5

Legal Safeguards in the EU Legal Order

In Chapter 4, I analysed how algorithmic regulation (discussed in Chapter 2) affects the rule of law and its principles (discussed in Chapter 3), and identified a threat which I conceptualised as *algorithmic rule by law*, marking a deviation of the rule of law's ideal, facilitated by the use of algorithmic systems. In light of that analysis, let me now consider how the EU legal framework deals with this threat, and what safeguards it offers to counter it.

Two legal domains are of particular relevance in this regard: regulation pertaining to the protection of the rule of law (*the EU's rule of law agenda*), and regulation pertaining to (automated) personal data processing and the use of algorithmic systems (*the EU's digital agenda*). Each of these domains is vast and consists of a broad range of legislation, including not only primary and secondary EU law, but also soft law. In what follows, I therefore confine my investigation to those areas of legislation that are most relevant for the identified concerns, with a primary focus on binding legislation. In terms of safeguards, drawing on the conclusions of Chapter 4, I will be evaluating EU legislation based on whether it provides effective mechanisms enabling prior and continuous oversight and accountability over algorithmic regulation, also as regards the upstream choices; public participation mechanisms; private and public enforcement, at national and EU level; constitutional checks and balances; and the availability of contestability, as well as opportunities for internal critical reflection.

After some preliminary remarks about the EU's competence to take legal action in this field (Section 5.1), I respectively examine safeguards provided by regulation pertaining to the rule of law (Section 5.2), to personal data (Section 5.3) and to algorithmic systems (Section 5.4), before concluding (Section 5.5).

5.1 A NOTE ON EU COMPETENCES IN THE FIELD

Pursuant to the principle of conferral, the European Union can only act based on competences explicitly conferred to it.[1] Conversely, "*competences not conferred upon the Union in the Treaties remain with the Member States*".[2] Accordingly, whenever the EU seeks to undertake legal action, whether in the form of proposing the harmonisation of national legislation, or in the form of challenging a Member State's action in court, it needs to be able to rely on a legal basis to do so.[3] For each action at the EU level, whether preventative or mitigative in nature, one must hence first identify a legal basis that enables its execution.[4]

In addition, EU action is also constrained by the principles of subsidiarity and proportionality. Pursuant to the former, whenever the EU seeks to act in an area that does not fall under its exclusive competence, "*the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level.*"[5] Pursuant to the latter, "*the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties*".[6] Collectively, the constraints posed by the principle of conferral, subsidiarity and proportionality can be considered as giving expression to the principle of legality at the level of the EU, underpinned by the fact that the EU legal order is based on the rule of law, and that the actions of EU institutions likewise need to adhere to its principles.[7]

This demarcation of competences is particularly relevant in an area that deals so intricately with a matter laying close to Member States' national identity (protected by Article 4(2) TEU[8]), namely the way in which national public authorities exercise their power and take administrative actions vis-à-vis their citizens. Accordingly, "*striking a balance between taking the effective action necessary to defend the Rule*

[1] See Article 5(2) TEU, stating that "*under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States*".

[2] See Article 4(1) TEU.

[3] Koen Lenaerts, Piet Van Nuffel and Tim Corthaut, *EU Constitutional Law* (Oxford University Press 2021) 84.

[4] See also Annegret Engel, *The Choice of Legal Basis for Acts of the European Union: Competence Overlaps, Institutional Preferences, and Legal Basis Litigation* (Springer International Publishing 2018).

[5] See Article 5(3) TEU.

[6] See Article 5(4) TEU.

[7] See Koen Lenaerts, Ignace Maselis and Kathleen Gutman, *EU Procedural Law* (Janek Tomasz Nowak ed, Oxford University Press 2015) 2. See also Theodore Konstadinides, *The Rule of Law in the European Union: The Internal Dimension* (Bloomsbury 2017).

[8] Article 4(2) TEU states that the Union must respect Member States' national identities, "*inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government*".

of Law and respecting the limitations placed on the EU's competences is tricky".[9] At the same time, Article 4(3) TEU also enshrines the principle of sincere cooperation, demanding that the Union and the Member States shall, in full mutual respect, assist each other in carrying out tasks which flow from the Treaties. Furthermore, it also establishes the obligation for Member States to "*take any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union.*"[10] Member States can hence not invoke 'national identity' as an excuse to escape their obligations under EU law.[11]

This raises the question of how much 'diversity' EU Member States can maintain as regards the exercise of public power by national authorities, without overly endangering 'unity' in their respect for values that are considered to be common to all.[12] The answer to this question is highly complex, and not one that I will tempt to discuss in this book. Instead, I will formulate a different question, focusing on which EU obligations currently exist that relate to Member States' need to respect the rule of law, and that can provide protection against the risks posed by algorithmic regulation. After all, "*while the EU owes respect to its Member States' right to organize their government, the latter must observe the rule of law as it is understood in the EU legal order*".[13]

5.2 REGULATION PERTAINING TO THE RULE OF LAW

The EU legal framework counts several mechanisms that are aimed at ensuring Member States' compliance with the rule of (EU) law. In what follows, I respectively analyse the protection afforded by Article 2 TEU in combination with the procedure of Article 7 TEU (Section 5.2.1), the Conditionality Regulation (Section 5.2.2), and the role played by infringement procedures and challenges before national courts – including through the preliminary reference procedure (Section 5.2.3).

[9] Kim Lane Scheppele, Dimitry Vladimirovich Kochenov and Barbara Grabowska-Moroz, 'EU Values Are Law, After All: Enforcing EU Values through Systemic Infringement Actions by the European Commission and the Member States of the European Union' (2020) 39 Yearbook of European Law 3, 8.

[10] Article 4(3), §2.

[11] Luigi Corrias, 'National Identity and European Integration: The Unbearable Lightness of Legal Tradition' (2016) 1 European Papers – A Journal on Law and Integration 383.

[12] Note that 'United in Diversity' is also the EU's motto, which started being used from 2000 onwards. See also Jean-Marc Favret, 'L'union européenne: "L'unité dans la diversité". Signification et pertinence d'une devise' (2003) 39 Revue trimestrielle de droit européen 657.

[13] Pekka Pohjankoski, 'Rule of Law with Leverage: Policing Structural Obligations in EU Law with the Infringement Procedure, Fines and Set-Off' (2021) 58 Common Market Law Review 1341.

5.2.1 *Article 2 and 7 TEU*

The rule of law is listed in Article 2 TEU as one of the foundational values of the EU, common to all Member States. It needs to be respected by states who aspire EU membership,[14] and it needs to be respected throughout a state's EU membership.[15] At the same time, the Treaty does not detail what, precisely, it means by 'to respect the value of the rule of law'. The drafters of the Treaty explained their selection for the values to be listed in Article 2 TEU based on the fact that these values "*have a clear non-controversial legal basis so that the Member States can discern the obligations resulting therefrom which are subject to sanction*".[16] Given that I had to develop an analytical framework in Chapter 3 to concretise, based on an extensive examination of legal sources, the rule of law requirements that Member States must meet when exercising public power, I would beg to differ.[17]

Be that as it may, Article 7 TEU provides a mechanism of protection in case the values listed in Article 2 TEU are threatened or infringed by a Member State. Although Article 7 TEU hence protects multiple values, it is typically referred to as the rule of law protection mechanism, since it not only protects the rule of law as one value amongst others, but it also consists of a legal provision that literally embodies the protective role of the law in a liberal democratic system. Article 7(1) TEU enables the Council, acting by a majority of four fifths of its members, to determine that there is a "*clear risk of a serious breach by a Member State of the values referred to in Article 2*". This determination must be based on a reasoned proposal by one third of the Member States, by the European Parliament or by the European Commission, and it can only be taken after the European Parliament consented. The mechanism of Article 7(1) TEU requires only the clear *risk* of a serious breach,[18] and hence serves as a warning mechanism.[19] In that case, the Council will hear the Member State in question and can address recommendations to it.[20] While I will not elaborate on this point here, it is worth highlighting that the analysis of Chapter 4 did indicate that the increasingly widespread use of algorithmic regulation, without the adoption of appropriate protection mechanisms to counter its risks, can entail a clear risk of a serious breach of the rule of law.

[14] See Article 49 TEU, stating that "*any European State which respects the values referred to in Article 2 and is committed to promoting them may apply to become a member of the Union.*"

[15] Gabriel N Toggenburg and Jonas Grimheden, 'Managing the Rule of Law in a Heterogeneous Context: A Fundamental Rights Perspective on Ways Forward' in Werner Schroeder (ed), *Strengthening the Rule of Law in Europe: From a Common Concept to Mechanisms of Implementation* (Hart Publishing 2016) 225.

[16] Praesidium, 'Draft of Articles 1 to 16 of the Constitutional Treaty' (The European Convention Secretariat 2003) CONV 528/03 11.

[17] See also the doubts raised in this regard by Toggenburg and Grimheden (n 15) 222.

[18] For a discussion of the meaning of this threshold, see *supra*, Section 4.2.5.

[19] See also Scheppele, Kochenov and Grabowska-Moroz (n 9) 8.

[20] Article 7(1) TEU.

Article 7(2) TEU goes a step further, as it enables the determination of the 'existence' of a 'serious and persistent' breach by a Member State of the values referred to in Article 2. In this case, however, the determination can only be made through a *unanimous* decision of the European Council, based on a proposal by one third of the Member States or by the Commission and after obtaining the consent of the European Parliament.[21] This is because the stakes of this determination are higher. Once a decision has been taken, Article 7(3) TEU enables the Council, acting by a qualified majority, to decide to suspend certain rights deriving from the application of the Treaties to the Member State in question, including voting rights in the Council. Before the determination of a 'clear risk' of a serious breach, or of the 'existence of a serious and persistent breach' of EU values, the Member State concerned always has the right to be heard and to submit its observations.

Thus far, the European Commission[22] and the European Parliament sought to trigger Article 7(1) against both Poland and Hungary,[23] and the Council has organised several hearings to hear the countries' positions. However, despite the calls by scholars, civil society organisations and even EU institutions to take further action,[24] and despite the fact that the concerns remain unaddressed (especially in Hungary),[25] the Council has come to the determination of neither a 'clear risk' nor the 'existence of a serious and persistent breach' of the rule of law. In addition, the Council's unwillingness to ensure that the Commission's recommendations to ameliorate the

[21] Article 7(2) TEU.

[22] In 2017, the European Commission triggered Article 7(1) for the first time in light of the clear risk of a serious breach of the rule of law by Poland. See European Commission, Reasoned proposal in accordance with Article 7(1) of the Treaty on European Union regarding the rule of law in Poland. Proposal for a Council decision on the determination of a clear risk of a serious breach by the Republic of Poland of the rule of law, COM(2017) 835 final, 20 December 2017.

[23] In 2018, the European Parliament adopted a resolution to determine the clear risk of a serious breach of the rule of law as regards Hungary. See 'European Parliament resolution of 12 September 2018 on a proposal calling on the Council to determine, pursuant to Article 7 (1) of the Treaty on European Union, the existence of a clear risk of a serious breach by Hungary of the values on which the Union is founded (2017/2131(INL)', 2018.

[24] R Daniel Kelemen and Kim Lane Scheppele, 'How to Stop Funding Autocracy in the EU' (*Verfassungsblog*, 10 September 2018) <https://verfassungsblog.de/how-to-stop-funding-autocracy-in-the-eu/>; Laurent Pech, 'The Rule of Law as a Well-Established and Well-Defined Principle of EU Law' (2022) 14 Hague Journal on the Rule of Law 107. See also Kerstin McCourt, 'European Commission Lacks Tenacity on the Rule of Law' (*Human Rights Watch*, 20 July 2022) <www.hrw.org/news/2022/07/20/european-commission-lacks-tenacity-rule-law>.

[25] In its resolution of 18 January 2024 on the situation in Hungary, the European Parliament stressed that its rule of law concerns have not been alleviated, and that it is '*strongly concerned about the further erosion of democracy, as well as the deterioration of the rule of law and the fundamental rights situation in Hungary*'. It also '*regrets the failure of the Council to make meaningful progress in the ongoing Article 7(1) TEU procedures*' and '*calls on the European Council and the Member States to take action and to determine whether Hungary has committed serious and persistent breaches of EU values under Article 7(2) TEU*'. See European Parliament resolution of 18 January 2024 on the situation in Hungary and frozen EU funds (2024/2512 (RSP)), 2024.

situation are implemented has led to much frustration.[26] Given the role of the Council (consisting of representatives from the twenty-seven EU Member States), the procedure in question is primarily political in nature. Considering the extensiveness of the procedure's potential consequences and the sheer symbolically weighty nature of its invocation, it is only considered a measure of last resort. Moreover, as long as there is at least one other Member State who vetoes the determination of the existence of a 'serious and persistent breach', the procedure of Article 7(2) stands no chance given the requirement for unanimity.[27]

The inability of Article 7 TEU to counter the ongoing rule of law threats in some EU Member States and, in particular, the reluctance to deploy its mechanism has been subjected to heavy criticism. It also pinpoints the dilemma that the EU and its Member States are faced with, in between maintaining the cooperation and goodwill of the Member States on other fronts, and ensuring adherence to the rule of (EU) law without further alienating infringing states. Either way, by the time Article 7 TEU finally comes into play, if ever, a lot of damage will already have been done.

One problem, which is also relevant to the risks identified in the context of algorithmic regulation, is that the erosion of the rule of law often occurs incrementally rather than suddenly.[28] However, as previously noted, incremental changes will rarely trigger a sufficiently strong counter-reaction so as to lead to the adoption of a measure which is deemed as far-reaching as Article 7 TEU. This gives rise to a tragic observation: the mechanism designed to avoid systemic breaches of the rule of law is, precisely because of the systemic and incremental nature of those breaches, unable to carry out its proper function.

Setting the ineffectiveness of Article 7 TEU aside, the EU's increased attention for the (dis)respect of the rule of law in Member States (perhaps precisely due to this ineffectiveness) did give rise to a number of soft-law initiatives that monitor the rule of law situation across the Union.[29] Indeed, in recent years, the Commission's rule of law toolbox has expanded, and now encompasses several evidence-gathering and documentation mechanisms based on rule of law-indicators. Examples are the

[26] See also Laurent Pech and Jakub Jaraczewski, 'Systemic Threat to the Rule of Law in Poland: Updated and New Article 7(1) TEU Recommendations' (2023), UCD Working Papers in Law, Criminology & Socio-Legal Studies Research Paper No. 13, 9.

[27] Scheppele, Kochenov and Grabowska-Moroz (n 9) 8. See also 'Four European Organisations of Judges Sue EU Council for Disregarding EU Court's Judgments on Decision to Unblock Funds to Poland' (AEAJ 28 August 2022) <www.rechtersvoorrechters.nl/uploads/2022/08/PRESS-RELEASE-EN-2022-08-28.pdf>.

[28] See also Kim Lane Scheppele, 'Autocratic Legalism' [2018] The University of Chicago Law Review 545; Aziz Huq and Tom Ginsburg, 'How to Lose a Constitutional Democracy' (2018) 65 UCLA Law Review 78.

[29] See European Commission, 'Communication from the Commission to the European Parliament, the European Council and the Council: Further Strengthening the Rule of Law within the Union – State of Play and Possible next Steps' (Brussels, 3 April 2019) COM/2019/163 final.

'European Semester',[30] the 'EU Justice Scoreboard',[31] and the annual 'Rule of Law Reports'[32] that essentially institutionalise a dialogue between the Commission and Member States. These mechanisms also provide useful information that could support the triggering of Article 7 TEU, the Conditionality Regulation or infringement actions, which I discuss in the following sections.[33] While non-binding, and not providing any guarantee that they will contribute to a successful triggering of the Article 7 TEU procedure, unlike the former, these initiatives are able to play a

[30] Introduced in 2011, the European Semester is the framework for integrated surveillance and coordination of economic and employment policies across the European Union. While it was initially mainly an economic exercise, it now also integrates other policy fields. It is not explicitly aimed at protecting 'the rule of law', yet its monitoring activities also cover areas that are relevant for the rule of law, including the European Justice Scoreboard. See also Amy Verdun and Jonathan Zeitlin, 'Introduction: The European Semester as a New Architecture of EU Socioeconomic Governance in Theory and Practice' (2018) 25 Journal of European Public Policy 137.

