FIU Law Review

Volume 17
Number 2 *Privacy Discussion Forum – University of Stockholm (Stockholm, Sweden, 2022)*

Article 5

Spring 2023

Supervision of Artificial Intelligence in the EU and the Protection of Privacy

Johanna Chamberlain
Uppsala University, johanna.chamberlain@fek.uu.se

Jane Reichel
Stockholm University, jane.reichel@juridicum.su.se

Online ISSN: 2643-7759

Recommended Citation
Johanna Chamberlain & Jane Reichel, *Supervision of Artificial Intelligence in the EU and the Protection of Privacy*, 17 FIU L. Rev. 267 (2023).
DOI: https://dx.doi.org/10.25148/lawrev.17.2.5

SUPERVISION OF ARTIFICIAL INTELLIGENCE IN THE EU AND THE PROTECTION OF PRIVACY

Johanna Chamberlain & Jane Reichel*

I. INTRODUCTION: ARTIFICIAL INTELLIGENCE, RISK MANAGEMENT, AND SUPERVISORY AUTHORITIES

One of the most rapidly changing legal and societal fields at the moment is that of Artificial Intelligence (AI). While AI technology has been advancing for decades and is now in a dynamic and expansive phase, the societal and legal perspectives have long been both underdeveloped and under researched. This is slowly beginning to change, causing many new questions to arise throughout the social sciences and humanities—not least in law. Among these uprising issues is the connection between regulating AI and protecting fundamental rights. AI often automatically entails mass collection, surveillance, handling, and sharing of massive amounts of data, including data on identifiable persons. This means that AI systems raise significant privacy and data protection concerns.[1] Furthermore, AI can be manipulative and obscure, sometimes to the extent that so-called dark

* Dr. Johanna Chamberlain is a post doc researcher within WASP-HS project "AI and the Financial Markets," Uppsala University, Department of Business Studies, e-mail: johanna.chamberlain@fek.uu.se, ORCID: https://orcid.org/0000-0003-0473-2076.

Professor Jane Reichel is a Professor in Administrative Law, Stockholm University, Faculty of Law, e-mail: jane.reichel@juridicum.su.se, ORCID: https://orcid.org/0000-0001-7509-4804.

[1] These are some of the issues that were discussed at the 2022 Privacy Discussion Forum in Stockholm, Sweden, as described by Professor Russell L. Weaver in the introduction to this issue. *See generally* Russell L. Weaver, *Privacy Discussion Forum: Introduction*, 17 FIU L. REV. 263 (2023).

patterns[2] and deep fakes[3] impact human consciousness and actions. This becomes particularly problematic when it comes to vulnerable parties who may not be aware of such phenomena—although it should be said that it can be difficult for most people today to distinguish between real and manipulated digital content.

In short, AI techniques, while often beneficial from an efficiency perspective, pose significant risks not only to privacy and data protection but also to human dignity and autonomy—to name but a few of the fundamental rights at stake. For this reason, legal initiatives regarding AI tend to focus largely on risk, and this is true also for the budding EU regulation in the area: The General Regulation on AI that was proposed by the Commission in April 2021 and is now being negotiated between the EU institutions.[4] Up until this proposal, the ICT[5] revolution has first and foremost prompted the EU legislator to address concerns relating to privacy, intellectual property, and the free movement of information. Certain aspects of manipulative information may be approached within existing EU consumer law[6] or data protection law,[7] but with AI our understanding of information as such is

2 Dark patterns have been defined as "design features used to deceive, steer, or manipulate users into behavior that is profitable for an online service, but often harmful to users or contrary to their intent." *See* Statement of Commissioner Rohit Chopra Regarding Dark Patterns in the Matter of Age of Learning Inc., FED. TRADE COMM'N (Sept. 2, 2020), https://www.ftc.gov/system/files/documents/public_statements/1579927/172_3086_abcmouse_-_rchopra_statement.pdf.

3 According to the Cambridge Dictionary, a deep fake (or deepfake) is "a video or sound recording that replaces someone's face or voice with that of someone else, in a way that appears real." *Deepfake*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/deepfake (last visited Oct. 1, 2022); *see generally* EUR. PARLIAMENTARY RSCH. SERV., TACKLING DEEPFAKES IN EUROPEAN POLICY (2021), https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf (providing an overview of EU initiatives in the area).

4 *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021) [hereinafter *Commission Proposal Laying Down Harmonised Rules on Artificial Intelligence*].

5 Information and Communications Technology.

6 *See* European Parliament and Council Directive 2005/29, art. 5, 2005 O.J. (L 149) 27, 28 (EC); European Parliament and Council Directive 2011/83, 2011 O.J. (L 304) 64, 72 (EU); Council Directive 93/13, 1993 O.J. (L 95) 29 (EC); *"Dark Patterns" and the EU Consumer Law Acqui: Recommendations for Better Enforcement and Reforms*, BEUC 1–2 (2022), https://www.beuc.eu/publications/beuc-x-2022-013_dark_patters_paper.pdf (discussing application of these frameworks on dark patterns).

7 *See EDPB Adopts Guidelines on Art. 60 GDPR, Guidelines on Dark Patterns in Social Media Platform Interfaces*, EUR. DATA PROT. BD. (Mar. 15, 2022), https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-art-60-gdpr-guidelines-dark-patterns-social-media-platform_en (stating that dark patterns have been part of the motivation for some of the national data protection authorities' decisions regarding administrative sanctions according to the GDPR); *Cookies: The Council of State Confirms the 2020 Sanction Imposed by the CNIL Against Amazon*, COMM'N NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (June 28, 2022), https://www.cnil.fr/en/cookies-council-state-confirms-2020-sanction-imposed-cnil-against-amazon

challenged. Who and what may be trusted? Can the complex problems that are caused by the accelerating technical developments be addressed through existing data protection and privacy laws, through the regulation on AI systems that is currently being created, or will there be a need for new specialized rules? How can freedom of information be safeguarded?

