AI-REGULATION.COM

You Say You Want AI Regulation?
Welcome to AI-Regulation.com

CHRISTAKIS Theodore & BANNELIER Karine

AI-Regulation.com
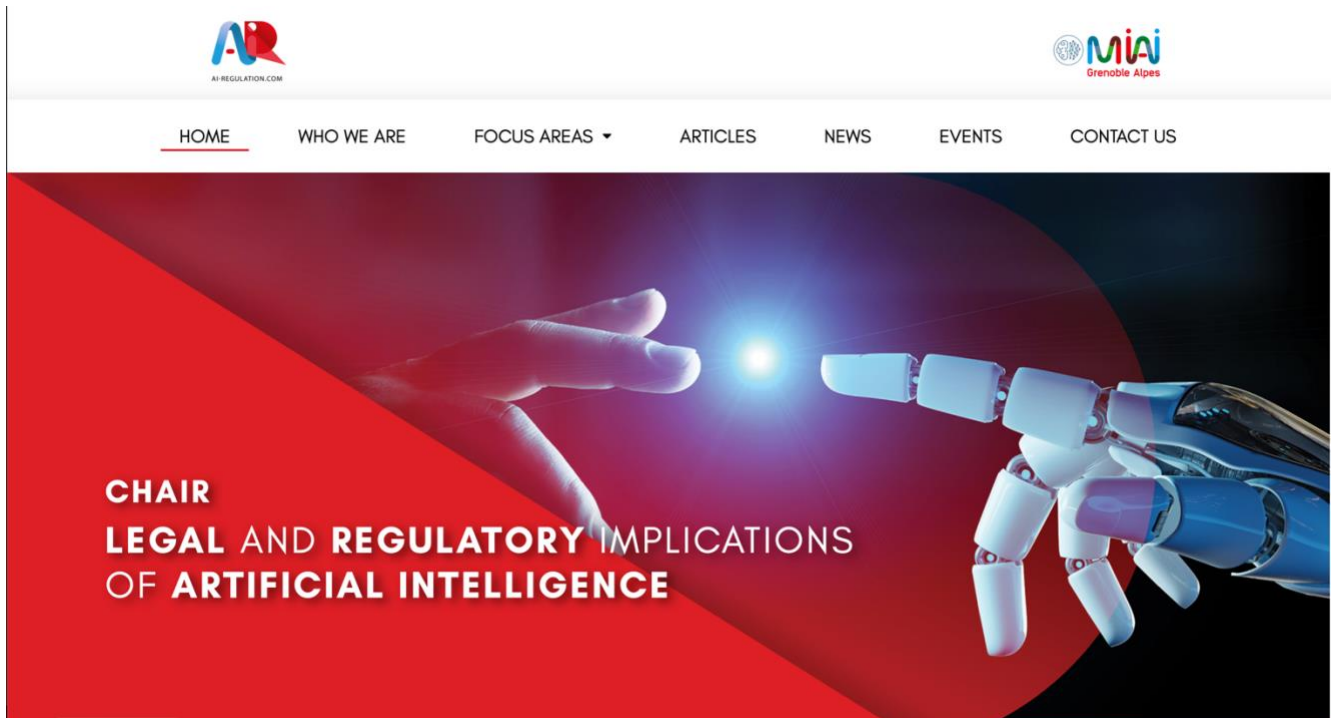
CHAIR LEGAL AND REGULATORY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

Welcome to AI-Regulation.com, the website of the Chair on the Legal and Regulatory Implications of Artificial Intelligence at MIAI Grenoble Alpes!

The Chair has been chosen by an international panel of experts to form part of the Multidisciplinary Institute on Artificial Intelligence created at the Université Grenoble Alpes, following a particularly competitive selection process commissioned by the French Government. Our members are experts in law, economics, computer and data science, all actively working in the field of data protection, privacy, cybersecurity and AI. The Chair's objective is to become a valuable point of reference regarding the legal and regulatory questions raised by artificial intelligence and to contribute to national, European and international debates on these issues.

The Chair, and its website, come at a key juncture in the rise of AI. AI has the potential to make breakthrough advances in several areas, but its growing applications raise complex questions and provoke broad concerns throughout society. How can we guarantee that AI is designed and used responsibly? How do we establish ethical and legal rules to protect people, avoid bias and help establish fair and adequate liability schemes? Given the risks posed by the growing power of artificial intelligence and its widespread applications, more and more voices in Europe and the rest of the world are calling for an appropriate regulation of artificial intelligence.

You say you want AI Regulation?

The European Commission President Ursula von der Leyen had initially promised that in her "first 100 days in office" she would "put forward legislation for a coordinated European approach to the human and ethical implications of AI". The general idea was that the EU should take the lead on regulation of AI – exactly as it did in the field of personal data protection. Regulation of artificial intelligence is seen by some in Europe as a kind of "the next GDPR".

In reality, Ursula von der Leyen's promise was overly ambitious: AI is not a monolithic block to regulate with a magic wand. Regulation in this field requires a careful, sector-by-sector and risk-based approach.