[31] The European Justice Scoreboard presents an annual overview of indicators on the efficiency, quality and independence of justice systems, and is meant to assist EU Member States in improving the effectiveness of their national justice systems through comparable data. Its findings feed into the annual rule of law reports. See also András Jakab and Lando Kirchmair, 'How to Develop the EU Justice Scoreboard into a Rule of Law Index: Using an Existing Tool in the EU Rule of Law Crisis in a More Efficient Way' (2021) 22 German Law Journal 936.

[32] The annual rule of law reporting mechanism was launched by the Commission in 2020, as part of its initiative to strengthen its rule of law toolbox. It is essentially a monitoring tool, meant to maintain a yearly dialogue with Member States as regards several areas that are of relevance to the rule of law, resulting in a report with data and conclusions on the state of the rule of law in each EU Member States (though no detailed recommendations or legal conclusions are made). Based on the Commission's rule of law methodology, these areas are: (1) justice systems; (2) the anti-corruption framework; (3) media pluralism; and (4) other institutional issues related to checks and balances. The Commission draws on data from Member States, case law, EU bodies, but also from the Council of Europe and other international organisations. See European Commission, 'European Rule of Law Mechanism: Methodology for the Preparation of the Annual Rule of Law Report' (2020) <https://commission.europa.eu/system/files/2020-09/2020_rule_of_law_report_methodology_en.pdf>.

[33] Recital 16 of the Conditionality Regulation, for instance, provides that, when the Commission seeks to identify potential breaches of the rule of law by Member States for the purpose of the triggering the regulation's mechanism,

> that assessment should be objective, impartial and fair, and should take into account relevant information from available sources and recognised institutions, including judgments of the Court of Justice of the European Union, reports of the Court of Auditors, the Commission's annual Rule of Law Report and EU Justice Scoreboard, reports of the European Anti-Fraud Office (OLAF) and the European Public Prosecutor's Office (EPPO) as relevant, and conclusions and recommendations of relevant international organisations and networks, including Council of Europe bodies such as the Council of Europe Group of States against Corruption (GRECO) and the Venice Commission, in particular its rule-of-law checklist, and the European networks of supreme courts and councils for the judiciary. The Commission could consult the European Union Agency for Fundamental Rights and the Venice Commission if necessary for the purpose of preparing a thorough qualitative assessment.

preventative role rather than a mere reactive one.[34] Furthermore, they enable the dissemination of information about the status of the rule of law in every EU Member State to the public at large, thereby contributing to transparency and potentially accountability at the national level too.

Regrettably, however, none of these initiatives currently have indicators about the potentially adverse impact of algorithmic regulation on the rule of law, or on the checks and balances that have been implemented to counter such impact. Quite to the contrary, if discussed at all, 'digitalisation' is presented as a desirable feature that Member States should ideally swiftly implement in light of the 'efficiencies' it can enable.[35] The risks attached to it, particularly in the area of public administration, are left unspoken and unmonitored, despite their *systemic* nature and potential contribution to the *systemic* breaches of the rule of law. In other words, the effects of algorithmic regulation on the rule of law remains a blind spot. As it currently stands, neither Article 7 TEU nor the soft-law mechanisms aimed at monitoring the rule of law situation seem to offer safeguards against the threat conceptualised under Chapter 4.

5.2.2 *The Conditionality Regulation*

Besides soft-law initiatives, the European Union also sought to expand its rule of law toolbox with binding mechanisms. The adoption of the Conditionality Regulation, or Regulation 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget, can be seen as a highlight in this regard.[36] In addition to its legal relevance, I already noted in Chapter 3 that the Conditionality Regulation also has significant definitional relevance, as it provides "*the first comprehensive all-encompassing internal-oriented definition of the rule of law adopted by the EU co-legislators*".[37] While the European Commission had already proposed a conceptualisation of the rule of law and its six principles in 2019,[38] by means of the Conditionality Regulation, this conceptualisation was also formally adopted by the

[34] See also Toggenburg and Grimheden (n 15) 225.

[35] While the references to digitalisation are sporadic, the 2022 rule of law report, for instance, recommends several Member States to continue their digitalisation efforts (with particular focus on the justice system). See European Commission, 'The Rule of Law Situation in the European Union. 2022 Rule of Law Report.' (2022) COM(2022) 500 final <https://ec.europa.eu/info/sites/default/files/1_1_194062_communication_rol_en.pdf>.

[36] See, e.g., Antonia Baraggia and Matteo Bonelli, 'Linking Money to Values: The New Rule of Law Conditionality Regulation and Its Constitutional Challenges' (2022) 23 German Law Journal 131, 132.

[37] Pech (n 24).

[38] See also *supra*, Section 3.2.4.

European Parliament and the Council and enshrined in a piece of secondary legislation.[39]

The Regulation foresees a mechanism to suspend the transmission of EU funds to 'rogue'[40] Member States – or, more diplomatically, it conditions the transmission of EU funds to compliance with the rule of law. Its primary aim is hence to protect the EU budget and ensure the sound financial management thereof by Member States, while at the same time incentivising rule of law compliance through financial means. In essence, the regulation seeks to prevent that EU funds are being used for authoritarian or rule of law-infringing ends.[41] Some scholars[42] noted that the European Union already had a similar mechanism at its disposal through Regulation 1303/2013, laying down common provisions regarding the governance of a number of EU funds, including the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development and the European Maritime and Fisheries Fund.[43] Article 142 of that Regulation foresees a procedure for the suspension of payments by the Commission if, inter alia, "*there is a serious deficiency in the effective functioning of the management and control system of the operational programme, which has put at risk the Union contribution to the operational programme and for which corrective measures have not been taken*".[44] Based on the idea that "*surely, a country without the rule of law cannot generate effective management and control systems*", Kelemen and Scheppele argue that this provision already enabled the suspension of EU funds to rule of law-infringing Member States, yet they "*note with disappointment that the Commission has not yet had the will to use the power already in its hands*".[45]

Despite the seeming pre-existence of similar remedies, the adoption of the Conditionality Regulation, as a general regime of conditionality, was not without difficulty or controversy.[46] As soon as it was adopted, both Hungary and Poland

[39] ibid.

[40] See Laurent Pech and Kim Lane Scheppele, 'Illiberalism Within: Rule of Law Backsliding in the EU' (2017) 19 Cambridge Yearbook of European Legal Studies 3.

[41] See also Renáta Uitz, 'Funding Illiberal Democracy: The Case for Credible Budgetary Conditionality in the EU', BRIDGE Network – Working Paper 7 [2020] SSRN Electronic Journal <https://ssrn.com/abstract=3722936>.

[42] Kelemen and Scheppele (n 24).

[43] See Regulation (EU) no. 1303/2013 of the European Parliament and of the Council of 17 December 2013 laying down common provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund, the European Agricultural Fund for Rural Development and the European Maritime and Fisheries Fund and laying down general provisions on the European Regional Development Fund, the European Social Fund, the Cohesion Fund and the European Maritime and Fisheries Fund and repealing Council Regulation (EC) no. 1083/2006 2013 (OJ L 347 20122013, p. 320). This Regulation has been amended multiple times since its adoption, the last time on 13 April 2022.

[44] See Article 142(1)(a) TFEU.

[45] Kelemen and Scheppele (n 24).

[46] Not only were negotiations between the Parliament and Council lengthy and challenging, but the Commission's initial proposal also received a negative opinion from the Council's Legal

challenged the validity of the regulation's legal basis before the Court.[47] They claimed that the EU did not have the legal competence to adopt a regulation that defines the rule of law or determines criteria to establish breaches thereof.[48] Moreover, they stated that the Regulation was not compatible with Article 7 TEU, which already, in their view, exhaustively, provides for a mechanism to protect the rule of law, thus precluding the EU to adopt another one.[49] As noted in Chapter 3, the EU does not have a 'general' legal competence to enforce the rule of law, and hence had to resort to a domain-specific legal basis. Given the link of the Regulation's suspension mechanism with the multi-annual financial framework (MFF), some have argued that the Regulation would need to be adopted under the MFF's legal basis, Article 312 TFEU, which requires adoption through unanimity in the Council.[50]

Instead, the Commission resorted to Article 322(1)(a) TFEU as the Regulation's legal basis, well aware that the unanimity requirement of Article 312 TFEU would prevent the Regulation to ever see the light of day, since Poland and Hungary would never agree to it. Article 322(1)(a) TFEU provides that the European Parliament and the Council, acting in accordance with the ordinary legislative procedure (i.e. without unanimity), can adopt regulations to set the financial rules determining "*the procedure to be adopted for establishing and implementing the budget and for presenting and auditing accounts*". Accordingly, the Conditionality Regulation can be seen as an example of the EU's use of legal competences in one particular field (e.g. the EU budget) to promote other aims in a more indirect way (e.g. the rule of

Service. See also Kim Lane Scheppele, Laurent Pech and R Daniel Kelemen, 'Never Missing an Opportunity to Miss an Opportunity: The Council Legal Service Opinion on the Commission's EU Budget-Related Rule of Law Mechanism' (*Verfassungsblog*, 12 November 2018) <https://verfassungsblog.de/never-missing-an-opportunity-to-miss-an-opportunity-the-council-legal-service-opinion-on-the-commissions-eu-budget-related-rule-of-law-mechanism/>.

[47] This legal challenge can be seen as part of the compromise in the European Council in December 2020, during which it was agreed that the implementation of the regulation would not be initiated before the CJEU could analyse its legality. See General Secretariat of the Council, 'European Council Meeting (10 and 11 December 2020) – Conclusions' (EUCO 2020). See also Baraggia and Bonelli (n 36) 132. Some scholars have argued that these Council conclusions were adopted *ultra vires* and constituted a violation of the principle of institutional balance by undermining the prerogatives of the Parliament, Council, Commission and Court of Justice. See, e.g., Alberto Alemanno and Marijn Chamon, 'To Save the Rule of Law You Must Apparently Break It' (*Verfassungsblog*, 11 December 2020) <https://verfassungsblog.de/to-save-the-rule-of-law-you-must-apparently-break-it/>.

[48] See Case C-157/21, *Republic of Poland v European Parliament and Council*, 16 February 2022, ECLI:EU:C:2022:98, §69.

[49] See ibid, §§87–88. Note that they also claimed that the Conditionality Regulation breaches the principle of legal certainty – i.e. a rule of law principle that the EU must respect, as part of its *horizontal* commitment to the rule of law – since it provides insufficient clarity as to how it would be applied to Member States. See ibid, §311.

[50] ibid, §83. See also Kelemen and Scheppele (n 24).

law), thereby overcoming the hurdles of potentially limited competences.[51] This approach, while not uncriticised, is not new. Various legislative initiatives which are based on Article 114 TFEU, aimed at advancing the harmonisation of the EU's internal market, also contribute (directly or indirectly) to the protection of fundamental rights, an area in which the EU's competences are also not generalised.[52]

In the past, the Court has already frequently been called upon to ensure that the EU does not overstep its competences by adopting an erroneous legal basis, and did not shy away from invalidating legislation where it deemed this to be the case.[53] However, in this case, the challenge raised by Poland and Hungary was unsuccessful, and the Court upheld the Regulation's validity. It found that the Regulation does not create a general rule of law protection mechanism, and only limits itself to those rule of law-infringements that are directly linked to the EU budget, hence remaining within the confines of Article 322 TFEU.[54] The Court also distinguished the Regulation's mechanism from the procedure in Article 7 TEU, which hence did not preclude its adoption.

With the Court's blessing, the Commission thus no longer faced an obstacle or excuse to launch the suspension mechanism.[55] In April 2022, it therefore announced the initiation of the procedure against Hungary[56] – the first step of a lengthy

[51] See also Baraggia and Bonelli (n 36) 134.

[52] For instance, before the enshrinement of Article 16 TFEU – granting the Union a specific legal basis to adopt regulation in the sphere of personal data processing, for instance the GDPR – the Union relied on Article 114 TFEU as the legal basis for its previous data protection directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)). See in this regard Case C-101/01, *Bodil Lindqvist*, 6 November 2003, ECLI:EU:C:2003:596. See also Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, vol 16 (Springer International Publishing 2014). Similarly, environmental protection legislation has likewise been relying on Article 114 TFEU before a more specific legal basis was adopted in the Treaties. See also David Langlet and Said Mahmoudi, *EU Environmental Law and Policy* (Oxford University Press 2016); Geert van Calster and Leonie Reins, *EU Environmental Law* (Edward Elgar Publishing 2017).

[53] See for instance Case C-376/98, *Germany v European Parliament and Council*, 5 October 2000, ECLI:EU:C:2000:544, where the Court annulled Directive 98/43/EC of the European Parliament and of the Council of 6 July 1998 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the advertising and sponsorship of tobacco products, pursuant to the fact that it was adopted based on an inappropriate legal basis. See also Stephen Weatherill, 'The Limits of Legislative Harmonization Ten Years after Tobacco Advertising: How the Court's Case Law Has Become a "Drafting Guide"' (2011) 12 German Law Journal 827.

[54] See Case C-157/21, *Republic of Poland v European Parliament and Council* (n 48), §130 and following.

[55] Note that this obstacle was primarily a *political* one, given the compromise solution reached by the European Council in its conclusions on 11 December 2020. See General Secretariat of the Council (n 47). See also Alemanno and Chamon (n 47).

[56] See Vlad Makszimov, 'Hungary: Commission Officially Launches Procedure Linking Bloc Funds to Rule of Law' *Euractiv* (27 April 2022) <www.euractiv.com/section/politics/news/

procedure.[57] Indeed, before the suspension mechanism could actually be implemented, the procedure set out by the Regulation had to be followed, including a written notification to the Member State concerned, setting out the factual elements and specific grounds on which the findings are based; the Member State's response and potential proposal of remedial measures; the Commission's notification of its intention to propose an implementing decision in case it considers the remedial measures to be insufficient; yet another opportunity for the Member State to share its observations, particularly regarding the proportionality of the Commission's envisaged measure; and, finally, an implementing decision by the Council acting by qualified majority, based on the Commission's proposal.[58] In March 2022, the Commission also adopted guidelines in which it set out how it will apply the regulation in more detail.[59]

Importantly, the suspension mechanism can only be invoked with regards to a limited set of rule of law-infringements that have a link with the EU budget, hence not providing a general suspension clause for all rule of law-infringements. After all, its purpose and its legal basis concern the protection of the EU budget rather than the rule of law in general. Article 3 of the Regulation sets out which Member State actions may be 'indicative' of breaches of principles of the rule of law for the purpose of the regulation, namely:

(a) endangering the independence of the judiciary;
(b) failing to prevent, correct or sanction arbitrary or unlawful decisions by public authorities, including by law-enforcement authorities, withholding financial and human resources affecting their proper functioning or failing to ensure the absence of conflicts of interest;
(c) limiting the availability and effectiveness of legal remedies, including through restrictive procedural rules and lack of implementation of judgments, or limiting the effective investigation, prosecution or sanctioning of breaches of law.

hungary-commission-officially-launches-procedure-linking-bloc-funds-to-rule-of-law/>. See also Nathalie Smuha, 'Een doosje vijgen na Pasen voor Viktor Orban' *De Standaard* (8 April 2022) <www.standaard.be/cnt/dmf20220407_97729796>.

[57] The European Commission decided to postpone the initiation of the Conditionality Regulation's procedure against Hungary until the Court's judgment came out. However, on 20 October 2021, the European Parliament, fed up with the Commission's delay, submitted an action in court against the Commission for failure to act under Article 265 TFEU. On 18 May 2022 – after the Commission had announced the launch of the Regulation's suspension mechanism – the European Parliament informed the Court that it wished to discontinue its action, after which the President of the Court removed the case from the register. See Order of the President of the Court in Case C-657/21, *European Parliament v European Commission*, 8 June 2022.

[58] See Article 6 of the Conditionality Regulation.

[59] European Commission, 'Communication from the European Commission: Guidelines on the Application of the Regulation (EU, EURATOM) 2020/2092 on a General Regime of Conditionality for the Protection of the Union Budget' (2022) C(2022) 1382 final.