The proposed AI regulation sets out a risk-based approach, where supervisory authorities at the EU and national level play a central role. In a model building on and expanding the role of supervisory authorities under the General Data Protection Regulation (GDPR), the supervisory authorities of the proposed AI regulation are to be equipped with vast investigatory powers as well as competence to decide on very high administrative sanctions. As AI systems may be used in very different fields of policy areas, the proposed supervisory regime foresees that several categories of already existing supervisory bodies will be involved, namely authorities within data protection, product safety, financial markets, and law enforcement.[8] Also, other authorities may be given access to documentation created under the proposed regulation.[9]

In this paper, the supervisory regime in the proposed EU General Regulation on AI will be analyzed, with the aim to critically assess the role of supervisory authorities with regards to AI systems in safeguarding both the development of AI systems and protecting democratic and individual rights. As with other supervisory structure in EU law, such as data protection and financial market law, the proposed network is to consist of an agency at the EU level, the new European Artificial Intelligence Board (EAIB), as well as supervisory authorities located at the national level. These regulatory and supervisory administrative structures can be identified as a part of the success story described as the *Brussels effects,* where EU regulatory regimes on data protection have had a global impact.[10] However effective, can a network of independent supervisory authorities be trusted to effectively monitor the use of developing AI systems and at the same time balance the benefits and risk of the new technologies with the fundamental rights of privacy, data

(discussing the French data protection authority CNIL's decision regarding Amazon, where the extensive use of cookies was considered unlawful and resulted in fines of 35 million euro).

8 *See Commission Proposal Laying Down Harmonised Rules on Artificial Intelligence*, *supra* note 4, at recital 80 (Preamble); *see also Commission Proposal Laying Down Harmonised Rules on Artificial Intelligence*, *supra* note 4, arts. 9, 18–20, 29, 43, 61; European Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) 1 [hereinafter GDPR]; European Parliament and Council Regulation 2019/1020, 2019 O.J. (L 169) 1 [hereinafter Market Surveillance Regulation]; European Parliament and Council Directive 2013/36, 2013 O.J. (L 176) 338 (the Capital Market Directive IV).

9 *Commission Proposal Laying Down Harmonised Rules on Artificial Intelligence*, *supra* note 4, at recital 79 (Preamble).

10 ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD 34 (Oxford Univ. Press 2020).

protection, freedom of information, and non-discrimination?[11] Considering the largely unknown, dynamic character of AI, the central democratic function of freedom of information, and the individual right to privacy and data protection, the question must be asked if there is a limit to how much power it is reasonable to bestow on these networks of supervisory authorities. Since the focus of the paper is on administrative supervision, the AI proposal relating to law enforcement will not be included in the analysis.

The outline of the article is the following: section II focuses on the role and function of administrative supervision in the EU, while sections III and IV introduce the proposed AI Regulation and its risk-based approach. Sections V and VI present an analysis of the administrative supervisory regime in the proposed AI regulation. In a final section, conclusions are drawn.

II. ADMINISTRATIVE SUPERVISION IN EU LAW

The administrative infrastructure for the implementation of EU law can be described as a constitutionally rather complex story. Initially, implementation was conducted by the member states, with national competent authorities working independently each within its own constitutional and administrative setting, what is referred to as institutional and procedural autonomy.[12] The authorities remain accountable within national judicial, political, and financial accountability regimes.[13] Gradually, the EU legislature has introduced collaborative measures and instruments for the national authorities in the form of networks, organizational and procedural standards, and information exchange regimes. Together with a successive establishment of EU sector specific agencies, collaborating with the competent authorities at national level, a new form of administrative governance structure, often labeled a European composite administration, has developed.[14] Within several areas, for example in approval of medicinal and

---

11 Charter of Fundamental Rights of the European Union, arts. 7, 8, 11, 21, 2012 O.J. (C 326) 389. (The respect for privacy is codified in Article 7, the right to protection of personal data is codified in Article 8, the right to freedom of information in Article 11 and non-discrimination in Article 21 of the Charter).

12 Joined Cases 51 to 54/71, Int'l Fruit Co. v. Produktschap voor Groenten en Fruit, 1971 E.C.R. 1113 (introducing the principle of the institutional autonomy of the Member States); Case 33/76, Rewe-Zentralfinanz v. Landwirtschaftskammer für das Saarland, 1976 E.C.R. 1997–98 (introducing the principle of procedural autonomy).

13 Paul Craig, *The Locus and Accountability of the Executive in the European Union*, *in* THE EXECUTIVE AND PUBLIC LAW: POWER AND ACCOUNTABILITY IN COMPARATIVE PERSPECTIVE 315 (Paul Craig & Adam Tompkins eds., Oxford Univ. Press 2006); JANE REICHEL, ANSVARSUTKRÄVANDE – SVENSK FÖRVALTNING I EU [Accountability – Swedish Administration Within the EU] 23 (2010).

14 *See* Herwig C. H. Hofmann & Alexander Türk, *The Development of Integrated Administration in the EU and its Consequences*, 13 EUR. L. J. 253, 253–71 (2007); Eberhard Schmidt-Aßmann,

chemical products, implementation and monitoring of competition, and migration law, networks of European and national authorities work closely together in all stages of the governance circle. Even though the administrative structures, tasks, and competences vary between the areas, a common trait is that the networks of administrative authorities are to monitor the correct, uniform, and efficient application of EU law in the member states. As will be discussed further in section V, the diversity in institutional structures may in itself diminish efficiency and transparency in the implementation, especially when a matter involves several sector-specific policy areas.[15]