Instead of "hard rules", the European Commission finally published on February 19th, 2020 a White Paper on Artificial Intelligence, which will remain [open for comments until 19 May 2020](#). This is not a legally binding text but a kind of roadmap for the future regulatory framework.

Some found it disappointing that the European Commission was unable to go further, at least concerning some important points.

For instance, the part of the White Paper dedicated to **facial recognition** (or what the Commission prefers to call *"remote biometric identification"*) might seem at first sight to be disappointing to those who are calling for a moratorium on the use of Facial Recognition Technologies ("FRTs") in public spaces. Indeed, a [first draft of the White Paper, leaked on January 19th](#), included the eventual option that a "future regulatory framework could include a time-limited ban (e.g. 3-5 years) on the use of FRT in public spaces" in order to provide the leeway required to implement "a sound methodology" for assessing the potential impact of FRTs and to develop possible risk management measures.

The final version of the White Paper does not include any such option. In fact, it does not include anything new at all on a substantive level with regards to FRTs: it just recalls that according to existing EU rules (such as the General Data Protection Regulation (GDPR) and the Law Enforcement Directive) the use of FRTs must be "duly justified, proportionate and subject to adequate safeguards".

However, the White Paper does include some important news about FRTs: the Commission decided to launch a broad European debate on the specific circumstances, if any, which might justify use of FRTs in public places and on what safeguards should be adopted. Sceptics could say that the Commission is "kicking the can down the road" but ["it only seems reasonable that the Commission needs more time to examine such a complicated issue and to advance carefully in this field"](#).

More generally, the Commission's adoption of a cautious approach in relation with AI regulation, rather than ["scrambling to roll out policies to meet political deadlines"](#), could be seen in a positive light.

This is not to say that the White Paper does not include strong ideas. There are at least two important elements that need to be highlighted in this respect.

You say you got a real solution? Well, we'd all love to see the plan

First, the White Paper compiles an impressive list of existing EU rules (see figure 1) that are technologically neutral and apply to the field of AI – and proceeds to an interesting discussion concerning the necessary adjustments to these rules in order to address the specific risks and concerns raised by AI.

B. POSSIBLE ADJUSTMENTS TO EXISTING EU LEGISLATIVE FRAMEWORK RELATING TO AI

An extensive body of existing EU product safety and liability legislation[38], including sector-specific rules, further complemented by national legislation, is relevant and potentially applicable to a number of emerging AI applications.

As regards the protection of fundamental rights and consumer rights, the EU legislative framework includes legislation such as the Race Equality Directive[39], the Directive on equal treatment in employment and occupation[40], the Directives on equal treatment between men and women in relation to employment and access to goods and services[41], a number of consumer protection rules[42], as well as rules on personal data protection and privacy, notably the General Data Protection Regulation and other sectorial legislation covering personal data protection, such as the Data Protection Law Enforcement Directive[43]. In addition, as from 2025, the rules on accessibility requirements for goods and services, set out in the European Accessibility Act will apply[44]. In addition, fundamental rights need to be respected when implementing other EU legislation, including in the field of financial services, migration or responsibility of online intermediaries.

While the EU legislation remains in principle fully applicable irrespective of the involvement of AI, it is important to assess whether it can be enforced adequately to address the risks that AI systems create, or whether adjustments are needed to specific legal instruments.

---

[38] The EU legal framework for product safety consists of the General Product Safety Directive (Directive 2001/95/EC), as a safety net, and a number of sector-specific rules covering different categories of products ranging from machines, planes and cars to toys and medical devices aiming to provide a high level of health and safety. Product liability law is complemented by different systems of civil liability for damages caused by products or services.
[39] Directive 2000/43/EC.
[40] Directive 2000/78/EC.
[41] Directive 2004/113/EC; Directive 2006/54/EC.
[42] Such as the Unfair Commercial Practices Directive (Directive 2005/29/EC) and the Consumer Rights Directive (Directive 2011/83/EC).
[43] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
[44] Directive (EU) 2019/882 on the accessibility requirements for products and services.

Figure 1: The existing EU Legal Framework relevant for AI applications: capture of the White Paper

Second, the White Paper introduces the strong regulatory idea of protection from harmful AI: "in view of the high risk that certain AI applications pose for citizens and our society", **high-risk AI applications** should have to be tested and receive certification before reaching the single market.

The Commission lays out two cumulative criteria for what it considers a **"high risk" use of AI**. First, is the AI application *deployed in a sector* (e.g. health, energy or transportation) where, given the characteristics of the activities typically undertaken, significant risks can be expected to occur? Second, is the AI application *used in such a manner* as to pose significant risks of injury, death, material or immaterial damage, or harm to the rights of an individual or a company?

For all these cases, the Commission introduces the idea of mandatory, objective, prior **conformity assessments** to ensure that such AI systems meet some mandatory requirements (especially linked to human rights considerations). In essence, the Commission is inspired here by conformity assessment mechanisms that already exist for a large number of products destined for the EU's internal market (ex. cars or chemicals). Inversely, the Commission suggests a lighter touch for "non-high-risk" data uses, to avoid hindering innovation.