In addition to these 'general' indications, Article 4 sets out that action can be undertaken where it is established that "*breaches of the principles of the rule of law in a Member State affect or seriously risk affecting the sound financial management of the Union budget or the protection of the financial interests of the Union in a sufficiently direct way*".[60] To be deemed sufficiently direct, the breaches of the principles of the rule of law should fall under one of the following exhaustively listed categories:[61]

(a) the proper functioning of the authorities implementing the Union budget, including loans and other instruments guaranteed by the Union budget, in particular in the context of public procurement or grant procedures;
(b) the proper functioning of the authorities carrying out financial control, monitoring and audit, and the proper functioning of effective and transparent financial management and accountability systems;
(c) the proper functioning of investigation and public prosecution services in relation to the investigation and prosecution of fraud, including tax fraud, corruption or other breaches of Union law relating to the implementation of the Union budget or to the protection of the financial interests of the Union;
(d) the effective judicial review by independent courts of actions or omissions by the authorities referred to in points (a), (b) and (c);
(e) the prevention and sanctioning of fraud, including tax fraud, corruption or other breaches of Union law relating to the implementation of the Union budget or to the protection of the financial interests of the Union, and the imposition of effective and dissuasive penalties on recipients by national courts or by administrative authorities;
(f) the recovery of funds unduly paid;
(g) effective and timely cooperation with OLAF[62] and, subject to the participation of the Member State concerned, with EPPO[63] in their

[60] See Article 4(1) of the Conditionality Regulation.

[61] See Article 4(2) of the Conditionality Regulation.

[62] While OLAF – the European Anti-Fraud Office – is able to investigate potential cases of corruption relating to the use of EU funds, it does not have the competence to prosecute fraudsters. Instead, it passes on its investigation results to the Member State in which the fraudulent behaviour took place, so that its public authorities can take the necessary action. Evidently, such a set-up is not ideal if potentially problematic behaviour comes from Member States' public authorities themselves, or if their independence is doubted. See also Kelemen and Scheppele (n 24).

[63] The European Public Prosecutor's Office (EPPO) is the Union's independent public prosecution office, established by Council Regulation 2017/1939 in October 2017 pursuant to the mechanism of enhanced cooperation. It started its operations in June 2021 and is able to investigate, prosecute and bring to judgment crimes against the EU's financial interests. It is also able to exercise the function of prosecutor in the courts of Member States. However, given

investigations or prosecutions pursuant to the applicable Union acts in accordance with the principle of sincere cooperation;

(h) other situations or conduct of authorities that are relevant to the sound financial management of the Union budget or the protection of the financial interests of the Union.

Following the Regulation's application to Hungary, on 15 December 2022, the Council decided to freeze about €6.3 billion of budgetary commitments,[64] citing rule of law breaches pertaining to public procurement procedures and prosecutorial action, as well as conflicts of interest and concerns around the fight against corruption (though not the concerns around judicial independence). At the same time, inspired by the Conditionality Regulation's approach of financial incentivisation, the Commission also started relying on legal provisions in other funding mechanisms that tie a Member States' receipt of funding to certain conditions (such as the Resilience and Recovery Regulation[65] and the Common Provisions Regulation[66]), including the obligation to uphold the Charter of Fundamental Rights. On this basis, on 22 December 2022 the Commission decided to freeze about €21.7 billion of EU cohesion funds until Hungary adopted several measures regarding LGBTQI+ rights, academic freedom, asylum policies and judicial independence.[67]

These actions were initially applauded, yet the applause for the Commission was short-lived. A year later, on 13 December 2023, it decided to unblock €10.2 billion of the frozen EU cohesion funds, justifying its decision based on a 'thorough assessment' of Hungary's newly adopted measures to strengthen the judiciary's independence.[68] While critics have characterised those measures as mere window

that it is based on the mechanism of enhanced cooperation, it only has those powers in the Member States that explicitly opted in. Currently, twenty-two of the twenty-seven Member States are participating. The five non-participants are Hungary, Poland, Sweden, Denmark and Ireland (though the latter two have a general opt-out from the Union's activities in the area of freedom, security and justice (AFSJ)).

[64] See Council Implementing Decision (EU) 2022/2506 of 15 December 2022 on measures for the protection of the Union budget against breaches of the principles of the rule of law in Hungary, ST/14247/2022/INIT, 2022.

[65] Regulation 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility, OJ L 57, 18 February 2021.

[66] Regulation (EU) 2021/1060 of the European Parliament and of the Council of 24 June 2021 laying down common provisions on the European Regional Development Fund, the European Social Fund Plus, the Cohesion Fund, the Just Transition Fund and the European Maritime, Fisheries and Aquaculture Fund and financial rules for those and for the Asylum, Migration and Integration Fund, the Internal Security Fund and the Instrument for Financial Support for Border Management and Visa Policy, PE/47/2021/INIT, OJ L 231, 30 June 2021.

[67] For a detailed discussion of those actions and their legal basis, see pages 176–183 in Kim Lane Scheppele, 'The Treaties without a Guardian: The European Commission and the Rule of Law' (2023) 29 Columbia Journal of European Law 93.

[68] The Commission, however, stressed that it "*will closely and continuously monitor, notably through audits, active engagement with stakeholders and in monitoring committees, the*

dressing, others have pointed to the politically strategic move of the Commission, as its decision to unfreeze the funds came a day before European leaders needed Hungary's cooperation to approve new aid to Ukraine.[69] In March 2024, the European Parliament therefore decided to challenge the Commission's decision before the Court of Justice, claiming that the Commission failed to fulfil its obligation to protect the EU budget and ensure that taxpayers' money is not misused.[70] If anything, this saga highlights that, despite the availability of *several* legal mechanisms to freeze EU funds, their application and effect are still highly dependent on the political willingness of EU actors and Member States to do so, and the bridging of political hurdles.

Let us, however, bracket this political aspect for a moment, and examine to what extent the Conditionality Regulation could at least theoretically serve as a mechanism to counter the threat of algorithmic rule by law. While it was certainly not conceived to offer protection in the specific context of algorithmic systems, it is worth asking whether it can nevertheless play a role in this context. Based on the contours set out above, a number of observations can be made.

First, given the Regulation's focus on the governance and sound management of EU funds, it appears to be most suitable in countering actions relating to fraudulent behaviour by officials or corrupt public procurement practices. Conversely, many of the examples discussed under Chapter 4, for instance in the area of social welfare or criminal risk assessments, would hence not easily fall under its scope. As regards the examination of tax fraud (an area in which algorithmic regulation is already widely used) the Regulation requires a link with the EU budget, and hence would not apply to all fraud examinations (for instance under points (c) and (e)). That said, the Court's judgment in *Ackerberg Fransson*[71] already clarified that, since the European Union's own resources include revenue from Member States' collection of VAT, the investigation and prosecution of tax fraud relating (even in part) to VAT affects the financial

application of the measures put in place by Hungary. If, at any point in time, the Commission considers that this horizontal enabling condition is no longer fulfilled, it may again decide to block funding." See European Commission, 'Commission considers that Hungary's judicial reform addressed deficiencies in judicial independence, but maintains measures on budget conditionality', Brussels, 13 December 2023, <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6465>.

[69] Jakob Hanke Vela and Claudia Chiappa, 'Brussels vs. Brussels: EU Parliament to Sue Commission over Hungary Cash' (*Politico*, 12 March 2024) < www.politico.eu/article/parliament-sues-commission-over-unfreezing-of-hungary-funds/>.

[70] Eddy Wax, '5 Questions about the EU Parliament Suing the Commission over Hungary Cash' (*Politico*, 18 March 2024), <www.politico.eu/article/5-questions-european-parliament-legal-action-commission-hungary-funds/>.

[71] See Case C-617/10, *Åklagaren v Hans Åkerberg Fransson*, 26 February 2013, ECLI:EU:C:2013:105.

interests of the European Union.[72] It could hence reasonably be argued that, when public authorities deploy algorithmic systems to detect and prosecute tax fraud (including VAT), and they do so in a manner that does not comply with the six rule of law principles set out above, this would likewise fall under the Regulation's scope.[73]

Yet one can also raise a more straightforward example of where algorithmic regulation might play a role. When the analysis of elements and risks based on which a procurement contract is allocated (or not) occurs with the help of algorithmic systems,[74] one could argue that the potentially problematic design and use of these systems can adversely impact the rule of law in a way that is relevant for the purpose of the regulation. Procurement processes are increasingly supported by analyses carried out by algorithmic systems, and one can easily imagine that 'objectivity' might also be invoked to this end. And while such automation could make procurement processes more 'efficient',[75] at the same time, one might also imagine the risk that, whether through negligence or deliberate design choices, the outcomes of the automated process favour some tenderers over others. This scenario would, at least in theory,[76] fit rather neatly under Article 4(2)(a) of the Conditionality Regulation, and hence be susceptible to trigger (the first step of) the suspension mechanism. Accordingly, it appears that a number of applications of algorithmic regulation could relevantly fall under the scope of the Conditionality Regulation.

However, that fact in and of itself does not yet help us much further. Certainly, the Regulation could in theory disincentivise Member States to adopt algorithmic regulation in an irresponsible manner in the abovementioned areas. However, for this to be the case, Member States must first be aware of the risks posed thereby to the rule of law, which is not a given. Furthermore, these provisions will still not

[72] See for instance §22 of the Judgment, in which the Court states inter alia that

> Given that the European Union's own resources include, as provided in Article 2(1) of Council Decision 2007/436/EC, Euratom of 7 June 2007 on the system of the European Communities' own resources (OJ 2007 L 163, p. 17), revenue from application of a uniform rate to the harmonised VAT assessment bases determined according to European Union rules, there is thus a direct link between the collection of VAT revenue in compliance with the European Union law applicable and the availability to the European Union budget of the corresponding VAT resources, since any lacuna in the collection of the first potentially causes a reduction in the second.

[73] Recall that several examples discussed under Section 4.1 concerned uses of algorithmic regulation to detect fraud.

[74] See for instance Su Jin Choi and others, 'AI and Text-Mining Applications for Analyzing Contractor's Risk in Invitation to Bid (ITB) and Contracts for Engineering Procurement and Construction (EPC) Projects' (2021) 14 Energies 4632.

[75] See also Oihab Allal-Chérif, Virginia Simón-Moya and Antonio Carlos Cuenca Ballester, 'Intelligent Purchasing: How Artificial Intelligence Can Redefine the Purchasing Function' (2021) 124 Journal of Business Research 69.

[76] In practice, it would, however, be highly difficult to establish this connection, given a general lack of insight into such processes.

ensure that they set up appropriate transparency, control and oversight mechanisms over the algorithmic systems' design and deployment process. And while, in theory, the Regulation could provide a means to penalise Member States who do not take the risks emanating from algorithmic regulation seriously, by the time such penalisation arrives, a lot of damage may already have occurred – damage that could potentially have been prevented or at least mitigated in case of ex ante oversight. Furthermore, as already noted previously, any ex post remedy will in any case be dependent upon the realisation that the algorithmic system was inappropriately designed or used, a realisation that is difficult to achieve if the use of the system is not transparent and open to *systemic* review rather than mere individual review.[77]

Consequently, while the Conditionality Regulation can at least help prevent that *more* EU funds are made available to Member States that, with or without the assistance of algorithmic regulation, infringe the rule of law's principles, its relevance remains confined to areas that have an explicit link with the EU financial interests, and to Member States who disregard the rule of law to *such* extent that the Commission feels itself forced to launch the mechanism provided in the regulation. As a preventative tool for Member States who are negligent rather than deliberate in countering the adverse impact that their algorithmic systems can have on the rule of law, it will have little to no effect. It can thus be concluded that other safeguards, preferably of an ex ante character, are needed to address the threat of algorithmic rule by law.

5.2.3 *Infringement Actions and Proceedings before National Courts*

The two mechanisms I discussed above seek to counter, respectively, Member State breaches of EU values (including the rule of law) that are 'serious and persistent'; and Member State breaches of the rule of law that directly affect the financial interests of the EU. Yet when it comes to the protection of the rule of *EU* law (namely Member States' adherence to European Union law more generally), there are two other mechanisms that can be pointed out. The first concerns the infringement procedure enshrined in Articles 258–260 TFEU, which allows the European Commission or a Member State to seize the CJEU in case a fellow Member State failed to fulfil an obligation under the Treaties. The second concerns the ability to challenge a national act that breaches EU law before a national court, potentially through the preliminary reference procedure laid down in Article 267 TFEU. Both of these procedures enable the judicial review of the legality of Member States'

[77] To concretise: the tenderer who saw her bid refused in favour of a bid by someone who is openly pro-government – and who fears that something might be wrong with the algorithmic system used during the evaluation process – may, for instance, challenge this administrative act before a court. However, as noted *supra*, in Section 4.1.5, this court will not necessarily be able to carry out a systemic review of the way in which the government uses algorithmic systems to evaluate bids.

actions in light of their obligations under EU law.[78] Indeed, Member States are obliged to take "*any appropriate measure, general or particular, to ensure fulfilment of the obligations arising out of the Treaties or resulting from the acts of the institutions of the Union*,"[79] including obligations they might have under both primary and secondary EU legislation.

By virtue of the infringement procedure of Article 258 TFEU, the Commission may sue a Member State before the CJEU when it considers that it has failed to fulfil an obligation under the Treaties.[80] It must first deliver a reasoned opinion on the matter and give the State concerned the opportunity to submit its observations. In the absence of the State's compliance with the opinion within the period laid down by the Commission, it may take the matter to Court.[81] Article 259 TFEU also foresees that a Member State which considers that another State failed to fulfil an obligation under the Treaties can bring the matter to Court – after first passing by the Commission.[82] If the Court finds that the Member State has indeed failed to fulfil an obligation, the State shall be required to take the necessary measures to comply with the judgment of the Court.[83]

Importantly, if the Commission subsequently finds that the Member State did not comply with the Court's judgment, it may take the matter before the Court again, this time with the request that the Member State be imposed a lump sum or penalty payment.[84] Accordingly, the infringement procedure also provides the Commission with financial leverage to ensure that Member States comply.[85]

Note that the threshold for such a procedure does not consist of a 'serious', 'persistent' or 'systemic' breach of EU law, but simply of the failure to fulfil an obligation. This can also concern the mere obligation to transpose a directive into national law within the specified deadline.[86] It should be noted that the European Commission has discretion as to whether or not it decides to bring a case to court, and it has no obligation to do so.[87] That said, pursuant to Article 17(1) TEU, it is the Commission's task to ensure that EU law is duly applied.[88]

[78] See in this regard also Lenaerts, Van Nuffel and Corthaut (n 3), chapters 29 and 30. See also Matteo Bonelli, 'Effective Judicial Protection in EU Law: An Evolving Principle of a Constitutional Nature' (2019) 12 Review of European Administrative Law 35; Koen Lenaerts, 'New Horizons for the Rule of Law within the EU' (2020) 21 German Law Journal 29.

[79] Article 4(3), §2.

[80] See Lenaerts, Maselis and Gutman (n 7) 179.

[81] Article 285 TFEU.

[82] Article 259 §2 TFEU.

[83] Article 260(1) TFEU.

[84] Article 260(2) TFEU.

[85] See also Lenaerts, Maselis and Gutman (n 7) 208.

[86] ibid 169.

[87] ibid 179.

[88] Article 17(1) TEU provides that the Commission shall promote the general interest of the Union and take appropriate initiatives to that end. It shall ensure the application of the Treaties, and of measures adopted by the institutions pursuant to them.