With regard to EU supervisory authorities, it must first be submitted that there is no commonly accepted definition of the concept of administrative supervision.[16] In legal doctrine, the main function of administrative supervision has been identified as the function of independently assessing and ensuring that actors within a sector fulfill their obligations and tasks according to the relevant law and that they can be held to account for failing to do so.[17] Within the administrative sectors targeted in the proposed AI Regulation, several have supervisory functions. Within Data protection, the independency of the supervisory authorities is founded in the EU Treaty, Article 16 of the Treaty of the Functioning of the European Union (TFEU), as well as in Article 8 of the Charter of Fundamental Rights (the Charter).[18] Each member state is to provide for "one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union."[19] The GDPR defines requirements for the independence of the national data protection authorities, general conditions, and rules for their establishment, as well as what competences, tasks, and powers they are to have.[20] The national data protection authorities collaborate closely with the European Data Protection Board (EDPB).[21] There is further an authority monitoring the application of data protection law for the EU

Introduction: European Composite Administration and the Role of European Administrative Law, *in* THE EUROPEAN COMPOSITE ADMINISTRATION (Oswald Jansen & Bettina Schöndorf-Haubold eds., 2011).

15 *See* Luca De Lucia, *Conflict and Cooperation within European Composite Administration (Between Philia and Eris)*, 5 REV. EUR. ADMIN. L. 43, 44.

16 IDA ASPLUND, DEN ENSKILDES RÄTTSSÄKERHET I INDIVIDNÄRA TILLSYN [THE INDIVIDUAL'S LEGAL CERTAINTY IN INDIVIDUAL SUPERVISION] 13 (2021).

17 *Id.*; HERWIG C.H. HOFMANN, GERARD C. ROWE & ALEXANDER H. TÜRK, ADMINISTRATIVE LAW AND POLICY OF THE EUROPEAN UNION 712 (2011).

18 Johanna Chamberlain & Jane Reichel, *The Relationship Between Damages and Administrative Fines in the EU General Data Protection Regulation*, 89 MISS. L. J. 668, 671–72 (2020).

19 GDPR, *supra* note 8, art. 51.

20 *Id.* arts. 52–58.

21 *Id*. arts. 68, 70.

level, the European Data Protection Supervisor.[22] Within financial market supervision, three European Supervisory Authorities (ESAs) have been set up: the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and European Securities and Markets Authority (ESMA).[23] The ESAs are to collaborate with authorities at the national level, as set out in other EU acts, defined either as supervisory authorities or competent authorities.[24] Within the area of product safety, the EU has introduced another concept, surveillance authorities. Also within this sector, the member states should appoint authorities which are to monitor and control the products put on the market, which may take corrective measures.[25] In comparison to the data protection and financial market area, the product safety laws are more flexible as to how the institutional structure is implemented at a national level, and the member states may allocate the corrective measures either to appointed authorities or upon application to courts.[26] The regulation covers a wide range of products and sectors, and most member states have allocated the surveillance tasks to quite a number of different authorities.[27]

III. REGULATING ARTIFICIAL INTELLIGENCE: THE PROPOSED EU LEGISLATION AND ITS TAKE ON PRIVACY AND DATA PROTECTION

Considering the fact that AI systems pose new and potentially serious risks to individuals, in comparison to other industries and products, it appears quite unique that no legal rules yet apply to the new technologies. Many actors, including the EU, therefore believe it is time for the law to take over the initiative from the tech industry when it comes to developing responsible and ethical AI. In light of these developments, the EU Commission adopted its proposal for a new General Regulation on AI. The suggested regulation will most certainly be altered a number of times before it reaches its final

22 European Parliament and Council Regulation 2018/1725, art. 52, 2018 O.J. (L 295) 39.

23 European Parliament and Council Regulation 1093/2010, 2010 O.J. (L 331) 12; European Parliament and Council Regulation 1094/2010, 2010 O.J. (L 331) 48; European Parliament and Council Regulation 1095/2010, 2010 O.J. (L 331) 84.

24 European Parliament and Council Regulation 1093/2010, *supra* note 23, art. 4; European Parliament and Council Regulation 1094/2010, *supra* note 23, art. 4.

25 Market Surveillance Regulation, *supra* note 8, arts. 14–16. Article 41 further requires the member states to enact rules on penalties for breaches of the regulation. *Id.* art. 41.

26 *Id.* art. 14.3.

27 The Commission has published two lists of the Market Surveillance Authorities within the member states, one by sector and one by country. *The Implementation of the Market Surveillance in Europe,* EUR. COMM'N, https://ec.europa.eu/growth/single-market/goods/building-blocks/market-surveillance/organisation_en (last visited on June 7, 2022) The lists are 255 and 271 pages, respectively.

shape but is nevertheless expected to come into force during the coming few years. Designing this legal framework is certainly a challenge, as multiple interests must be considered. While evolving risks do need to be addressed, the legislative project has met skepticism from AI enterprises, who claim that the EU, by regulating the area, will obstruct innovation and hand the AI market over to the U.S. and China.[28] In the suggested regulation, the social and economic benefits of AI are acknowledged and the goal of the AI act is described as creating a *proportionate legislation* that balances different interests.[29]

Privacy and data protection are noted as areas at risk several times in the proposed regulation and its preamble. While "data protection" is mentioned thirty times, the word "privacy" appears four times. Paragraph 15 of the preamble reads:

> Aside from the many beneficial uses of artificial intelligence, that technology can also be misused and provide novel and powerful tools for manipulative, exploitative and social control practices. Such practices are particularly harmful and should be prohibited because they contradict Union values of respect for human dignity, freedom, equality, democracy and the rule of law and Union fundamental rights, including the right to non-discrimination, data protection and privacy and the rights of the child.[30]

Further, privacy concerns relating to AI systems are mentioned in the context of employment. AI solutions that measure performance and behavior of employees may "impact their rights to data protection and privacy."[31] Another important area is the health sector, where access to health data in the EU for the purpose of training AI algorithms is to be designed in a "privacy-preserving" way.[32] Regarding data governing and special categories of personal data, Article 10.5 of the proposed regulation states that such data may be processed with appropriate safeguards for fundamental rights and

---

28 *See* Laurie Clarke, *The EU's Leaked AI Regulation is Ambitious but Disappointingly Vague*, TECHMONITOR (Apr. 20, 2021, 5:15 PM), https://techmonitor.ai/policy/eu-ai-regulation-machine-learning-european-union. The EU legislator is aware of the critique and has attempted to address it through the suggested articles 53–55 of the AI act on "Regulatory sandboxes," described as "measures in support of innovation."

