held liable for harm** caused by the system, as she/he is “controlling the risk associated with it and benefitting from its operation”, and because she/he will be in many cases the first visible contact point for the victim. Furthermore, “high-risk” AI systems such as drones and autonomous vehicles should fall under a strict liability regime. The Report also states that the Product Liability Directive should be used for civil liability claims against producers of a defective AI product, and it should be subject to a potential review if necessary. While Parliamentary Own-Initiative Reports are non-binding, they will inform the Parliament’s general approach to the AI framework - and consequently, the Commission’s final proposal as well.
- 

The EU Product Liability Package includes the [Product Liability Directive](#) and the [General Product Safety Directive](#). According to the Product Liability Directive, **producers of defective products are subject to strict liability, and the injured party is entitled to compensation** if she/he can prove the damage, the defect in the product and the causal link between the two. Discussions are ongoing in the European Parliament on whether the Directive should be revised to explicitly include AI systems and/or services. The Product Safety Directive complements sector-specific legislation and requires that all consumer products be safe. The existing product safety framework is by nature technology neutral, and as such it also applies to products that incorporate AI technologies.
- 

The European Union is currently finalising a review process of consumer law through the [New Deal for Consumers](#). This includes a Directive on representative actions for the protection of the collective interests of consumers (“[Collective Redress](#)” Directive), which is currently subject to interinstitutional negotiations. The Directive aims to **make it easier for consumers to seek redress, particularly in situations of mass harm** and which may have cross-border impacts. Under the current proposal, Member States would be required to designate independent qualified entities who can organise collective action cases, and to potentially empower an administrative authority to issue a declaratory decision regarding the liability of the trader for consumer harm, including unfair business practices. This Directive is meant to be technology-neutral, and hence would be applicable to AI applications.
- 

The so-called “[Villani Report](#)”, which complements France’s [national strategy for AI](#) (2018), puts forward a series of policy recommendations to make sure that AI respects the principles of accountability and transparency. Among these is the formulation of **improved “collective rights” concerning data** (recognising that AI systems often have a mass effect, rather than an individual one), such as support for data class actions and right to compensation.





Germany's [Ethics Commission Report on Automated Driving](#) (2017) states that **liability for damage caused by activated automated driving systems is governed by the same principles as in other product liability**. From this, it follows that manufacturers or operators are obliged to continuously optimize their systems and also to observe systems they have already delivered and to improve them where this is technologically possible and reasonable.



Last year, the Estonian Parliament considered a 'kratt-law' legislative package ([#KrattAI](#)) which proposed that **AI be given separate legal status and corresponding liability**, similar to that of companies. It was decided that, for the time being, the liability and responsibility of AI decisions should continue to fall to the company or individual that directly caused its use. The company would thus be held responsible for the damage and thus object of consumer redress, for instance.



## Inaccuracy



[Article 16 of the GDPR](#) means that if the output of an AI system is personal data, **any inaccuracies can be challenged by data subjects**. For example, if a marketing AI application predicted a particular individual was a parent when they in fact have no children, its output would be inaccurate as a matter of fact. In such an instance, the individual concerned would have the right to ask the controller to rectify the AI output. Similarly, Article 22 of the GDPR requires that if AI outputs have legal or similar effect on data subjects (regardless of whether it classifies as personal data or not), then organisations are obliged to put in place “appropriate mathematical and statistical procedures” for such profiling to ensure accuracy.



In February 2020, the Estonian Ministry of National Affairs and the Hungarian Ministry of Innovation and Technology signed a [Memorandum of Understanding](#) to collaborate in **establishing a Trustworthy AI Training Range**. Among other things, the project will allow for reliability testing of AI systems before they are used in medicine, ensuring that all incoming data is reliable and unbiased, and that the outputs are subsequently consistent. The first AI applications to be tested through this will be those that support radiologists in breast cancer screening; support pathologists when screening for early changes in colon cancer patients; and an algorithm for the prevention of heart disease.



The [Barcelona Declaration of March 2017](#), which was endorsed in 2019 by the Spanish Ministry of Science, Innovation and Universities, called for greater attention in national policy to the reliability and security of AI systems. Specifically, it proposed the development of **verification and validation procedures for data-driven machine learning systems** that would be shared by ‘a network of agencies’ across European countries.



As a part of the broader work that the ICO is undertaking on developing a framework for auditing AI, the data protection regulator also issued specific guidance in May 2019 regarding [ensuring accuracy of AI systems](#). The regulator stated that any organisations adopting AI systems should a) ensure that all functions and individuals responsible for AI development, deployment and monitoring are adequately trained to understand the associated accuracy requirements and measures; b) adopt an official common terminology that staff can use to discuss accuracy performance measures; and c) **ensure that accuracy and its associated measures be considered from the design phase, and be tested throughout the AI lifecycle**. The guidance makes clear that “accuracy measures should also be regularly reviewed to mitigate the risk of concept drift and change policy procedures should take this into account from the outset”.



The Netherlands’ Ministry of Economic Affairs and Environment launched in October 2019 a [Strategic Action Plan on Artificial Intelligence](#) which established a priority of **improving the accuracy of algorithmic decision-making** by, along with other measures, making available high quality datasets for AI processing.

# Get in touch with Inline

If you would like more information about the issues affecting you, or to discuss the political and regulatory challenges that your business faces, then please get in touch.



**Megan Stagman**

**Senior Policy Analyst**

megan.stagman@inlinepolicy.com



**Giulia Iop**

**Policy Analyst**

giulia.iop@inlinepolicy.com



**Alessandra Venier**

**Policy Analyst**

alessandra.venier@inlinepolicy.com



## Inline Policy are the specialists in politics and regulation for the tech sector

We work at the heart of UK and EU markets to provide some of the world's most innovative companies with:

- Policy analysis and intelligence across the EU
- Advocacy campaigns to influence policy makers
- Profile raising and reputation management

[www.inlinepolicy.com](http://www.inlinepolicy.com)

All rights reserved. You are free to share this publication with others. However, no part of it may be reproduced in any form or by any means, electronic or manual, without prior written permission from the publisher.

Copyright© Inline Policy 2020



The specialists in politics and  
regulation for the tech sector

[www.inlinepolicy.com](http://www.inlinepolicy.com)