Some have argued that the infringement procedure avenue constitutes an important tool for the Commission to counter rule of law infringements in the EU.[89] Others have claimed, however, that: "*despite ten years of EU attempts at reining in Rule of Law violations and even as backsliding Member States have lost cases at the Court of Justice, illiberal regimes inside the EU have become more consolidated: the EU has been losing through winning*".[90] Admittedly, the infringement procedure is not designed to address systemic deficiencies of the rule of law, but rather provides a mechanism to ensure the enforcement of Member States' *specific* EU law obligations. However, used tactically, it can serve to challenge Member States' actions that adversely impact the rule of law, and the Commission is increasingly doing so. The Court is thereby enabled to carry out a judicial review of the conformity of a Member State's actions with EU law, and to call out their illegality in case of non-conformity.[91]

Another, more indirect, route to enable judicial review of Member States' actions at EU level is provided by Article 267 TFEU, which establishes a procedure that can be initiated by natural and legal persons before their national courts, hence complementing public enforcement with private enforcement.[92] National courts play an essential role in the EU legal order, as they safeguard the application of EU law at the national level. Given the primacy of EU law and its direct effect in national legal orders,[93] national courts must interpret national acts in line with EU law, and must even leave them aside when they breach EU law.[94] When they are uncertain about the way in which they should interpret EU law to assess the validity of a national (administrative) act, a national court can initiate a preliminary reference procedure and seek guidance from the CJEU.[95] In theory, the Court can only express itself about the interpretation of EU (primary and secondary) law rather than taking a stance about the validity of the national act. However, it should provide the national court with all the information it needs to undertake that assessment by itself.[96] When based on such guidance, which is binding for all courts in the EU, the national

[89] Pohjankoski (n 13). See also the discussion in Sonja Priebus and Lisa H Anders, 'Fundamental Change Beneath the Surface: The Supranationalisation of Rule of Law Protection in the European Union' (2024) 62 Journal of Common Market Studies 224, 235.

[90] Scheppele, Kochenov and Grabowska-Moroz (n 9).

[91] Through this mechanism, the Court is hence playing a pivotal role in the protection of the rule of law in Europe. See also John Morijn, 'Separate Charter Invocation as a New Enforcement Method: The Lex NGO Case' (2022) 59 Common Market Law Review 1137.

[92] See Lenaerts, Van Nuffel and Corthaut (n 3) 768.

[93] See also Bruno de Witte, 'Direct Effect, Primacy, and the Nature of the Legal Order' in Paul Craig and Gráinne de Búrca (eds), *The Evolution of EU Law* (Oxford University Press 2021).

[94] See Lenaerts, Van Nuffel and Corthaut (n 3) 769. See for instance Case C-573/17, *Popławski*, 24 June 2019, ECLI:EU:C:2019:530, §§58–62.

[95] See also Morten Broberg, 'Preliminary References as a Means for Enforcing EU Law' in András Jakab and Dimitry Kochenov (eds), *The Enforcement of EU Law and Values: Ensuring Member States' Compliance*, vol 1 (Oxford University Press 2017).

[96] See Lenaerts, Maselis and Gutman (n 7) 233.

court concludes that a legal act at national level breaches EU law, it needs to set it aside.

The disadvantage of this procedure is that a natural or legal person already needs to be involved in a legal challenge before a national court in order to request a preliminary reference procedure. Moreover, the invalidation of the national act does not necessarily imply an invalidation of the public authority's working method more generally, as the judicial review is limited to the particular act in question rather than being systemic in nature, which showcases the limits of ex post judicial review rather than an ex ante preventative approach at the system level. But at least it offers natural and legal persons a legal avenue to protect the rights they derive from EU law, and to ensure that Member States fulfil their EU law obligations. In the context of Member States' citizen surveillance, for instance, this procedure has already proven to be effective in invalidating national (and even EU) legislation that undermines the fundamental right to privacy and data protection.[97]

The question then is: which EU law obligations are relevant for the context of algorithmic regulation deployed by public authorities, and can pertinently be the object of an infringement procedure or of a legal challenge before a national court? Indeed, to trigger the use of these procedures, a specific provision of EU law must be breached – hence requiring the existence of a relevant EU law provision in the first place.

There is currently no general EU regulation or directive setting out the obligations that public authorities must fulfil to comply with the rule of law when taking administrative acts, regardless of whether they do so through reliance on algorithmic systems. The functioning of public administrations largely remained a matter of national competence, given its entwinement with the exercise of national powers. In situations where algorithmic regulation by public authorities leads to infringements of purely domestic law rather than EU law, the procedures mentioned above cannot be invoked and national remedies – to the extent available – need to be relied on instead. That said, in a wide array of public sector domains, a link to EU law can nevertheless be established given the increasing harmonisation of national law in fields that influence public administration, thus rendering purely domestic situations ever more rare. The EU has, for instance, adopted legislation in the area of

[97] The Court, for instance, invalidated the Data Retention Directive (Directive 2006/24/EC) which it found to entail a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and the protection of personal data, without that interference being limited to what is strictly necessary. See Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, 8 April 2014, ECLI:EU:C:2014:238. It also invalidated Commission Implementing Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield, in a case brought by a citizen in light of concerns that the Commission's Decision breached the fundamental right to data protection. See Case C-311/18, *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems*, 16 July 2020, ECLI:EU:C:2020:559.

migration law,[98] social security,[99] public procurement,[100] environmental protection,[101] international transport and border control,[102] data (re)use[103] and criminal justice.[104]

Whenever Member States implement EU law, they must respect fundamental rights as enshrined in the Charter[105] (including, for instance, the right of defence, the presumption of innocence and the right to a good administration) as well as general principles of EU law.[106] Therefore, if public authorities rely on algorithmic regulation while implementing EU law in a way that breaches individuals' fundamental rights or general principles of EU law – for instance the general principle of equality, due to the discriminatory design or use of an algorithmic system – this constitutes the breach of a Member State's obligation that can become the object of an infringement action or preliminary reference procedure. Yet when does a public authority implement EU law?

The most obvious case concerns the situation in which Member States' public authorities act based on an EU regulation, directive or other legal act with binding force. To provide an example of an area of administrative law that has been (partially) harmonised, consider the domain of migration law, and more specifically the right to asylum. This right is enshrined in Article 18 CFREU, and has been

[98] See, e.g., Directive 2011/95/EU of the European Parliament and of the Council of 13 December 2011 on standards for the qualification of third-country nationals or stateless persons as beneficiaries of international protection, for a uniform status for refugees or for persons eligible for subsidiary protection, and for the content of the protection granted, 20 December 2011, L 337/9. See more generally Loèic Azoulai and Karin de Vries, *EU Migration Law: Legal Complexities and Political Rationales* (Oxford University Press 2014).

[99] See, e.g., Regulation (EC) no. 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems.

[100] See, e.g., Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement, OJ L 94, 28 March 2014.

[101] See, e.g., Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on the assessment of the effects of certain public and private projects on the environment, OJ L 26, 28 January 2012.

[102] See, e.g., Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ L 119, 4 May 2016.

[103] See, e.g., Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), OJ L 172, 26 June 2019.

[104] See, e.g., Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings; Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty.

[105] See Article 51(1) CFREU.

[106] See Lenaerts, Van Nuffel and Corthaut (n 3) 684. See also Emily Hancox, 'The Relationship between the Charter and General Principles: Looking Back and Looking Forward' [2020] Cambridge Yearbook of European Legal Studies 22, 233–257.

further specified by secondary EU legislation that sets out which obligations Member States should respect vis-à-vis asylum applicants, and how they should evaluate an asylum application.[107] Accordingly, when a mistranslation from law to code (whether deliberate or inadvertent) occurs in the context of algorithmic regulation that helps assess asylum applications, this can give rise to an EU law infringement, both in terms of the public authority's failure to comply with the EU regulation or directive, and in terms of a potential breach of a fundamental right or general principle of EU law.

Besides harmonisation in vertical domains, there are also relevant pieces of legislation of horizontal nature. Consider, for instance, Council Directive 2000/43 that prevents discrimination based on racial or ethnic origin in a number of areas like social security and healthcare, thus setting out obligations that Member States must comply with.[108] When algorithmic regulation affects the rights of individuals based on their ethnicity, this can hence constitute a breach of EU law when the administrative act pertains to social security, the provision of healthcare, or another area of administration listed in the directive. Moreover, beyond situations of implementing EU legislation, the case law of the CJEU has indicated that also acts "*that constitute derogations from provisions of EU law, or acts adopted by the national authorities that only remotely are connected with EU law*",[109] can fall under the heading of 'EU law implementation'.[110]

Finally, some authors have argued that Article 2 TEU could in and of itself be understood as the basis for an EU law obligation based on which an infringement action can be launched in case of non-adherence to the rule of law.[111] For instance, Scheppele, Kochenov and Grabowska-Moroz have argued that Article 2 TEU could be relied upon to group isolated yet systemic infringements of EU law and, on that basis, to launch an infringement action, denoting this approach as a 'tool of militant

[107] See e.g. Directive 2013/32/EU of the European Parliament and of the Council of 26 June 2013 on common procedures for granting and withdrawing international protection (recast), 29 June 2013, L 180/60.

[108] See, for instance, EU Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin. See also Colm O'Cinneide and Kimberly Liu, *The Ongoing Evolution of the Case-Law of the Court of Justice of the European Union on Directives 2000/43/EC and 2000/78/EC: A Legal Analysis of the Situation in EU Member States* (Publications Office of the European Union 2019).

[109] Mihaela Vrabie, 'Judicial Review of Administrative Action at National Level under the EU Charter of Fundamental Rights and General Principles of EU Law' (2020) 18 Central European Public Administration Review (CEPAR) 25, 28.

[110] See, e.g., Case C-60/00, *Carpenter*, 11 July 2002, ECLI:EU:C:2002:434; Case C-36/02, *Omega*, 14 October 2004, ECLI:EU:C:2004:614; and Case C-208/09, *Wittgenstein*, 22 December 2010, ECLI:EU:C:2010:806. See also the abovementioned *Åklagaren v Hans Åkerberg Franson* case, C-617/10 (n 71).

[111] See, e.g., Scheppele, Kochenov and Grabowska-Moroz (n 9). See also Kim Lane Scheppele, 'Enforcing the Basic Principles of EU Law through Systemic Infringement Actions' in Carlos Closa and Dimitry Kochenov (eds), *Reinforcing Rule of Law Oversight in the European Union* (Cambridge University Press 2016).

democracy' through the launch of 'systemic infringement procedures'.[112] They believe that this approach could enable the Court, which has already shown itself an innovative protector of the principle of judicial independence by relying on Article 19(1) TEU, to play a more significant role in protecting other rule of law principles, which Article 7 TEU currently cannot due to the abovementioned political impasse. However, this understanding of Article 2 TEU is controversial, and as the authors themselves have noted, it is not widely supported.[113] Accordingly, the majority of scholars seem to consider that in order to be the object of an infringement procedure, the legal provision in question and the precise obligation it imposes on Member States needs to be more concrete, and cannot be brought under a collective Article 2 TEU umbrella.

That said, in December 2022, the Commission for the first time launched an infringement action against Hungary for rule of law-related breaches which not only cites violations of secondary EU legislation, but also the direct violation of Article 2 TEU itself.[114] Regardless of the outcome of this case, Bonelli and Claes point out that "*the autonomous enforceability of Article 2 TEU remains a controversial legal construction, one that, if accepted by the Court, could put its legitimacy and authority under strain*".[115] They also rightfully question whether "*the full judicialization of questions of 'values'*" is truly "*the most promising and effective response to the challenges that constitutional backsliding processes create*".[116]

Furthermore, notwithstanding the increasing harmonisation of national legislation, it should be stressed that a link with EU law cannot *always* be established, as there are still situations that are purely governed by domestic law. As I will discuss below,[117] this ups the game for any (new) EU legislative act that can provide safeguards for citizens whenever Member States deploy algorithmic regulation, as it can legally create a link with EU law (and hence with EU remedies) even in situations that are in principle considered domestic. Indeed, adopting EU legislation that governs the responsible use of algorithmic regulation by Member States in line with the rule of law would open up an avenue for the enforcement of these

[112] Scheppele, Kochenov and Grabowska-Moroz (n 9) 9–10.

[113] As the authors state: "*We recognise that most commentators have argued that only political mechanisms can be used to enforce the values of Article 2 TEU*". See ibid 8.

[114] The case concerns a new law that was introduced by the Hungarian government as a way of improving children's protection against paedophilia, while in effect containing several discriminating measures that specifically target the LGBTIQ+ community. See the Commission action brought on 19 December 2022 in Case C-769/22, *Commission v. Hungary*, still pending at the time of writing this book. See also Jannes Dresler, 'Der Brüsseler Testballon – Kommission betritt mit Klageschrift gegen Ungarns Anti-LGBTQ-Gesetz Neuland', (Verfassungsblog 21 February 2023) <https://verfassungsblog.de/der-brusseler-testballon/>.

[115] Matteo Bonelli and Monica Claes, 'Crossing the Rubicon? The Commission's Use of Article 2 TEU in the Infringement Action on LGBTIQ+ Rights in Hungary' (2022) 30 Maastricht Journal of European and Comparative Law 3, 4.

[116] ibid.

[117] See *infra*, Section 5.4.

provisions both through the infringement procedure of Articles 258–260 TFEU, and through legal challenges brought by individuals before national courts (with the associated preliminary reference procedure pursuant to Article 267 TFEU).

At the same time, the utility of these remedies, even in situations where a concrete obligation under EU law exists, must not be overstated. While the judicial review they enable can certainly play a role in the protection of the rule of (EU) law at Member State level, this is woefully insufficient to tackle the adverse effects of algorithmic regulation as identified in Chapter 4.

First, the ex post nature of these procedures means that the damage has already been done. As noted previously, if the damage is irreversible, any ex post remedy will be of little consolation to those adversely affected. If the damage is not (entirely) irreversible, in any event, a lot of time will inevitably pass between the damage caused and the judicial action. In the case of an infringement action, it typically takes the European Commission (which can decide to launch an action at its sole discretion) months if not years to collect sufficient evidence and arrive at a decision to initiate proceedings, if it decides to act at all.[118] In the case of a legal challenge brought by an individual before a national court, the speed of the potential remedy will depend on how swift the administration of justice in a particular country is organised. Moreover, the count starts not from the moment that problematic algorithmic regulation is used, but from the moment that someone is aware of such use and decides to bring a case.[119] By the time a condemning judgment arrives, significant harm can have occurred, and it may be too late to meaningfully remedy the situation. In addition, if the national court decides to stay proceedings to submit a request for a preliminary reference by the CJEU, the waiting time is extended by on average at least another year.[120] I invite the reader to reflect how much damage an infrastructure of algorithmic regulation, and the mass-decision-making it enables regarding millions of individuals, can cause in the time span of one year if left unaddressed.

Second, for an individual to bring a case before a court, she must not only be aware that algorithmic regulation is used (this is not straightforward given that many algorithmic applications are used in an untransparent manner[121]) but she must also have a sufficient incentive to start litigation.[122] If the damage at individual level is

[118] Recall that the Commission can initiate an infringement procedure at its own discretion. See Lenaerts, Van Nuffel and Corthaut (n 3) 784.

[119] See also *supra*, Section 4.1.5.

[120] Based on the Court of Justice's annual report of 2022, which includes statistical information about the court's activities, the average duration of proceedings that year was 16.4 months (and 17.3 months for requests for preliminary rulings). See Court of Justice of the European Union, 'Annual Report 2022 – The Year in Review' (CJEU 2023) 27, <https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-04/qd-aq-23-001-en-n.pdf>.

[121] Emre Bayamlıoğlu, 'Contesting Automated Decisions: A View of Transparency Implications' (2018) 4 European Data Protection Law Review 433.

[122] As discussed *supra*, in Section 4.1.5.

relatively small, the person may be unwilling to incur time and costs to do so, even if the damage at societal level may be significant. Furthermore, in many jurisdictions one needs to be able to demonstrate individual harm to have standing in court, which may not always be easy to prove when the harm primarily manifests itself at societal level or over the longer term, rather than at individual level and in the short term.[123] And if individual harm can be proven (for instance when a right was erroneously denied) we have seen that courts may not always be well-equipped to deal with the *systemic* problems raised by the scaled use of algorithmic systems, as they are typically tasked with case-by-case reviews only.[124] This means that the upstream design choices will remain untouched. The person may be re-allocated her benefits that were wrongfully denied, but this does not necessarily mean that choices at the upstream level will become transparent and contestable, and that harm to other interests will be avoided.

Finally, to invoke the procedures discussed above, a link with EU law must first be argued. As explained, while such a link can often be found, there are also situations that may not be governed by current EU law, hence precluding reliance on an existing EU remedy. Moreover, even if such a link is present, in certain Member States, the executive power is already exercising undue influence on national courts, and compromised their independence and impartiality.[125] In those jurisdictions, which already showcase authoritarian tendencies, one can question the effectiveness of national judicial review as a means to prevent the exacerbation of those very tendencies.