29 *Commission Proposal Laying Down Harmonised Rules on Artificial Intelligence*, *supra* note 4, at 1.1 (Explanatory Memorandum).

30 *Id.* at recital 15 (Preamble).

31 *Id.* at recital 36 (Preamble).

32 *Id.* at recital 45 (Preamble).

freedoms, including "privacy-preserving measures" such as pseudonymization or encryption.[33]

The term "data protection" appears much more frequently than "privacy" in the AI proposal, most times in connection to the existing regulation on data protection. The collection and handling of data is an integrated part of AI solutions and one of the challenges when it comes to regulating AI systems is thus to identify (1) which issues already fall under the GDPR, and (2) how the two legal frameworks are to interact.[34] For example, data protection is mentioned in relation to the proposed prohibition on AI practices of unacceptable risk, where it is stated that such manipulative or exploitative practices could already be covered by existing data protection regulation.[35]

As mentioned above, the supervisory regime in the AI proposal builds on and expands the supervisory regime in the GDPR and there are many references in the proposal of the national data protection authorities, the European Board of Data Protection (EDPB) and the European Data Protection Supervisor, as well as the supervisory bodies within financial markets and product safety. In summary, the relationship between the AI regulation, the GDPR and other forms of market control might be seen as chronological, where the AI proposal will be filling in an AI dimension into the already existing supervisory regimes.

IV. THE RISK-BASED APPROACH AND HIGH-RISK ARTIFICIAL INTELLIGENCE SYSTEMS

In this section, some general remarks will be made on the structure of the proposed regulation, followed by a closer look at the rules applying to certain AI systems that will be of interest within the issues of supervision and sanctions. The AI act uses a "risk-based approach," often illustrated by a "pyramid of criticality." The risk pyramid is new in the EU context but not unique when it comes to regulating AI; similar models have already been developed in the U.S., Canada, and Germany.[36] The tiered risk structure thus appears to be globally establishing itself as a new norm for regulating AI

---

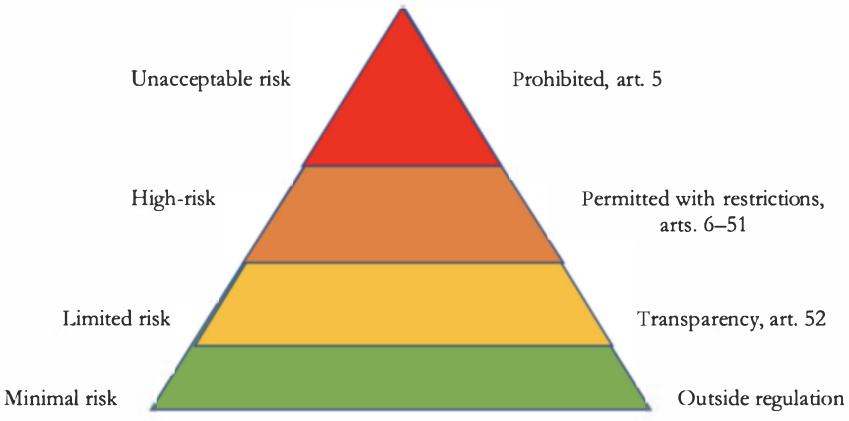
33 *Id.* art. 10.5.

34 *Id.* at 1.2 (Explanatory Memorandum).

35 *Id.* at 5.2.2 (Explanatory Memorandum).

36 *See* Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019); GOV'T OF CAN., CANADIAN DIRECTIVE ON AUTOMATED DECISION-MAKING (2021); *Opinion of the Data Ethics Commission – Executive Summary*, BUNDESMINISTERIUM DER JUSTIZ 173–182 (2019), https://www.bmj.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN.pdf?__blob=publicationFile&v=2.

systems.[37] The risk pyramid of the proposed AI regulation illustrates that this legal instrument largely focuses on high-risk AI systems:



As seen above, the bottom tier of the pyramid suggests that AI systems with "minimal risk" (for example, spam filters and video games) will fall outside the scope of the regulation. According to the EU Commission, the vast majority of all existing AI systems will belong in this category.[38] In the next level up, "limited risk" AI systems will be under the obligation to inform users that they are interacting with AI (and not human beings—a distinction that can sometimes be difficult to make).[39] Continuing up the pyramid, the next tier sets comprehensive restrictions for "high-risk" AI systems, and at the top level AI systems with "unacceptable risk" are to be prohibited. In the following the focus will be on high-risk systems—but first a brief note on the relationship to prohibited AI systems.

Regarding the top level of the pyramid, unacceptable risk AI systems are said to contravene the Union's values—for example through violating

---

37 *See* Eve Gaumond, *Artificial Intelligence Act: What Is The European Approach for AI?,* LAWFARE (June 4, 2021, 11:50 AM), https://www.lawfareblog.com/artificial-intelligence-act-what-european-approach-ai. It should also be noted that risk structures have been central to other legal areas for some time. *See e.g.*, European Parliament and Council Regulation 1907/2006, 2006 O.J. (L 136) 1; European Parliament and Council Regulation 2019/1381, 2019 O.J. (L 231) 1. Another example is the EU food sector. *See* European Parliament and Council Regulation 178/2002, 2002 O.J. (L 31) 1.