It is clear, from the above, that, far from being done in "100 days", AI regulation in the EU will be a long process, either in order to adjust existing rules (such as those concerning EU liability law) or in order to develop new ones. Similar developments are to be expected in several countries outside Europe, as there is a multiplication of calls for AI regulation worldwide, including in countries such as the US, where Federal agencies are nonetheless strongly called upon to "avoid regulatory or non-regulatory actions that needlessly hamper AI innovation and growth".

"We're doing what we can": Mission statement and scientific objectives

The main mission of the Chair on the Legal and Regulatory Implications of Artificial Intelligence will be to undertake research on whether and how AI regulation can support sustainable and ethical innovation.

How should the requirements of fairness, non-discrimination, meaningful human oversight, respect for privacy, safety, transparency, accountability and effective redress be implemented and applied in the different fields of application of AI? How can we open the algorithmic "black-box" - thus facilitating the auditability and scrutiny of AI Systems - while at the same time preserving industrial secrets? What are the different legal models of liability and responsibility that we need to design when it comes to algorithmic systems? How should we interpret and apply existing rules to AI, such as the GDPR or technology-neutral rules related to human rights, non-discrimination and competition law? What are the potential legal loopholes and how can we adopt a risk-based approach in order to elaborate new rules? How should we regulate AI's use in a way that is beneficial to society and protective of fundamental rights while at the same time ensuring that innovation is not hindered and legal regimes do not become obstacles to AI's development?

Our website aims to become a forum to provide some answers to these questions and share the results of our research as well as insights on these issues from external collaborators and contributors. We publish substantive articles and reports as well as brief notes and news updates on worldwide developments in AI regulation.

Our research covers 8 Focus Areas:

1) [AI Governance and Regulation](#) (a cross-sectional field of research analysing the appropriateness of existing law (e.g., the RGPD) for AI applications and what AI governance might resemble in the future).

2) [Facial recognition](#).

3) [Virtual assistants and Chatbots](#).

4) [Smart cities, smart homes and IoTs](#).

5) [Data manipulation, AI and democracy](#).

6) [Health, AI and transhumanism](#).

7) [Connected and autonomous vehicles](#).

8) [AI, National and International Security](#).

You ask me for a contribution? Our first articles

We are launching our website today with an important study on facial recognition written by two members of our Chair, Claude Castelluccia and Daniel Le Metayer, Directors of research at [Inria](#) (the French National Institute for Research in Digital Science and Technology). The two authors highlight the importance of conducting impact assessments of applications and uses of facial recognition technologies and propose methodological approaches for the conduct of such impact assessments, illustrated by examples. While their risk analysis framework concerns facial recognition systems, their methodology could apply, *mutatis mutandis*, to other AI or algorithmic systems.

We are also very pleased to host today an op-ed on the French National Committee for Digital Ethics (FNCDE) by Claude Kirchner, emeritus research director at INRIA and Director of the FNCDE. Following a request by the French prime minister, the FNCDE was created in November 2019 and is composed of [27 members](#) from different disciplines, from IT specialists working in public or private research to philosophers, medical doctors, lawyers and members of civil society. The committee has already been commissioned by the Prime Minister to issue opinions on the ethical issues arising from three specific digital applications using machine learning: 1) Conversational agents (chatbots); 2) Autonomous cars; and 3) Medical diagnosis and health AI.

A third article, written by the Chair's member Camille Dubedout, a joint PhD candidate at Université Grenoble-Alpes and at the French National Cybersecurity Agency (ANSSI), focuses on the "Safe City" project initiated in the southern French city of Nice. The municipality intends to transform Nice into a model of "Safe city", through the deployment of AI solutions and, especially, facial recognition technologies. In order to achieve this, the City has planned a series of facial recognition tests in real-time conditions. Interestingly, these trials are also testing the tolerance of the French Data Protection Authority (CNIL). Indeed, CNIL has expressed great concerns over the compatibility of one of these "experiments" (conducted in French High Schools) with the GDPR – leading to a discontinuation of the "experiment" and to

some ferocious attacks against the French DPA by the City's Mayor and a few other politicians involved in this project.

We are also hosting today two contributions from our research fellows Katia Bouslimani and Mathias Becuywé, following the participation of our Chair in CPDP 2020, which was dedicated to "Data Protection and Artificial Intelligence".

The first paper presents some key takeaways of a CPDP panel discussing the important issue of secondary uses of health data, i.e. the re-use of data for another purpose than the one for which it was originally collected. These highlights include issues such as the role of consent in health AI, the issue of de/re-identification or an interesting discussion on who is benefiting from secondary uses of health data.

The second paper presents a report on another very interesting CPDP panel which focused on the use of FRTs in the United Kingdom. This panel discussed particularly interesting issues such as the following: Is there an appropriate legal basis for the different uses of FRTs by the police? What are/should be the safeguards in these cases? Is there a truly comprehensible review of *who* is using facial recognition and *for what exact purposes*? And what about the major issue of transparency?

To receive our future publications sign up here. Also sign-up to receive our Newsletter and follow us on Twitter in order to receive updates about all our activities and events.

* Thanks to The Beatles for their help!