For all these reasons, the mechanisms discussed above are inadequate to ensure that the implementation of algorithmic regulation by public authorities occurs in accordance with the rule of law, and that it does not exacerbate the threat of algorithmic rule by law. As stressed in Chapter 4, the extent and scale of the risks associated with algorithmic regulation require *preventative* action, inter alia through the organisation of ex ante and continuous oversight over the crucial decisions taken in the design and deployment process of algorithmic systems, rather than mere *remedial* action. Yet the currently available EU mechanisms that deal with the protection of the rule of (EU) law (Article 7 TEU, the Conditionality Regulation,

[123] Nathalie A Smuha, 'Beyond the Individual: Governing AI's Societal Harm' (2021) 10 Internet Policy Review 3, 9. See also Bart van der Sloot and Sascha van Schendel, 'Procedural Law for the Data-Driven Society' (2021) Information & Communications Technology Law 1.

[124] Abe Chauhan, 'Towards the Systemic Review of Automated Decision-Making Systems' [2021] Judicial Review 1.

[125] Werner Schroeder, 'The European Union and the Rule of Law – State of Affairs and Ways of Strengthening', in Werner Schroeder (ed), *Strengthening the Rule of Law in Europe: From a Common Concept to Mechanisms of Implementation* (Hart Publishing 2016); Jörg Polakiewicz and Julia Katharina Kirchmayr, 'Sounding the Alarm: The Council of Europe as the Guardian of the Rule of Law in Contemporary Europe' in Armin von Bogdandy and others (eds), *Defending Checks and Balances in EU Member States: Taking Stock of Europe's Actions* (Springer 2021).

or Articles 258–260 TFEU and 267 TFEU) are, in my view, not tailored to prevent the adverse impact of algorithmic regulation on the rule of law. This is not only so because they lack specific references to algorithmic systems as the potential cause of such adverse impact – and hence lack specific requirements as regards their use – but also because they only enable ex post solutions, which risk being too little too late. In sum, EU regulation pertaining to the protection of the rule of law does not seem to be sufficiently extended to tackle the risks of algorithmic regulation.

The question is now whether EU regulation that pertains to algorithmic systems can play a meaningful role in the protection of the rule of law. While there is, as of yet, no piece of EU legislation that deals specifically with public authorities' rule of law obligations in the context of algorithmic regulation, there are several regulations that apply to public and private organisations alike when they inform or take their decisions with the assistance of algorithmic systems.[126] For reasons of time and space, I will focus on the two most relevant ones for the purpose of my investigation: the General Data Protection Regulation (and neighbouring Law Enforcement Directive), which I discuss in Section 5.3, and the Artificial Intelligence Act, which I discuss in Section 5.4.

5.3 REGULATION PERTAINING TO PERSONAL DATA: THE GDPR

Few pieces of legislation are as relevant for the use of algorithmic regulation today as the General Data Protection Regulation (GDPR)[127] – and, in the context of

[126] Accordingly, when it comes to the regulation of algorithmic systems, instead of speaking of a legal vacuum, one can rather speak of legal gaps. Consider for instance the Machinery Directive which is relevant when algorithmic systems are embedded in hardware (Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast), OJ L 157, 9 June 2006), or the Digital Services Act (amending Directive 2000/31/EC) which touches upon algorithmic systems used in online platforms. More generally, the Product Liability Directive, for instance, also deals with liability questions related to certain algorithmic systems (Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products OJ L 210, 7 August 1985). It can be noted that the European Commission also proposed a new directive to harmonise liability rules pertaining to AI systems. See the Proposal for a Directive of the European Parliament and the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) 2022 [COM(2022) 496 final], which has not yet been adopted at the time of writing this book. See in this regard also European Commission, 'Commission Staff Working Document *Liability for emerging digital technologies*, accompanying the Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial intelligence for Europe', SWD/2018/137 final, Brussels, 25 April 2018.

[127] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) 2016 1.

criminal matters, the Law Enforcement Directive (LED).[128] The regime provided in these (highly similar) pieces of legislation shields individuals against infringements of their fundamental right to personal data protection,[129] by granting them protective rights and imposing obligations on organisations[130] that process their personal data.[131] Since a significant part of algorithmic systems used to inform or adopt administrative acts process personal data, these rights and obligations play an important role in this domain. The scope of application of the GDPR and LED is wider than algorithmic regulation though, as they apply to "*the processing of personal data wholly or partly by automated means*".[132] These legal instruments set out a dense legal framework and, in what follows, I will only point out some of its most relevant features.

Pursuant to their obligations under these legal instruments, when public authorities deploy algorithmic systems to inform or adopt administrative acts and in the course thereof process personal data, such data must be processed in line with a number of principles, including the principle of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity

[128] 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, and repealing Council Framework Decision 2008/977/JHA 2016.

[129] Article 8(1) CFREU and Article 16(1) TFEU provide that all individuals have the right to the protection of their personal data.

[130] The GDPR applies to private and public actors alike, though, given the focus of this book, I will only focus on the latter. The LED in principle only applies to 'competent authorities', meaning "*any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*" or "*any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security*". See in this regard Article 3(7) LED. Note that both pieces of legislation in principle do not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law. See Article 2(2)(a) GDPR and Article 2(3)(a) LED.

[131] Personal data is defined broadly, as

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

See Article 4(1) GDPR and Article 3(1) LED.

[132] As well as to "*the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system to any processing of personal data*". See Article 2(1) GDPR and Article 2(2) LED respectively.

and confidentiality; and accountability.[133] Moreover, the lawfulness of the data processing relies on the availability of a legal basis which, in the context of public authorities, will often come down to the fact that "*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller*".[134]

5.3.1 *Need for a Legal Basis*

To legitimise such data processing, Member States should in principle adopt a law that sets out the purpose of the processing, and that contains more specific provisions about the types of data that are processed; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and any processing operations and procedures.[135] This is also why the implementation of algorithmic systems by public authorities must have a lawful basis, which typically requires the adoption of a specific law that authorises the use of the system in line with the provisions of the GDPR (or the LED). The legal basis should indicate that the introduction of the algorithmic system, which can be invasive and impactful given the data processed and the scale at which it is deployed, is necessary and proportionate.

Importantly, the existence of a legal basis also renders it possible to subsequently challenge the system's use if the basis on which it was adopted does not provide sufficient protection against potential adverse impacts of the system, or is not in accordance with human rights law. This is precisely what happened in the Dutch SyRI case, which centred around an algorithmic system aimed at identifying natural and legal persons which, based on a set of risk-indicators, ought to be further examined for social security or tax fraud.[136] According to the government, the purpose of the system concerned "*the prevention of and combating the unlawful use of government funds and government schemes in the area of social security and income-dependent schemes, preventing and combating taxes and social security fraud and non-compliance with labour laws*".[137] The system allowed for the exchange of data amongst a variety of public authorities to facilitate the identification of fraud. Based on the system's risk-indications, a risk report was made concerning an individual's fraud potential. The SyRI-law defined a 'risk report' as

[133] See Article 5 GDPR. In the LED, these principles are formulated in a similar way, though with omission of the principle of transparency. See Article 4(1) LED.

[134] See Article 6(1)(e) GDPR.

[135] See Article 6(3) GDPR.

[136] See in this regard also Marvin van Bekkum and Frederik Zuiderveen Borgesius, 'Digital Welfare Fraud Detection and the Dutch SyRI Judgment' (2021) 243 European Journal of Social Security 323.

[137] *NJCM et al. en FNV v Staat der Nederlanden (SyRI Judgment)* [2020] Rechtbank Den Haag C-09-550982-HA ZA 18-388, ECLI:NL:RBDHA:2020:865, section 4.4.

> the provision of individualised information from [SyRI] containing a finding of an increased risk of unlawful use of government funds or government schemes in the area of social security and income-dependent schemes, taxes and social security fraud or non-compliance with labour laws by a natural person or legal person, and of which the risk analysis, consisting of coherently presented data from [SyRI], forms part.[138]

The system was already in use for years when, in 2014, a law was finally adopted to ensure a legal basis for its deployment, known as the SyRI-law. When the law was challenged in court, it was, however, found to be an insufficient legal basis to justify the system's use. The court concluded that it did not provide sufficient safeguards to protect individuals against the impact on their right to privacy, after which the government halted the system's use. For instance, the risk reports established by the system were put into a register.[139] This left a clear trace for other public authorities which risked stigmatising those individuals, even if the flagging turned out to be erroneous. Moreover, the persons concerned were not informed of the fact that a risk report was made about them (unless they specifically asked for this information by themselves).[140] And while the law also foresaw that public authorities had to justify the necessity and proportionality of the data exchange for the purpose of the risk analysis, no safeguards were included to ensure an adequate and comprehensive review of those justifications.

This case demonstrates that the GDPR is able to offer individuals protection by ensuring that the use of algorithmic systems needs to have an adequate legal basis. At the same time, it should be noted that the provisions of the GDPR, as such, do not necessarily provide insight (let alone participation) in any of the upstream decisions made by the coders, such as the assumptions that underlie the system, the interpretation and translation choices, or the model's optimisation function. Moreover, in many cases, the legal basis can be overly vague or provide overly extensive processing powers to avoid that the law must be amended whenever new processing activities take place, thus also undermining the protection it offers towards those subjected thereto.[141] Note that the processing of special categories of

[138] Article 65(2) SUWI Act or Wet structuur uitvoeringsorganisatie werk en inkomen. The implementation of that law was further specified through the Decree of 1 September 2014 to amend the SUWI Decree in connection with rules for tackling fraud by exchanging data and the effective use of data known within the government with the use of SyRI, Bulletin of Acts and Decrees 2014, 320.

[139] In line with the storage limitation principle, the law did foresee that the risk report could only be kept for as long as necessary to execute the relevant task, and for a maximum period of two years. See Article 65 of the law.

[140] *NJCM et al. en FNV v Staat der Nederlanden (SyRI Judgment)* (n 137), section 4.14.

[141] See, for instance, Degrave's observation that the law which is meant to provide a legal basis for the OASIS system – used by public authorities to identify fraud – is far too vague to comply with the GDPR, in Elise Degrave, 'The Use of Secret Algorithms to Combat Social Fraud in Belgium' (2020) 1 European Review of Digital Administration & Law 167.

personal data, such as data revealing racial or ethnic origin, political opinions, biometric data for the purpose of uniquely identifying a natural person, or data concerning a person's sexual orientation, is in principle prohibited, yet exceptions exist,[142] and public authorities can typically rely on them to exercise their functions if such processing is authorised by law.[143]

5.3.2 *Automated Decision-Making*

The GDPR and LED allocate certain rights to persons whose personal data is processed, such as the right to information about the data processing, the right of access to their data, the right to rectify their data and the right to erasure.[144] In addition to these general rights, natural persons also have specific rights in the context of automated decision-making. It should be pointed out that, for the purpose of the GDPR, automated decision-making is much broader than the adoption of an administrative act, but covers any type of decision taken through automated means, including profiling.[145] Accordingly, all intermediate decisions that are taken by automated means to inform an administrative act (for instance the automated classification of individuals in one category or another) also count as such.[146] Pursuant to Article 22 of the GDPR,[147] whenever a decision is being taken about an individual based solely on automated processing[148] which produces legal effects

[142] In this regard, it can also be noted that the AI Act (discussed *infra* in Section 5.4), establishes a specific legal basis to process such sensitive data '*to the extent that it is strictly necessary for the purpose of ensuring bias detection and correction in relation to the high-risk AI systems*', though several safeguards need to be fulfilled. See Article 10(5) AI Act.

[143] See Articles 9 and 10 GDPR. Note that, in this case, despite the existence of a legal basis, public authorities must provide appropriate safeguards for the fundamental rights and the interests of the data subject.

[144] See sections 2 and 3 of the GDPR.

[145] Article 4(4) of the GDPR defines profiling as "*any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements*".

[146] See in this regard also the Court's interpretation of automated decision-making in case C-634/21, *OQ v SCHUFA Holding* AG, 7 December 2023, ECLI:EU:C:2023:957.

[147] Under the legal regime of the LED, individuals have no right to object to automated individual decision-making. Pursuant to Article 11(1) of the LED, this practice is prohibited unless authorised by Union or Member State law and providing "*appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller*." Nothing is, however, mentioned about a right to receive "meaningful information about the logic involved in the automated decision-making process", such as foreseen in Article 14 GDPR (see below).

[148] Recital 71, §2 of the GDPR also specifies that, in order to ensure fair and transparent processing in respect of the data subject,

> the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the

concerning her, or similarly significantly affects her, that individual has the right *not* to be subject to such decision.[149] While inclusion of the word 'solely' seemingly excludes situations where a decision is merely recommended by an algorithmic system and subsequently reviewed and adopted by a human being, such review should in principle be meaningful in order to warrant the exclusion. Merely "fabricating" human involvement will not do.[150]

Moreover, under those circumstances, the data controller[151] has the obligation to provide the individual concerned with information about the existence of automated decision-making and "*meaningful information about the logic involved*", as well as the significance and the envisaged consequences of such processing for her.[152] Recital 71 of the GDPR also states that "*such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision*". Yet given that recitals are non-binding, scholars disagree as to whether an actual individualised 'right to explanation' of an automated decision exists.[153]

These rights, along with other rights listed in the GDPR, can be restricted by Member State law as long as this restriction "*respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard*" a range of interests, including national and public security, the prevention of criminal offences, and even – rather generally – "*other important objectives of general public interest of a Member State*".[154] In that case, the Member

risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect.

[149] Article 22(1) GDPR. Note, however, the argument by Aziz Huq *against* a right to a human decision (as it still seems "too early" to assume that human decisions will be globally superior to machine decisions). Instead, he suggests that a better option may be a right to a well-calibrated machine decision, in 'A Right to a Human Decision' (2020) 106 Virginia Law Review 611.

[150] Article 29 Data Protection Working Party, 'Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679' (last Revised and adopted on 6 February 2018, 2017) 17/EN WP251rev.01 21.

[151] Article 4(7) GDPR defines the controller as "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*".

[152] See Article 14(2)(g) GDPR.

[153] See, e.g., Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76; Bryce Goodman and Seth Flaxman, 'European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation"' (2017) 38 AI Magazine 50; Margot E Kaminski, 'The Right to Explanation, Explained' (2019) 34 Berkeley Technology Law Journal 189.

[154] Article 23(1) GDPR.

State law should however contain provisions that describe the data processing activity and its purpose, as well as the safeguards to prevent abuse.[155]

Also noteworthy is the fact that, whenever a type of processing ("*in particular using new technologies*") is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data, referred to as a Data Protection Impact Assessment or DPIA).[156] Pursuant to Article 35(3)(a) of the GDPR, a DPIA is particularly required in the case of "*a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*".

Data controllers are, however, not obliged to make this assessment public, and input from the individuals concerned is only warranted "*where appropriate*" and "*without prejudice to the protection of public interests or the security of processing operations*".[157] Finally, to oversee compliance with these rights and obligations, the GDPR established national data protection authorities, acting "*with complete independence in performing its tasks and exercising its powers*", which is especially important when supervising the data processing activities of public authorities.[158]

5.3.3 *Evaluation: Necessary but Not Sufficient*

With this in mind, to which extent can the safeguards afforded by the GDPR help counter the adverse impact of algorithmic regulation on the rule of law? Unfortunately, the conclusion is not overly optimistic. Certainly, the GDPR establishes a critical and necessary set of EU obligations that Member States should respect (which can also become the object of a procedure under Articles 258–260 TFEU or Article 267 TFEU) and provides individuals with important rights they can directly invoke in a national court against public authorities. And since algorithmic regulation very often implies personal data processing, those rights and obligations are unquestionably relevant in this context. That said, these safeguards cannot be called comprehensive.

As observed by Maja Brkan, the provision that aims to protect individuals against the adverse effects of automated decision-making, by containing "*numerous*

[155] Article 23(2) GDPR. More generally, it should be noted that exceptions provided for in the GDPR must be interpreted strictly. See in this regard also §70 of the abovementioned PNR Judgment (Case C-817/19, *Ligue des droits humains ASBL v Conseil des ministres (PNR Case)*, 21 June 2022, ECLI:EU:C:2022:491).