38 *See Regulatory Framework Proposal on Artificial Intelligence*, EUR. COMM'N (Sept. 29, 2022), https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. However, see the suggested Article 69 on the developing of codes of conduct for minimal risk AI systems. Norms for these systems may thus be created outside the legal requirements laid down in the regulation.

39 *Commission Proposal Laying Down Harmonised Rules on Artificial Intelligence*, *supra* note 4, at 5.2.4 (Explanatory Memorandum). It is in these settings that so-called deep fakes appear.

fundamental rights.[40] According to Article 5 of the proposed AI act, the prohibitions in the category include dark patterns, described as practices "that have a significant potential to manipulate persons through subliminal techniques beyond their consciousness" and that "exploit vulnerabilities of specific vulnerable groups such as children or persons with disabilities in order to distort their behavior in a manner that is likely to cause them or another person physical or psychological harm."[41] The use of real-time remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement is also prohibited (with certain exceptions), as is social scoring by public authorities for general purposes.

Although nothing is said in the Explanatory Memorandum of the Regulation about defining which fundamental rights that could be threatened by the above-mentioned AI practices, it is not difficult to see how they would threaten a number of provisions in any human rights instrument. In an EU context, the natural example is the EU Charter of Fundamental Rights, where the right to human dignity is protected in Article 1,[42] the right to integrity of the person in Article 3,[43] the right to respect for private and family life in Article 7,[44] the right to data protection in Article 8,[45] non-discrimination in Article 21,[46] and the rights of the child in Article 24.[47] On a societal level and in connection to AI in decision-making, the right to good administration may be mentioned (Article 41)[48] as well as the right to an effective remedy and a fair trial (Article 47).[49] Without this list being at all exhaustive, one can thus conclude that many—in one way or another perhaps most—of the Articles of the EU Charter can be related to AI. Although these rights, freedoms, and equalities must not be risked by AI systems, it is notable that limitations are possible in line with the general provisions of Article 52[50] of the EU Charter.

The majority of the articles in the proposed AI regulation, Articles 6–51, concern high-risk AI systems. Such systems do not directly contravene central EU values, but the Explanatory Memorandum states that they "create

---

40 *Id.* at 5.2.2 (Explanatory Memorandum).

41 *See id*. art. 5.

42 Charter of Fundamental Rights of the European Union, *supra* note 11, art. 1.

43 *Id.* art. 3.

44 *Id.* art. 7.

45 *Id.* art. 8.

46 *Id.* art. 21.

47 *Id.* art. 24.

48 *Id.* art. 41.

49 *Id.* art. 47.

50 *Id.* at 406–07.

a high risk to the health and safety or fundamental rights of natural persons."[51] Despite this starting point, the systems are to be permitted with certain restrictions. In the balancing act carried out by the EU legislature, potential threats to privacy, data protection, and other fundamental rights are weighed against the benefits of high-risk AI systems, and the result is expressed in the surrounding safety measures. As long as the suggested "life-cycle" monitoring of the systems is carried out, they may be used. High-risk systems will be subject to an ex-ante conformity assessment by notified bodies, mandatory safety measures, market supervision, and follow-up conformity assessments. Included in the requirements are the areas of data and data governance, documentation and registration, traceability, human oversight, robustness, and security.[52] A "CE marking" of conformity for AI systems, resembling the product safety marking in the EU, is to be developed (Article 49)[53] and will show that systems have been approved by a competent authority. The long-term EU vision is the creation of a database with approved high-risk AI systems (Article 60).[54]

The classification of an AI system as high-risk is obviously very important for every developer, importer, and user of AI technologies, as it will determine if a complex, potentially expensive and time-consuming process of risk assessment and conformity is required by law. The timeline of systems and products often stretches years ahead and, therefore, it is necessary to be as clear on this issue as possible—as soon as possible. According to the Explanatory Memorandum, the classification of an AI system as high-risk will depend on both existing product safety legislation and the purpose of the system.[55] In Article 6 of the suggested regulation, two main categories of high-risk AI systems are mentioned, namely: (1) systems that function as safety components of products that undergo third party ex-ante conformity assessments, such as machines, medical devices and "smart toys," and (2) systems with fundamental rights implications, listed in an annex to the suggested regulation, such as border control, law enforcement, public services, employment, and education (the annex may be updated along with technological advancements).[56]

In the following section, the supervisory regime of the AI proposal will be presented, as well as its connections to existing supervisory regimes.

---

51 *Commission Proposal Laying Down Harmonised Rules on Artificial Intelligence*, *supra* note 4, at 5.2.3 (Explanatory Memorandum).

52 *Id.* (describing the different steps and mandatory requirements).

53 *Id.* art. 49.

54 *Id.* art 60.

55 *Id.* at 5.2.3 (Explanatory Memorandum).

56 *Id*. art. 6.

V. SUPERVISION IN THE AI PROPOSAL – DEFINITIONS AND FUNCTIONS

As discussed above (section II), the supervisory regime in the AI proposal builds on and expands the regime set out in European data protection law and the GDPR, with many references to national data protection authorities, the European Board of Data Protection (EDPB), and the European Data Protection Supervisor (EDPS). The proposal foresees that the supervision can be conducted by existing sectorial authorities, who would also be entrusted with the powers to monitor and enforce the provisions of the regulation.[57] The AI proposal includes several different definitions of the national authorities involved (notifying authority, market surveillance authority, law enforcement authority, national supervisory authority, and national competent authority). It is for the member state to decide, in accordance with the principle of institutional autonomy, how the functions are to be distributed amongst national authorities. If more than one authority is appointed, one of them should be designated as the national supervisory authority.[58] At the EU level, the EDPS will act as the competent authority for the supervision of the EU institutions and bodies.[59] An addition to the current institutional structure is the European Artificial Intelligence Board (EAIB) which will be established at the EU level.[60] The relationship between the AI regulation, the GDPR, and other forms of existing supervision might thus be seen as chronological, whereas the AI proposal is adding an AI dimension to the already existing supervisory regimes.