[156] Article 35(1) GDPR.

[157] Article 35(9) GDPR.

[158] Articles 51 and 52 GDPR.

limitations and exceptions, looks rather like a Swiss cheese with giant holes in it".[159] While individuals should be informed of the fact that decisions are being made about them in an automated way, recall that the right not to be subjected to such decisions is only present in case of a 'solely' automated decision with 'legal effects' or similar, that exceptions exist in the 'public interest' and that no transparency is foreseen about the algorithm's functioning and the normative assumptions that underpin its design. In general, the GDPR contains no mechanisms that enable prior oversight over the upstream design of the algorithmic system (for instance to ensure its outcomes are accurate and non-biased); no obligatory mechanisms of public participation; no constitutional checks and balances as regards the translation from law to code; and no mechanisms that foster friction and internal critical reflection, for instance by mandating *meaningful* human oversight.

This is not to say that the GDPR and the LED, along with primary EU law protecting the rights to privacy and data protection, cannot play a role in ensuring that governments process the personal data of their citizens in a responsible manner, as previous legal challenges have demonstrated.[160] For instance, in June 2022, the CJEU was seized by a preliminary reference procedure regarding the Passenger Name Record (PNR) Directive and the Belgian law implementing it.[161] The case concerned the automated processing of passenger data by public authorities in the context of border control, enabled by the establishment of large databases to search and identify passengers involved in a terrorist offence or serious crime. While the Court found that the Directive poses an "*undeniably serious interference*" with the rights to privacy and data protection,[162] it nevertheless concluded it was compatible with the Charter, as it required the *predetermination* of the criteria based on which the database could be searched, and required these criteria to be non-discriminatory.[163] In the same breath, however, the Court noted that this "*requirement precludes the use of artificial intelligence technology in self-learning*

[159] Maja Brkan, 'Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond' (2019) 27 International Journal of Law and Information Technology 91, 97.

[160] For instance, in the abovementioned unlawful use of an algorithmic system in the Netherlands to detect fraud amongst child care benefit recipients, the Dutch data protection authority imposed a fine of €2.75 million on the Dutch Tax Administration, based on the fact that the authority had infringed the GDPR. See Autoriteit Persoonsgegevens, 'Tax Administration Fined for Discriminatory and Unlawful Data Processing' (8 December 2022) <https://autoriteitpersoonsgegevens.nl/en/news/tax-administration-fined-discriminatory-and-unlawful-data-processing>.

[161] See Case C-817/19 (n 155).

[162] Ibid., §111.

[163] More generally, the Court insisted on a narrow interpretation of the intrusive provisions of the Directive and the Belgian law implementing it, to ensure their proportionality. See also Thomas Wahl, 'CJEU: PNR Directive Valid if Limited to the "Strictly Necessary"' (*Eucrim*, 4 August 2022), <https://eucrim.eu/news/cjeu-pnr-directive-valid-if-limited-to-the-strictly-necessary/>.

systems ('machine learning'), capable of modifying without human intervention or review of the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based as well as the weighting of those criteria."[164] It added that

> given the opacity which characterises the way in which artificial intelligence technology works, it might be impossible to understand the reason why a given program arrived at a positive match. In those circumstances, use of such technology may deprive the data subjects also of their right to an effective judicial remedy enshrined in Article 47 of the Charter, for which the PNR Directive, according to recital 28 thereof, seeks to ensure a high level of protection, in particular in order to challenge the non-discriminatory nature of the results obtained.[165]

Accordingly, the PNR judgment affirms the important role that EU privacy legislation can play in the context of algorithmic regulation, and the importance of transparency about the way in which individuals' data are being processed.[166]

At the same time, the lack of *ex ante* oversight mechanisms means that external accountability remains largely confined to an ex post stage, when the damage already occurred. Moreover, the focus lays primarily on harm to individual rather than to societal interests, such as the rule of law. It does not touch upon the intricacies of translating legal rules to code, nor does it provide more *systemic* remedies and oversight.[167] In sum, these legal instruments do not provide sufficient safeguards to counter the threat of algorithmic rule by law, or even properly to counter the risks raised by algorithmic systems more generally. While this conclusion may be rather glum, it was not only reached by other scholars, but also by the European Commission itself, who in February 2020, when it published its White Paper on AI,[168] observed that the current framework, including the GDPR, insufficiently protects people against the adverse impact of algorithmic systems.[169] Consequently, in April 2021, it put forward a proposal for an AI Act in order to fill these legal gaps. I will therefore examine this Act next.

[164] Case C-817/19 (n 155) §194.

[165] ibid., §195.

[166] For an overview of the relevance of data protection law in the context of algorithmic systems, and its interaction with the AI-specific rules of the AI Act, see also Nathalie A Smuha, 'The paramountcy of data protection law in the age of AI (Acts)' in EDPS (ed), *Two Decades of Personal Data Protection. What's Next?* (Publication Office of the EU 2024), 214–227.

[167] Smuha, 'Beyond the Individual' (n 123).

[168] See European Commission, 'White Paper on Artificial Intelligence – A European Approach to Excellence and Trust', COM(2020) 65 final, Brussels, 19 February 2020.

[169] In the Commission's own words, after having provided an overview of existing legislation and the risks not yet properly covered thereby "*the Commission concludes that – in addition to the possible adjustments to existing legislation – a new legislation specifically on AI may be needed in order to make the EU legal framework fit for the current and anticipated technological and commercial developments*"; see ibid 16.

5.4 REGULATION PERTAINING TO ALGORITHMIC SYSTEMS: THE AI ACT

The AI Act has been heralded as the first comprehensive regulation of AI systems in the world, aiming to tackle risks to people's health, safety and fundamental rights in a horizontal manner – including in the public sector, thus meriting a more extended discussion in this book. While the European Union has certainly not been the only jurisdiction partaking in the global race to AI regulation, other jurisdictions have thus far primarily focused their legislative efforts on sector- or application-specific regulations.[170]

After three years of extensive negotiations, and numerous amendments[171] suggested by the European Parliament and the Council (respectively in December 2022[172] and in June 2023[173]), the new regulation was formally adopted in 2024.[174] Much ink has already been spilled about the AI Act's merits and flaws, long before its adoption. Yet the question I am interested in here concerns the extent to which the AI Act's provisions are able to tackle the threat of algorithmic rule by law. Its novelty rendered it an ideal vehicle to introduce new legal safeguards to address the many concerns identified by scholars and civil society organisations over the past few years, and to bridge the gaps left open by the GDPR. However, does the new regulation fulfil this expectation?

[170] China has, for instance, been an early adopter of AI regulation as well, with targeted rules for algorithmic recommendation systems, deepfakes, and generative AI services in particular. In this regard, see e.g. Angela Zhang, 'The Promise and Perils of China's Regulation of Artificial Intelligence', University of Hong Kong Faculty of Law Research Paper No. 2024/02, SSRN <https://ssrn.com/abstract=4708676>.

[171] Generally speaking, the Council's amendment aimed to limit the AI Act's scope, while the Parliament instead sought to widen it, bringing to the fore a strong divergence in terms of their desired regulatory approach. That said, neither the Council nor the Parliament are monolithic entities, and in each of these institutions, different views exist. Moreover, finding alignment across Member States, as well as across political parties, has been far from evident.

[172] The Council's general approach to the AI Act was formally adopted on 6 December 2022: Council of the European Union, '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' (6 December 2022) <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf>.

[173] The Parliament's position on the AI Act was adopted in June 2023, after lengthy negotiations between the various political parties: European Parliament, 'Amendments Adopted by the European Parliament on 14 June 2023 on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021)0206 – C9–0146/2021–2021/0106(COD))' P9_TA(2023)0236 <www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf>. In fact, already by the spring of 2022, a few thousands of amendments had been proposed by Members of Parliament. See Luca Bertuzzi, 'AI Regulation Filled with Thousands of Amendments in the European Parliament' *Euractiv* (2 June 2022) <www.euractiv.com/section/digital/news/ai-regulation-filled-with-thousands-of-amendments-in-the-european-parliament/>.

[174] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

To answer this question, I will respectively analyse the AI Act's scope and rationale (Section 5.4.1), its regulatory architecture (Section 5.4.2), the set of systems used by public authorities that fall under its provisions (Section 5.4.3), the requirements to which high-risk algorithmic regulation systems are subjected (Section 5.4.4), and the repercussions of its maximum approach to harmonisation (Section 5.4.5). Drawing on that analysis, I will assess the regulatory potential of the AI Act and conclude that it fails to provide a sufficient level of protection. Moreover, despite the critique provided thereon in Chapter 4, I argue that the AI Act effectively reinstates 'techno-supremacy' through its legal infrastructure, resulting in a relatively grim overall evaluation of this new regulation (Section 5.4.6).

5.4.1 *The AI Act's Goals and Scope*

5.4.1.a The AI Act's Origins

To understand the regulation's rationale, it is useful to briefly revisit its history. In essence, the AI Act builds on the work of the High-Level Expert Group on Artificial Intelligence, set up by the European Commission in June 2018 with the aim of drafting AI Ethics Guidelines[175] and Policy Recommendations.[176] At that time, one month after the GDPR came into force and modernised European privacy law, new legislation on the use of algorithmic systems seemed unnecessary, as it was the prevailing opinion at the Commission that existing rules already sufficed to protect individual and societal interests. Gradually, this stance changed, with the rise of both internal and external pressure to take action beyond the promotion of non-binding guidelines. Moreover, when submitting its deliverables in the spring of 2019, the High-Level Expert Group concluded that new legislation was needed to fill existing legal gaps, claiming that the risks posed by certain systems required stronger safeguards.[177] Concretely, the Expert Group proposed a risk-based approach[178] to

[175] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (European Commission 2019) <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>.

[176] High-Level Expert Group on AI, 'Policy and Investment Recommendations for Trustworthy AI' (European Commission 2019) <https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence>.

[177] While the Group's Ethics Guidelines for Trustworthy AI already indicated a number of 'critical concerns' that required being addressed (see page 33 and following), in its Policy and Investment Recommendations it formulated more concrete guidance to the Commission as regards legal gaps (see page 37 and following).

[178] The group noted that "*'risk' for this purpose is broadly defined to encompass adverse impacts of all kinds, both individual and societal*", emphasising that this includes "*not only tangible risks to human health or the environment, but also intangible risks to fundamental rights, democracy and the rule of law, and other potential threats to the cultural and socio-technical foundations of democratic, rights-respecting, societies.*" See High-Level Expert Group on AI, 'Policy and Investment Recommendations for Trustworthy AI' (n 176) 38.

regulate AI,[179] combined with a principle-based approach that avoids over-prescriptiveness, and a precautionary approach "*when the stakes are high*", highlighting hazards to some of the EU's core values, such as human health, the environment and the democratic process.[180] It also noted that questions about which kinds of risks are deemed unacceptable "*must be deliberated and decided upon by the community at large through open, transparent and accountable deliberation*".[181] As regards the public sector in particular, the group stressed that safeguards were needed to protect "*individuals' fundamental rights, democracy and the rule of law*",[182] the alignment of which was more generally stressed across its deliverables.[183]

The Commission listened in part. It started mapping the legal gaps left open by existing pieces of legislation and, in February 2020, it outlined a blueprint for new AI-specific legislation through its White Paper on Artificial Intelligence.[184] After inviting feedback through a public consultation, the Commission put forward its proposal for an AI Act in April 2021, with clear references to the Expert Group's work. The Expert Group's Ethics Guidelines for 'Trustworthy AI' (a term coined by the experts to denote systems that are lawful, ethical and robust) listed seven key requirements that should be met throughout the life cycle of AI systems, based on fundamental rights.[185] In the Explanatory Memorandum of the AI Act, the Commission presented its proposal as providing "*a legal framework for trustworthy AI*"[186] and translated these key requirements into a series of legal requirements that should be met whenever AI systems are put into use or placed on the market.[187]

5.4.1.b Objectives and Legal Basis

The AI Act has the dual aim of harmonising Member States' national legislation to eliminate potential obstacles to trade on the internal market, and protecting the health, safety and fundamental rights of individuals against AI's adverse effects – in

[179] ibid 37, 26.1.

[180] ibid 38, 26.2.

[181] ibid. Furthermore, the group proposed the adoption of a segment-specific methodology, whereby the protective measures of individuals against the adverse effects of AI would be tailored to, respectively, the private sector context and the public sector context. See ibid, 26.5.

[182] ibid 19, 9.4.

[183] See, e.g., High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (n 175) 35.

[184] European Commission, 'White Paper on Artificial Intelligence – A European Approach to Excellence and Trust' (n 168).

[185] High-Level Expert Group on AI, 'Ethics Guidelines for Trustworthy AI' (n 175) 14. See also Nathalie A Smuha, 'The EU Approach to Ethics Guidelines for Trustworthy Artificial Intelligence' (2019) 20 Computer Law Review International 97.

[186] See Explanatory Memorandum of the proposed AI Act, section 1.1, §2.

[187] See also Vera Lúcia Raposo, 'Ex Machina: Preliminary Critical Assessment of the European Draft Act on Artificial Intelligence' (2022) 30 International Journal of Law and Information Technology 88, 97.

that order. Indeed, as indicated by the AI Act's very first recital, and as the below discussion will highlight, the creation of an internal market for the free circulation of AI and the promotion of its uptake is the regulation's primary aim, with the protection of fundamental rights and other values being something to keep in mind while doing so.[188] Note that, despite the references thereto in the Expert Group's deliverables, the protection of the rule of law was not mentioned as an objective in the Commission's original proposal (an omission that scholars have criticised)[189] and is also barely mentioned in the AI Act's final version.[190]

Clearly, the regulation primarily pursues an internal market-oriented approach rather than a values-oriented one, in line with its underlying legal basis. Indeed, the Commission opted to rely on Article 114 TFEU (enabling the establishment and functioning of the internal market) as the Regulation's legal basis. This is not surprising, as the EU lacks a general legal basis to regulate (technology's adverse impact on) fundamental rights, democracy and the rule of law, and frequently relies on Article 114 TFEU to advance the protection of the interests for which it has no specific competence.[191] If the emphasis of the Regulation would have been on the protection of those values, Article 352 TFEU would arguably have been a more appropriate legal basis, as this Article allows the EU to adopt an act necessary to attain objectives laid down by the treaties whenever the treaties do not provide the

[188] Recital 1 of the AI Act – which has been lengthened by many amendments – reads as follows:

> The purpose of this Regulation is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of artificial intelligence systems (AI systems) in the Union, in accordance with Union values, to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter'), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation.

[189] See Nathalie A Smuha and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' (Social Science Research Network 2021) <https://papers.ssrn.com/abstract=3899991>.

[190] The only substantive article in which the rule of law is mentioned is Article 1(1) AI Act. While it sets out the AI Act's subject matter, the rule of law is clearly *not* the object of this regulation, thus making its inclusion mostly rhetorical.

[191] As previously noted, before Article 16 TFEU enshrined an EU legal basis to regulate the protection of personal data (based on which the GDPR was adopted), the harmonisation of national privacy legislation was based on Article 114 TFEU. Moreover, the Digital Services Act – which inter alia has the objective of protecting democracy and fundamental rights online – is likewise based on Article 114 TFEU. See Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27 October 2022.

necessary powers of action for this purpose.[192] Reliance on this legal basis, however, requires unanimity in the Council and is hence typically avoided.[193]

By definition, a market-oriented legal basis entails certain limitations, as it renders regulatory intervention in the public sector (especially as regards law enforcement activities, public administration or the justice system) more difficult to justify. The legislator therefore also added Article 16 TFEU as a legal basis, yet only to the extent that, for the purpose of law enforcement, it contains specific rules on the protection of individuals' personal data which concern restrictions of "*the use of AI systems for remote biometric identification*", "*the use of AI systems for risk assessments of natural persons*" and "*the use of AI systems of biometric categorisation*".[194] One can still question whether the combination of Article 114 TFEU and, very limitedly, Article 16 TFEU constitutes a sufficient legal basis to extend the AI Act to the use of algorithmic systems by public administrations, yet I will not be delving further into this question here. For the remainder of my analysis, I will therefore proceed under the assumption that the AI Act's legal basis is valid.

5.4.1.c AI's Definition

Before turning to the regulatory framework and content of the AI Act, let me make a brief note on how it defines AI. As previously stressed, the definition of artificial intelligence constitutes an important battleground as it sets out the contours of the technological applications that fall under the law's scope, thereby also determining its regulatory relevance.[195] I shall not repeat here the definition's history which I discussed in Section 2.1.5, but merely zoom in on the final version of the

[192] See Article 352(1) TFEU, stating that

> If action by the Union should prove necessary, within the framework of the policies defined in the Treaties, to attain one of the objectives set out in the Treaties, and the Treaties have not provided the necessary powers, the Council, acting unanimously on a proposal from the Commission and after obtaining the consent of the European Parliament, shall adopt the appropriate measures. Where the measures in question are adopted by the Council in accordance with a special legislative procedure, it shall also act unanimously on a proposal from the Commission and after obtaining the consent of the European Parliament.

This is referred to as the so-called flexibility clause and requires that national parliaments are made aware of any legislative initiative proposed on that basis, considering the potential encroachment thereof on their legislative powers. See Article 352(2) TFEU and Article 5(3) TEU.

[193] The Parliament only needs to consent. Ibid. See also Theodore Konstadinides, 'Drawing the Line between Circumvention and Gap-Filling: An Exploration of the Conceptual Limits of the Treaty's Flexibility Clause' (2012) 31 Yearbook of European Law 227.

[194] Recital 3 of the AI Act.

[195] See also Bilel Benbouzid, Yannick Meneceur and Nathalie Alisa Smuha, 'Quatre nuances de régulation de l'intelligence artificielle: Une cartographie des conflits de définition' (2022) 232–233 Réseaux 29.

definition. To recap, AI is defined as a "*machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*".[196]

Recital 12 of the AI Act clarifies that this covers knowledge- and data-driven methods alike. However, more narrowly than in the original proposal, it excludes from this definition "*simpler traditional software systems or programming approaches*" and "*systems that are based on the rules defined solely by natural persons to automatically execute operations*". It remains to be seen how this definition will be interpreted by the AI Act's implementers, but the recital raises doubts as to whether the algorithmic systems that are the subject of this book all fall under the AI Act's scope.[197] Throughout this section, I will assume it can reasonably be argued that they do, and use the term 'AI' interchangeably with algorithmic systems used for algorithmic regulation.

I do wish to stress, however, that this narrowing of AI's definition is rather unfortunate, as it creates the risk that harmful algorithmic systems can escape the AI Act's requirements through definitional gaps. This limitation is also unnecessary. Indeed, a broad definition of AI could have easily been maintained, since the systems that fall under the scope of the Act's requirements are not solely defined by this definition, but also by the regulation's specific provisions that categorise AI systems and impose different obligations per category. If the legislator's main focus had been the values it seeks to protect and the harmful conduct it wishes to avoid, it would not have mattered as much through which underlying algorithmic technique such harm occurred.

Let me also point out that the AI Act introduces a definition of general-purpose AI models, or models that are trained with a large amount of data using self-supervision at scale, that display significant generality and that are capable of "*competently performing a wide range of distinct tasks regardless of the way the model is placed on the market*" while also capable of being integrated into a variety of downstream systems or applications.[198]

[196] Article 3(1) AI Act.

[197] One can, for instance, wonder whether the Dutch system discussed under Section 4.1.4 to identify fraud based on blatantly discriminatory criteria (such as whether the individual is a taxi driver or hairdresser, or how high their level of education is) is still part of the AI Act's definition, as it concerns essentially a rule-based system with pre-defined rules and criteria that are automatically executed.

[198] See Article 3(63) AI Act. Unfortunately, this definition excludes "*AI models that are used for research, development or prototyping activities before they are placed on the market*". Since the AI Act was initially proposed before the launch of ChatGPT, when generative AI applications were not yet on the Commission's radar, there was no mentioning thereof in its original version. Yet the broad uptake of such applications during the AI Act's negotiations rendered their inclusion much more pressing, resulting in a new set of distinct requirements.

Finally, the regulation also introduces certain exceptions. AI systems and models that are developed and put into service for the sole purpose of scientific research and development fall outside its scope, as do systems that are used for national security, military and defence purposes. An exception also exists for AI systems that are released under free and open-source licences, unless they are placed on the market or put into service for a purpose that falls under one of the AI Act's explicit categories, which I will discuss next.[199]

5.4.2 *The AI Act's Regulatory Architecture*

There are many different ways of regulating (human behaviour related to) AI systems.[200] The drafters of the AI Act have let themselves be inspired by product (safety) legislation[201] instead of, for instance, legislation dealing with the protection of fundamental rights. The regulation hence treats AI as a product or service that must adhere to certain (primarily technical) requirements, meticulously set out in the regulation. The High-Level Expert Group's recommendation to adopt a principle-based approach to AI's regulation rather than an overly prescriptive one[202] has thus not been taken up. The legislator did take up the group's suggestion for a risk-based approach, by distinguishing different categories of AI systems based on the extent of risk[203] they raise to health, safety and fundamental rights,[204] and imposes different obligations for each risk category. The regulation's emphasis on *obligations*

[199] Article 2(12) AI Act.

[200] See also Nicolas Petit and Jerome De Cooman, 'Models of Law and Regulation for AI' in Anthony Elliott (ed), *The Routledge Social Science Handbook of AI* (Routledge 2021) 199.

[201] The AI Act is based on the New Legal Framework, which was adopted in 2008 and consists of three EU measures that are meant to improve the market surveillance of products and enhance the quality of conformity assessments: (1) EC Regulation No 765/2008 on accreditation and marketing surveillance; (2) Decision No 768/2008/EC on establishing a common framework for the marketing of products; and (3) EC Regulation No 764/2008 to strengthen the internal market for a wide range of other products not subject to EU harmonisation.

[202] See High-Level Expert Group on AI, 'Policy and Investment Recommendations for Trustworthy AI' (n 176) 38.

[203] Risk is defined in Article 3(2) AI Act as "*the combination of the probability of an occurrence of harm and the severity of that harm*". This definition has been criticised by scholars like Mireille Hildebrand, for when it comes to fundamental rights, the danger is the 'breach' of a right rather than 'harm'. It would hence be important to interpret this risk definition as also encompassing risks to rights breaches (and breaches of individual, collective and societal interests more generally).

[204] In its recitals, the regulation sparsely states that democracy, the rule of law and the environment are also values it seeks to protect. However, its substantive articles clarify that the risks it focuses on are primarily assessed in terms of their impact on health, safety and fundamental rights. This also explains, for instance, why certain systems – despite being included in the high-risk list – can still escape the high-risk obligations when they do "*not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making*". See Article 6(3) AI Act.

for AI providers and deployers, with only a very limited number of new *rights* for those subjected to the systems, further reflects its market-oriented vision.

The AI Act distinguishes five[205] categories:

(1) AI practices that pose an unacceptable level of risk and that are hence prohibited (with exceptions) (*chapter II of the Act*);
(2) AI systems that must comply with a set of requirements due to posing a high risk to health, safety or fundamental rights, and that must undergo a conformity assessment prior to their use or placement on the market (*chapter III of the AI Act*). These consist of two subcategories: a) AI systems that are (incorporated into products that are) already subjected to existing product safety legislation (Annex I of the AI Act); and (b) 'stand-alone' AI systems (Annex III of the AI Act);
(3) AI systems subjected to additional transparency obligations due to their risk of deceit or intrusiveness (*chapter IV of the AI Act*);
(4) General-purpose AI models, including a sub-category of models that pose a systemic risk due to their scale and capabilities (*chapter V of the AI Act*); and
(5) AI systems that are considered to pose only a minimal or no risk.

The last one is a residual category, including all systems and practices that are not explicitly listed under one of the other categories. These systems are not subjected to any new requirements, but can become the object of voluntary codes of conduct and guidelines (*chapter X of the AI Act*). AI systems that fall under the first four categories are described and listed either directly in the AI Act's text or – in the case of high-risk systems – in annexes that can be updated over time.[206] The AI Act's drafters hence coupled a *risk-based* approach with a *list-based* approach, to which I will come back later.

Categories and their requirements can overlap. Some systems can, for instance, be subjected to both the requirements imposed on high-risk systems and to the

[205] Originally, four such categories were proposed, which the Commission eagerly represented by reference to a pyramid to stress that only a small number of systems are subjected to strict requirements, and that "*the vast majority of AI systems*" (those represented by the large base of the pyramid) are not subjected to any new requirements. See European Commission, 'Press Release – Europe Fit for the Digital Age: Commission Proposes New Rules and Actions for Excellence and Trust in Artificial Intelligence' (Brussels, 21 April 2021) <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682>. A similar pyramidal approach had already been put forward by the German Data Ethics Commission, who differentiated five risk levels necessitating different regulatory requirements. See 'Opinion of the German Data Ethics Commission' (Data Ethics Commission of the Federal Government 2019). Over time, it became clear, however, that a pyramidal structure did not fit the bill to visualise the AI Act, as certain categories were overlapping, the new category of 'general-purpose AI models' was difficult to place, and the quantity of AI systems listed in certain categories did not always correspond to their place in the pyramid.

[206] See Article 7 AI Act.

additional transparency obligations. AI providers and deployers must self-assess the category under which their AI system falls. For high-risk systems listed in Annex III, they can even self-assess whether their system – though listed in the annex – is nevertheless exempt from the high-risk requirements if it, in their view, "*does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making*".[207] Coupled with the fact that the conformity assessment of virtually all high-risk systems can be carried out by the systems' providers themselves, this provides a high 'margin of appreciation' for the very actors the AI Act is supposed to regulate – a highly contentious point to which I will return.

Before discussing which applications of algorithmic regulation fall under the AI Act's respective categories, let me also briefly describe how the AI Act's requirements are enforced. The enforcement architecture of the AI Act is relatively complex, and involves several actors at different levels. The main action takes place at the national level. Member States must establish or designate an independent national competent authority (the role of which can also be undertaken by the data protection authority) to oversee the AI Act's requirements.[208] These take on the role of notifying authorities[209] and market surveillance authorities,[210] with the possibility for Member States to appoint different authorities for each task[211] as long as there is a "*single point of contact*".[212] The authorities' oversight primarily takes place ex post, when an investigation reveals that an AI provider or deployer did not comply with the regulation. To coordinate the activities of the national authorities, the AI Act also establishes a European AI Board, composed of Member States' representatives.[213]

While the Commission's initial proposal was limited to the above, both the Council and the Parliament underlined the need for a stronger enforcement role at the level of the EU, especially for systems that affect the EU population at large or

[207] Article 6(3) AI Act.

[208] See Article 70(1) AI Act.

[209] Notifying authorities play a role in the enforcement process of high-risk systems in particular. Pursuant to Article 28 of the AI Act, they are responsible for setting up and carrying out the necessary procedures for the assessment, designation and notification of conformity assessment bodies ('notified bodies') and for their monitoring. These bodies can act as an independent third-party that carries out conformity assessments of high-risk systems when system providers do not need or wish to do so themselves. Notified bodies must first submit an application for notification to the notifying authority, who will verify that they meet the conditions set out in Article 31 AI Act.

[210] Market surveillance authorities play the role of supervisory authority, and monitor organisations' compliance with the AI Act's requirements more generally. Often, the same authority will take on the role of both notifying authority and market surveillance authority.

[211] Article 70(1) AI Act.

[212] Article 70(2) AI Act

[213] Article 65 of the AI Act. Moreover, the European Data Protection Supervisor participates in the Board as an observer.

that cannot easily be monitored by individual states. This resulted in the establishment of an AI Office, housed at the European Commission.[214] The AI Office is responsible for the enforcement of the requirements imposed on general-purpose AI models. Moreover, it provides the secretariat for the Board, convenes the Board's meetings, and prepares its agenda.[215] To further complicate the landscape of relevant actors, Articles 67 and 68 also respectively set up an Advisory Forum and a Scientific Panel of Independent Experts. The former consists of a group of stakeholders that provide expertise and advice to the Board and the Commission.[216] The latter consists of experts that advise and support the AI Office in its enforcement tasks,[217] for instance by alerting it of possible systemic risks posed by general-purpose AI models or by developing methodologies to evaluate their capabilities.

Finally, let me point out three more characteristics of the AI Act's architecture. First, to expedite compliance monitoring of the Regulation's obligations, the AI Act establishes an EU-wide database, managed by the European Commission,[218] in which certain providers and deployers of AI systems need to register some basic information. Second, given the importance the EU attaches to AI-enabled innovation, the AI Act also provides measures 'in support of innovation', by setting up regulatory sandboxes in every Member State.[219] Third, compliance with the AI Act's requirements is facilitated by the establishment of harmonised standards (or common specifications).[220] Conformity therewith offers a presumption of conformity with the AI Act, which means that, in practice, the standards' interpretation of the AI Act's requirements can become the regulation's de facto authority. This approach is not without criticism, as European Standardisation Organisations are primarily populated by industry actors and technical experts, with little participation from civil society organisations and experts with an ethical or legal background.[221] More generally, one can also question whether requirements that are meant to ensure

[214] See Article 64 AI Act. Over time, the Office could be turned into a full-fledged Union agency if the Commission's evaluation of the Regulation's enforcement (which should be carried out seven years from the date of its entry into force) reveals enforcement shortcomings. See Article 112(13) AI Act.

[215] Article 65(8) AI Act.

[216] Article 67(1) AI Act.

[217] The scientific panel can also support the work of market surveillance authorities, pursuant to Article 68(3).

[218] Article 71 AI Act.

[219] Article 57 and following AI Act.

[220] Article 40 AI Act. In the absence of harmonised standards, the Commission can also adopt common specifications for the AI Act's requirements pursuant to Article 41 AI Act.

[221] See Nathalie A Smuha and Karen Yeung, 'The European Union's AI Act: Beyond Motherhood and Apple Pie?' in Nathalie A Smuha (ed), *The Cambridge Handbook of the Law, Ethics and Policy of AI* (Cambridge University Press). See also Joanna J Bryson, 'Belgian and Flemish Policy Makers' Guide to AI Regulation', KCDS-CiTiP Fellow Lectures Series: Towards an AI Regulator?, Leuven, 11 October 2022.

AI systems' alignment with fundamental rights can ever be captured by a set of technical standards.[222]

In what follows, let me now zoom in on the AI Act's merits and pitfalls specifically in the context of algorithmic regulation, and the risks it poses to the rule of law.

5.4.3 *Algorithmic Regulation in the AI Act*

To what extent is algorithmic regulation as defined in this book – namely reliance on algorithmic systems *to inform or take administrative acts* – covered by the AI Act? At the outset, it can be noted that the AI Act does not fundamentally distinguish between systems used by the private and the public sector when it comes to the *requirements* it imposes on AI systems. In most cases, these requirements are the same, regardless of whether a system is deployed by a private or a public actor. There are two notable exceptions: the obligation for public authority deployers to register the high-risk systems they use in the EU database, and the obligation to carry out a fundamental rights impact assessment pursuant to Article 27 of the AI Act.[223] That said, applications of algorithmic regulation can be found in all of the AI Act's categories, either explicitly (when a categorised system serves to inform or adopt administrative acts) or implicitly (when a categorised system *can* serve this purpose).

5.4.3.a Prohibited Practices

Article 5 of the AI Act enumerates eight practices that are prohibited in light of the unacceptable risk they pose.[224] Focusing only on the practices that are most relevant for the public sector, the AI Act prohibits generalised social scoring to evaluate or classify people based on their social behaviour (or based on their known, inferred or predicted characteristics), though only if it leads to their detrimental or unfavourable treatment in social contexts that are unrelated to those in which the data was collected, or to an unjustified or disproportionate treatment.[225] It also prohibits the use of AI systems to carry out risk assessments of natural persons that assess or predict the risk of a criminal offence based solely on the person's profiling or the assessment of her personality traits and characteristics. However, the prohibition does not apply

[222] For an extensive critique of this approach, see ibid.

[223] This obligation only applies to deployers of high-risk AI systems that are governed by public law, that provide public services, that evaluate people's creditworthiness or that analyse risks and prices relating to life and health insurance.