The AI proposal introduces a three-level supervisory infrastructure for high-risk AI systems: human oversight (Article 14), a supervisory authority on the national level (Article 59), and the EAIB at the EU level. The first level, the "human oversight" mechanism, is to be applied within each high-risk AI practice. The function of human oversight means that the AI system is to be designed in such a manner that it may be effectively overseen by natural persons during the period in which the systems are in use.[61] The providers are to construct the system so that a natural person who is assigned the task of overseeing the product may, amongst others, "fully understand the capacities and limitations of the high-risk AI system and be able to duly monitor its operation."[62] A partly parallel role in the GDPR could be the Data

57 *Id*. arts. 26, 40, 42–43.

58 *Id*. arts. 59.2.

59 *Id*. at 5.2.6 (Explanatory Memorandum).

60 *Id*. at 56–58.

61 *Id*. art. 14.1.

62 *Id.* art. 14.4.

Protection Officer, a role that has become vital for most actors handling personal data since the GDPR came into force.[63]

As in the GDPR, the competent authorities in the proposed Regulation will have the competence and obligation to monitor and investigate the compliance of the regulation. There are, however, important differences. First, the GDPR regulates the processing of personal data in any form but does not regulate products as such. The GDPR accordingly does not contain any rules on ex-ante product control, equivalent to the AI proposal on notified bodies and conformity assessments.[64] Secondly, the ex-post evaluation in the AI proposal is to be carried out by already existing sector-specific market surveillance authorities, under EU Market Surveillance Regulation, the Capital Requirements Directive for the financial market, and data protection directive for Police and Criminal Justice Authorities.[65] As noted above, this adds up to a very large number of public authorities, not least since each member state usually has several Market Surveillance Authorities appointed for different sectors of the market (toys, food, chemicals, to name just a few). These authorities may use the powers bestowed on them under the respective sector specific law to also monitor high-risk AI systems. There are, however, also some specific procedures set out in the AI proposal. For example, a Market Surveillance Authority may place requirements on an AI system provider even if the relevant AI system is in compliance with the rules of the proposal if the system can be deemed to present risks to the health and safety of persons, the compliance of fundamental rights laws, or other aspects of public interest protection.[66]

An important similarity with the GDPR is that the proposed AI Regulation also contains specific rules on penalties and administrative fines.[67] Just like in the GDPR, these fines are to be decided according to either a fixed maximum amount or a percentage of the annual turnover (if the offender is a company). The figures of 2% and 4% are familiar from the GDPR's Article 83 on administrative fines, as are the fixed amounts of 10,000,000 and 20,000,000 euros. However, in the proposed AI regulation a third level as high as 6% or 30,000,000 euros is introduced for the most serious breaches (for example, the use of prohibited AI systems with unacceptable risks). This is an interesting development that shows firstly that AI systems are generally regarded as riskier than the handling of personal

63 GDPR, *supra* note 8, arts. 37–39.

64 *Commission Proposal Laying Down Harmonised Rules on Artificial Intelligence*, *supra* note 4, arts. 30–51.

65 *Id.* arts. 63.1, 63.4, 63.5.

66 *Id.* art. 67.1.

67 *Id.* art. 71.

data, and secondly that the feared administrative fines of the GDPR[68] are perhaps just the start of rising fines and sharper sanctions within EU regulatory frameworks. The AI proposal does not specify what category of public authority is to be entrusted with the competence to enact these decisions, but merely refers to national law to decide.

Another similarity with the GDPR, as well as with the supervisory regime of the financial markets, is the function of the EDPB and the ESAs in the institutional structure. Although less elaborately regulated, the EAIB will be tasked with collecting and sharing expertise and best practices among member states, contributing to uniform administrative practices in the member states and issuing opinions, and preparing recommendations or written contributions on matters related to the implementation of this Regulation.[69] A fundamental difference in comparison with the European and national authorities under the GDPR is, however, weaker independent status of the public authorities involved in AI supervision. As mentioned above, the data protection authorities enjoy a constitutionally grounded independence, according to both the TFEU and the Charter. The independence of the Market Surveillance Authorities and the competent authorities under the Capital Requirements Directive IV is less marked, but member states must ensure that the national authorities are independent in performing their tasks.[70] The AI proposal merely states that the notified bodies conducting the pre-market assessment are to be independent, but no specific rules on the independence of the public authorities involved in the supervisory regime are added.

The AI proposal further differs from the GDPR through the extensive collection of information from the AI system providers. In order to ensure that the different actors within the supervisory regime are able to assess and monitor high-risk AI systems, the proposed regulation sets out several requirements for the system providers to share information, in both ex-ante and ex-post control. As mentioned above (section IV), AI providers are to take measures to ensure documentation, traceability, and transparency of the systems,[71] which also can be included in a public EU-wide database, to "enable competent authorities, users and other interested people to verify if the high-risk AI system complies with the requirements laid down in the

---

68 *See* Martin Brinnen & Daniel Westman, *What's Wrong with the GDPR? Description of the Challenges for Business and Some Proposals for Improvement*, SVENSKT NÄRINGSLIV [SWEDISH ENTER.] 1, 9 (2019).

69 *Commission Proposal Laying Down Harmonised Rules on Artificial Intelligence*, *supra* note 4, art. 58.

70 *See* Market Surveillance Regulation, *supra* note 8, art. 4.

71 *Commission Proposal Laying Down Harmonised Rules on Artificial Intelligence*, *supra* note 4, arts. 10–13, 15 (stating that high-risk AI systems must be "designed and developed in such a way that they achieve, in the light of their intended purpose, an appropriate level of accuracy, robustness and cybersecurity, and perform consistently in those respects throughout their lifecycle").

proposal and to exercise enhanced oversight over those AI systems posing high risks to fundamental rights."[72] The AI providers are under the duty to inform competent authorities if they become aware of risks arising from the system, as well as provide the competent authority with documentation and information upon request, including full access to the training, validation, and testing datasets used by the provider.[73] If there is a "serious incident or any malfunctioning of those systems which constitutes a breach of obligations under Union law intended to protect fundamental rights," the AI providers must report this to the supervisory authorities immediately, or at the latest after fifteen days.[74]

VI. THE AI SUPERVISORY REGIME AS A BLACK BOX?

As discussed above (sections IV and V), the proposed AI regulation establishes a regulatory framework where high-risk AI systems are to be monitored via a human oversight-mechanism as well as a network of European and national authorities from different policy sectors. Many different sectors of the market will be concerned, and many public authorities involved. The network of European and national public authorities will have access to large volumes of information on the AI systems, where some information will be included in a public database. In the preamble to the proposed regulation, it is further noted that other public authorities should also have access to any information collected under the Regulation—namely, national public authorities or bodies supervising the application of Union law protecting fundamental rights, including equality bodies.[75] On the other hand, all public authorities involved in the application of the AI proposal should respect the confidentiality of information and data obtained in carrying out their tasks.[76] To the extent that the information includes information that is sensitive on the part of the AI providers, this seems justified. Exactly how the information is to be collected and stored, and who will have access, is not entirely clear. The overall impression remains, that the very extensive network of public authorities may gain access to an unprecedented amount of information on the development of new technologies. It would have been reassuring if the AI proposal also included clearer rules on the transparency of the work of the networked public authorities, not least for reasons of accountability and the need for supervision of the supervisors, which will be discussed below.

---

72 *Id.* at 5.1 (Explanatory Memorandum).

73 *Id.* arts. 22–23, 64.

74 *Id.* art. 62.1.

75 *Id.* at recital 79 (Preamble).

76 *Id.* at recital 83 (Preamble), art. 70.

As seen above, the mandate of the public authorities involved in supervision is based on sector specific EU acts in the areas of market surveillance and data protection, while the AI proposal adds an AI dimension to the supervision, providing further monitoring and enforcement tools as well as penalties for breaches of the proposed regulation. This means that the prerequisites for the supervision will vary between sectors. As seen above, the EAIB will be tasked with contributing to uniform administrative practices and issuing opinions, recommendations, or written contributions on matters related to the implementation of this Regulation.[77] If the role of the EAIB will develop into something similar to the EDPB and the ESAs on this matter, the role can be described as proactive, where efficiency and uniformity in the supervisory functions are prioritized matters.[78] On the other hand, there is an apparent lack of a coherent administrative procedural regime to ensure good administration as in foreseeable, impartial and prudent handling of the supervisory matters, and ensuring the AI providers a right to be heard, to access files, and to reasoned decisions.[79] There is no comprehensive administrative procedural act at the EU level, and the relevant secondary law, the GDPR, the Market Surveillance Regulation, and the Capital Requirements Directive IV have included administrative procedural rules in very different ways. Article 18 of the Market Surveillance Regulation contains basic rules for the administrative procedures, which the GDPR to a large degree lacks and the financial markets rules only have to a limited extent.[80]

All in all, the supervisory regime set up in the AI proposal can be described as very broad when it comes to the number of public authorities involved in the supervision and the amount of information collected from AI providers concerned. The functions, mandates, and procedural limitations of the public authorities involved are regulated in several different acts in an incoherent manner. At the same time, the assessments of the risks of AI services may result in unprecedented high administrative fines. Which AI providers that will be targeted will in the end depend on how the different categories in the risk-based approach are defined, more concretely. The

---

77 *Id.* art. 58.

78 *See* Pawel Hajduk, *The Powers of the Supervisory Body in the GDPR as a Basis for Shaping the Practices of Personal Data Processing*, 45 REV. EUR. & COMPAR. L. 57, 64 (2021); Jane Reichel, *Ensuring the Principle of Good Administration in EU Financial Markets Law*, *in* LEGAL ACCOUNTABILITY IN EU MARKETS FOR FINANCIAL INSTRUMENTS: THE DUAL ROLE OF INVESTMENT FIRMS 127, 135 *et seq.* (Carl Fredrik Bergström & Magnus Strand eds., Oxford Univ. Press 2021).

79 *See* Charter of Fundamental Rights of the European Union, *supra* note 11, art. 41.

80 Market Surveillance Regulation, *supra* note 8, art. 18 (containing short but comparatively comprehensive rules on administrative procedures under the heading "procedural rights of economic operators," which the GDRP to a large degree lacks); *see also* Chamberlain & Reichel, *supra* note 18, at 690. The Capital Requirements Directive IV gives the right to reasoned decision in several matters.

future risks of technological developments are by nature indeterminate, and they are not easily assessed even in the present.[81] As seen in section V, a Market Surveillance Authority may place requirements on an AI system provider that actually is in compliance with the rules of the proposal, if the system can be deemed to present risks to the health and safety of persons, to compliance with fundamental rights laws, or to other aspects of public interest protection. The foreseeability for AI providers must be described as low.

VII. CONCLUSIONS: WHO SUPERVISES THE SUPERVISORS?

There is no doubt that the development of AI technology has impacted on society and prompted legislators and policymakers at national and international levels to take action. The Council of Europe set up an ad hoc committee on artificial intelligence, CAHAI, in 2019, who stated the following in a report:

> AI, as a general-purpose technology, has an impact on the entire fabric of society[.] In 2017, the European Economic and Social Committee, in what is widely considered the 'inception report' on the broader societal impact of AI, identified the most important societal impact domains including: safety; ethics; laws and regulation; democracy; transparency; privacy; work; education and (in)equality. This means that AI has an impact on our human rights, democracy and the rule of law, the core elements upon which our European societies are built.[82]

The conclusion drawn so far is thus that the proposed AI Regulation seeks to establish a broad and incoherently regulated supervisory regime, with far reaching competences to take severe measures against AI providers in a rather opaque manner. If the AI services are putting the society at risk, this may be warranted. On the other hand, an unproportionally restrictive and unforeseeable supervisory regime may also create risks for the societies and for democracy and the rule of law. In the end, such a regime cannot be expected to legitimately balance the interests of privacy, data protection, and the right to information.[83]

---

81 Stanley Greenstein, *Preserving the Rule of Law in the Era of Artificial Intelligence (AI)*, 30 A.I. & L. 291, 297 (2021).

82 CATELIJNE MULLER, AD HOC COMMITTEE ON ARTIFICIAL INTELLIGENCE REPORT: THE IMPACT OF ARTIFICIAL INTELLIGENCE ON HUMAN RIGHTS, DEMOCRACY AND THE RULE OF LAW (2020).

(CAHAI has now been succeeded by the Committee on Artificial Intelligence (CAI)).

83 *See also* Ida Varošanec, *On the Path to the Future: Mapping the Notion of Transparency in the EU Regulatory Framework for AI*, 36 INT'L REV. L. COMPUTS. & TECH. 95, 95 (2022).

How can this development be explained? The popularity of supervisory authorities within the EU can be explained by the flexibility of the administrative procedure, the possibility to pool relevant legal, technical, and economic expertise within an authority at the national and European level and accessibility of close cooperation with other authorities within networks set up in EU law. These are indeed convincing arguments, and the introduction of supervisory regimes in connection to AI regulations are common. Caradaică has held that eleven member states, just over half of those who have published a strategy on AI until April 2020, want to develop a monitoring instrument for supervising the Al implementation and the social changes that occur.[84] As seen, the administrative supervisory infrastructure has also been identified as a part of the success of EU regulatory regime on data protection at the global level.[85]

With the growing importance of supervisory authorities within the EU, the authorities have achieved a complementary role to the role traditionally held by national and European courts within the EU. Since the seminal cases *Les Verts*, *Johnston*, and *Heylens* from the mid-1980's, national courts have played a pivotal role in the EU constitutional infrastructure for achieving an effective and uniform application of EU law.[86] "The vigilance of individuals concerned to protect their rights," as the Court of Justice of the European Union, CJEU, put it in the *Van Gend en Loos* case, has been relied upon to effectively channel questions on the interpretation of EU law to court.[87] With the instrument of preliminary rulings, the EU Treaties have created a line of communication between courts at the national and European level, thereby avoiding the traditional public international law trap of implementation relying solely on the will of the political sphere.[88] The right to access an independent court remains a cornerstone of the EU interpretation of the rule of law, as shown for instance by the intense political and judicial dialogue between the Commission and CJEU on the one side and the Polish government and Polish Constitutional Court on the other.[89]

---

84 Mihail Caradaică, *Artificial Intelligence and Inequality in European Union*, 14 EUROPOLITY 5, 25 (2020); *see also* EUROPEAN LAW INSTITUTE, MODEL RULES ON IMPACT ASSESSMENT OF ALGORITHMIC DECISION-MAKING SYSTEMS USED BY PUBLIC ADMINISTRATION (2022) (includes a suggestion for a supervisory regime).

85 BRADFORD, *supra* note 10.

86 Case 222/84, Johnston v. Chief Constable of the Royal Ulster Constabulary, 1986 E.C.R. 1663; Case 222/86, Unectef v. Heylens, 1987 E.C.R. 4112; Case 294/83, Les Verts v. Parliament, 1986 E.C.R. 1357.

87 Case 26/62, Van Gend en Loos v. Nederlandse Administratie der Belastingen, 1963 E.C.R. 1.

88 TORBJÖRN ANDERSSON, RÄTTSSKYDDSPRINCIPEN 276 (1997); Daniel Keleman, *Adversial Legalism and Administrative Law in the European Union*, *in* COMPARATIVE ADMINISTRATIVE LAW 606, 615 (Susan Rose-Ackerman & Peter L. Lindseth eds., 2010).

89 *See* LAURENT PECH & DIMITRY KOCHENOV, RESPECT FOR THE RULE OF LAW IN THE CASE LAW OF THE EUROPEAN COURT OF JUSTICE (Swed. Inst. Eur. Pol'y Stud. 2021).

Compared to courts, the role of authorities is however fundamentally different. Supervisory authorities within the EU composite administration often have a role in developing both binding and non-binding rules, enforcement practices, routines for information sharing, and more. However, the public authorities remain within the executive branch, having as their task to implement rules within a specific policy area. They lack the procedural structures of courts, instead they often have wide discretionary powers in decision-making, assessing highly complex economical and technical matters. Even though the legal acts of authorities at both the national and EU level are reviewable by courts, the multifaceted activities of supervisory authorities are not easily controlled by courts alone, and other accountability mechanisms for holding the authorities within the EU composite accountable remain undeveloped.[90] Also, supervisors need to be supervised. As held by Rowe, the legal and institutional supervision of administrative action is mandated by at least the principles of rule of law and of good administration.[91] It seems the time has come to ask the question: is the EU putting too much trust in supervisory authorities?

90 Niamh Moloney, *The European Supervisory Authorities and Discretion: Can the Functional and Constitutional Circles be Squared?*, *in* EU EXECUTIVE DISCRETION AND THE LIMITS OF LAW 85, 108–117 (Joan Mendes ed., Oxford Univ. Press 2019); YANNIS PAPADOPOULOS, POLITICAL ACCOUNTABILITY IN EU MULTI-LEVEL GOVERNANCE 90–115 (Swed. Inst. Eur. Pol'y Stud. 2021).

91 Gerard C. Rowe, *Controlling Administrative Action: Internal Administrative Supervision in the European Union*, 61 ADMIN. L. REV. 223, 224 (2009) (discussing the role of supervision of administrative action).