[224] The first two concern the subliminal manipulation of persons or groups or the exploitation of their vulnerabilities due to their age, disability or social or economic situation in a way that materially distorts their behaviour and can cause significant harm. Article 5(1)(a) and (b) AI Act. For a discussion on this topic, see also Rostam J Neuwirth, *The EU Artificial Intelligence Act: Regulating Subliminal AI Systems* (Routledge 2022).

[225] Article 5(1)(c) AI Act. While the Commission proposed such a prohibition only for public authorities, the Council and Parliament decided to expand this provision to private actors too.

to systems used "*to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity*".[226]

Public and private actors are also not allowed to use AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage,[227] or to use biometric categorisation systems that individually categorise natural persons based on their biometric data to infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation. They can, however, still use the latter systems to infer other traits (as long as they comply with the GDPR and the LED), nor does this prohibition cover the "*labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement*", which is hence exempt therefrom.[228]

No prohibition is foreseen for public authorities' use of emotion recognition systems,[229] despite the fact that their use is scientifically so unsound that it is nearly impossible to come up with a single legitimate purpose for authorities to rely thereon.[230] Moreover, the prohibition on the use of facial recognition (or biometric identification systems) is so limited that it hardly merits this designation. It only applies to 'remote' and 'real-time' biometric identification, only in publicly accessible spaces, and only for the purposes of law enforcement (and thus not for the purposes of e.g. border control or other areas of public administration).[231] Furthermore, even this limited prohibition is subjected to exceptions, as remote biometric identification systems can still be used for the targeted search of victims or missing persons, the prevention of certain imminent threats, and the localisation or identification of (even) suspects of some criminal offences.[232]

Undoubtedly, this list of practices (very limited and full of exceptions) risks being incomplete, both in terms of problematic AI practices that already exist today, and

[226] Article 5(1)(d) AI Act.

[227] Article 5(e) AI Act.

[228] Article 5(g) AI Act.

[229] Pursuant to Article 5(f), these are only prohibited "*in the areas of workplace and education institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons*".

[230] See, e.g., Thomas Bøgevald Bjørnsten and Mette-Marie Zacher Sørensen, 'Uncertainties of Facial Emotion Recognition Technologies and the Automation of Emotional Labour' (2017) 28 Digital Creativity 297; Lisa Feldman Barrett and others, 'Emotional Expressions Reconsidered: Challenges to Inferring Emotion from Human Facial Movements' (2019) 20 Psychological Science in the Public Interest 1.

[231] Article 5(h) AI Act.

[232] ibid. To make use of these exceptions, Article 5(2) does set out a number of safeguards that law enforcement authorities must implement, including the need to carry out a fundamental rights impact assessment and the need to request prior authorisation from a judicial authority or an independent administrative authority (though also there, exceptions are foreseen in case of a "*duly justified situation of urgency*").

practices that may pop up in the next few years. Article 5 will be subjected to a periodic assessment by the Commission of the need for amendments, which will be submitted to the Parliament and the Council. However, the only way to amend this list in practice would be to re-subject the regulation to the ordinary legislative procedure, which is unlikely to occur within the near future.

5.4.3.b Systems Requiring Additional Transparency

Three types of systems have additional transparency obligations, which in essence entail the mandatory disclosure that a person is subjected to such a system. First, systems that directly interact with natural persons – such as chatbots, which are increasingly used by public authorities to 'more efficiently' provide citizens with information – must be developed in such a way that people are informed they are interacting with an AI system.[233] Second, whenever public authorities deploy algorithmic systems for the purpose of emotion recognition or biometric categorisation, they are likewise required to inform individuals of the fact that they are being subjected thereto.[234] Last, the Article also imposes disclosure obligations on providers and deployers of systems that generate synthetic data or deepfakes, whether it concerns audio, image, video or text content.[235]

Note how, in line with the AI Act's focus on product requirements, this Article merely imposes obligations on AI providers and developers, rather than granting individuals a *right* to be informed. Furthermore, all of these provisions have exceptions where the system's use "*is authorised by law to detect, prevent, investigate or prosecute criminal offences*". Finally, it can be noted that this Article does not seem to be the object of a robust targeted periodic assessment or revision process.

5.4.3.c General-Purpose AI Models

The AI Act also imposes a set of obligations on providers of general-purpose AI models. Virtually all those providers are private actors, rendering these obligations less relevant for public authorities. That said, a growing number of authorities have started using systems that incorporate general-purpose AI models – referred to as 'general-purpose AI systems' in the AI Act – such as chatbots that help citizens to retrieve information, answer questions or fill in forms. This means these requirements are nevertheless relevant whenever authorities procure or develop such systems, especially for a high-risk purpose.

[233] Article 50(1) AI Act. An exception to this obligation is foreseen if "*this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use*".

[234] Article 50(3) AI Act. The same, however, holds true for the private use of such applications, once again diminishing the distinction between private and public actors.

[235] Article 50(2) and 50(4) AI Act.

The AI Act's requirements for general-purpose AI models mainly concern tailored transparency measures to enable downstream AI providers that rely on those models to comply with their own obligations under the AI Act. Providers of such models must, for instance, draw up and keep up to date the model's technical documentation, including its training and testing process and the results of its evaluation.[236] They must also adopt a policy to ensure compliance with copyright law, and make available certain information and documentation to AI providers who intend to integrate the general-purpose AI model into their system (including information that enables those providers to have a good understanding of the capabilities and limitations of the model and to comply with their obligations under the AI Act).[237] In addition, they must make publicly available "*a sufficiently detailed summary about the content used for training of the general-purpose AI model, according to a template provided by the AI Office*".[238] Only the latter information is made accessible to the public at large, thus limiting the information that will be accessible for citizens who wish to learn more about the models underlying the systems used by public authorities.

As a reflection of the legislator's risk-based approach, providers of general-purpose AI models that pose a 'systemic risk' are subjected to additional obligations. These models must be notified to the Commission in order to be designated as such, akin to the gatekeeper designation process established by the Digital Markets Act.[239] General-purpose AI models that pose a systemic risk are defined as having "*high impact capabilities evaluated on the basis of appropriate technical tools and methodologies, including indicators and benchmarks*".[240] What, precisely, counts as a systemic risk is not defined. Furthermore, despite the constantly evolving nature of AI systems' computational capabilities, the drafters of the AI Act oddly enough decided to introduce a presumption of such capabilities "*when the cumulative amount of computation used for its training measured in floating point operations is greater than* 10^{25}". This rather arbitrary threshold can be amended by the Commission through delegated acts to ensure it keeps reflecting "*the state of the art*".[241]

Providers of general-purpose AI models must also perform model evaluations (including adversarial testing), and assess and mitigate possible systemic risks at Union level. They must report to national competent authorities any relevant information about serious incidents and corrective measures to address them, and

[236] See Article 53(1)(a) AI Act. The information that should be documented is set out in Annex XI of the Act.

[237] Article 53(1)(b) AI Act. The information that should be shared with those providers is set out in Annex XII of the Act.

[238] Article 53(1)(d) AI Act.

[239] Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives 2019/1937 and 2020/1828, OJ L 265, 12 October 2022.

[240] Article 51(1) AI Act.

[241] Article 51(1) and (3) AI Act.

ensure an adequate level of cybersecurity protection for the model and its physical infrastructure. Interestingly, despite the systemic risks they pose, and their use and integration by countless downstream providers and deployers (including public authorities), none of these obligations introduces the need for an independent verification of the model's compliance with EU law prior to its use.

5.4.3.d High-Risk Systems

Let me now turn to the category that is most relevant for the context of algorithmic regulation, namely high-risk AI systems. While the requirements that apply to such systems (listed in Articles 8 to 15 AI Act) are the same when it concerns a public or a private entity, Annex III does list numerous AI systems that are solely used in the public sector, reflecting the legislator's recognition that many such uses merit heightened attention and responsibility, given the asymmetrical power relationship between public authorities and individuals.

Annex III lists eight domains or purposes for which AI systems can be used. To be considered high-risk, a system must be explicitly listed as a use-case under one of the eight domain headings. While these lists can be updated by the Commission,[242] the headings themselves can only be altered by amending the regulation.[243] In other words, if an AI system does not fall under any of the eight listed domains, despite posing a high risk, it cannot be categorised as such without revisiting the entire legislative process.

Applications of algorithmic regulation covered by Annex III include, under the heading of 'biometrics' systems used for remote biometric identification, for biometric categorisation based on sensitive or protected attributes, and systems used for emotion recognition.[244] The heading of 'critical infrastructure' is relevant too, for it includes systems "*intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity*".

Under the domain of 'education and vocational training', systems used for student admissions, to assign them to educational institutions, and to evaluate their learning outcomes are considered high risk. Returning to the illustrations of Chapter 4, this means that a system that would be similar to Ofqual's algorithm in the UK or the Admission Post Bac algorithm in France would be covered. The domain also includes systems to monitor and detect prohibited behaviour of students during tests, and to assess the level of education that an individual should receive or

[242] Article 7 AI Act sets out a procedure for this purpose, enabling the Commission to adopt delegated acts (pursuant to Article 97 AI Act) to add, modify or delete use cases of high-risk AI systems when certain conditions are fulfilled.

[243] See Article 112(11)(a) AI Act.

[244] Annex III, 1 AI Act. Systems that are merely used for biometric *verification* purposes are excluded from the high-risk list.

access.[245] To the extent public authorities rely on algorithmic regulation in recruitments, promotions, dismissals and the monitoring and evaluation of public officials, this is likewise considered as high risk, under the heading 'employment, workers management and access to self-employment'.[246]

Many of the other examples discussed in Chapter 4 fall under the heading 'access to and enjoyment of essential private services and essential public services and benefits'.[247] This includes systems used to evaluate the eligibility of natural persons for essential public assistance benefits and services, as well as systems to grant, reduce, revoke or reclaim them.[248] Furthermore, systems used to dispatch or to establish priority in the dispatching of emergency first response services by police, firefighters and medical aid (including emergency healthcare) are likewise included.[249]

As regards 'law enforcement', which has a separate heading, the annex covers an array of applications, including systems used to make an assessment of the risk of natural persons (re)offending or becoming victims of criminal offences, and systems used to profile natural persons in the course of criminal investigations. The list also includes systems that are used as polygraphs, and systems used to evaluate the reliability of evidence during investigations.[250]

AI applications for 'migration, asylum and border control management' are grouped under a separate heading, and include inter alia systems to assess risks related to security, irregular migration and the health of individuals; systems to examine applications for asylum, visa and residence permits, and to examine complaints associated thereto; systems used to assess the reliability of evidence; and systems used to detect, recognise or identify individuals. In addition, notwithstanding their scientific unsoundness, systems used as polygraphs or to detect the emotional state of natural persons are also included in this list rather than being prohibited, despite the highly vulnerable state of the individuals subjected thereto.[251]

The last heading of the annex is titled 'administration of justice and democratic processes'.[252] This includes two sets of systems: those used by a judicial authority to assist it with researching and interpreting facts and the law and applying the law to a concrete set of facts, and those used to influence the outcome of an election or referendum (or people's voting behaviour). Interestingly, in its position on the AI Act, the Parliament also suggested including AI systems used by an *administrative*

[245] Annex III, 3 AI Act.

[246] Annex II, 4 AI Act.

[247] Annex III, 5(a). Note how the word 'essential' was added before 'public services' during the AI Act's negotiations, raising the question whether a system used in the context of a service that a public authority does not consider as 'essential' might escape the list.

[248] Annex III, 5(a) AI Act.

[249] Annex III, 5(d) AI Act.

[250] Annex III, 6 AI Act.

[251] Annex III, 7 AI Act.

[252] Annex III, 8 AI Act.

body or on their behalf (and hence not only by a judicial authority) to research and interpret facts and the law, and apply the law to a concrete set of facts. This could have been an important addition, as it would have provided a broader basis to cover algorithmic regulation applications under the high-risk list. The Parliament's suggestion, however, was rejected, leaving out of scope decisions taken by administrative authorities under this heading.

Let me pause here for a moment and make some observations. The systems listed above are without a doubt liable to cause adverse effects on the rights and interests of individuals (and society) if not used responsibly. The fact that they are listed as 'high risk' and that they will be subjected to mandatory requirements which need to be fulfilled *before* their use is hence a positive development. However, as already hinted at, some of these applications can reasonably be found to pose an 'unacceptable' risk rather than a 'high' risk, and their use, especially in a public sector context, may merit being prohibited altogether.[253]

Second, this list appears to be legitimising the use of the systems it contains, as it provides that their use, though risky, is acceptable as long as the requirements attached thereto are fulfilled. Accordingly, public deliberation about whether certain of these applications should be used in the first place risks being bypassed. Some of these applications may require, in consonance with the GDPR, a separate legal basis in the form of a legislation that sets out the permissible uses of the technology, which would at least enable parliamentary debate and hence some level of democratic oversight prior to their implementation.[254] This, however, may not be the case for all these systems, and in any case depends on how (well) Member States fulfil their obligations under the GDPR, and how they interpret concepts like the 'public interest'.

Third, I have already noted that the requirements these high-risk systems must meet (discussed in more detail in the next section) are subjected to a conformity *self*-assessment. This means the AI Act foresees no *independent ex ante* oversight over why or how these systems are designed and used, despite the significance of the impact they can have when deployed at scale by public authorities.[255] On the one

[253] See Smuha and others (n 189) 30. After the Commission's proposal came out, various civil society organisations started campaigning not only to include in the Act a full ban on facial recognition, but also a ban on predictive policing more generally. See also 'AlgorithmWatch Signs Statement on Ban of Predictive Policing in the Artificial Intelligence Act' (*AlgorithmWatch*, 1 March 2022) <https://algorithmwatch.org/en/ban-predictive-policing-aia/>.

[254] Recall in this regard the abovementioned discussion of the SyRi system used in the Netherlands, where a national court found that the system's legal basis as described in the relevant national legislation was not sufficiently precise to justify its use. Accordingly, in some cases, the GDPR also provides some level of protection in this regard (yet this will depend on the legal basis based on which the data processing takes place). See *supra*, Section 5.3.1.

[255] Pursuant to Article 43(1) AI Act, this is only different for the high-risk systems listed under point 1 of Annex III, which in principle have to undergo a third party conformity assessment (set out in Annex VII). Exceptions are, however, foreseen in cases where the provider applies harmonised standards or common specifications. For the systems listed under points 2 to 8 of Annex III, an internal control mechanism (set out in Annex VI) suffices. See Article 43(2) AI Act.

hand, their inclusion in the high-risk annex signals the acknowledgement that the risk associated with these systems is *high*. On the other hand, however, independent oversight over their use and sound development is only possible ex post and, meanwhile, the system can simply be self-assessed (often by people who, as was already discussed above, have little clue about the intricacies of the application of general legal rules to specific cases).

Finally, this list-based approach to applications that constitute a high risk is deeply problematic, as it is bound to be under-inclusive, by overlooking other algorithmic systems that can *also* have an adverse impact on individual, collective and societal interests.[256] Why did the legislator not opt to include *all* algorithmic systems used to inform or adopt administrative acts? Can it not be reasonably argued that these systems are by definition 'high risk'? Or even more broadly, could one not consider including all systems that can have an adverse impact on fundamental rights, the democratic process and the rule of law? Undoubtedly, such broader formulation provides less legal certainty for providers and deployers subject to the AI Act. Would it not, however, offer more protection for individuals subjected to the adverse effects of algorithm regulation? In Chapter 4, I discussed the importance of letting the law play its role. This includes embracing its inherent tensions, and the push-and-pull marriage between discretion and rules, flexibility and stability, vagueness and precision, openness and closeness. The list-based approach of the AI Act, unfortunately, risks overly emphasising the latter.[257] This is worrisome since, as noted above, a legalistic approach tends not to lead to justice, but to legalism.

What is more, during the negotiations, the EU legislator included a provision that introduces a so-called filter for high-risk systems, which enables the circumvention of the high-risk requirements if system providers can argue that – despite falling under Annex III – their particular AI application does *not* pose a significant risk of harm to the health, safety or fundamental rights of natural persons. Accordingly, even if a system is classified as high risk by the AI Act, system providers can avoid the high-risk requirements if they *self*-assess that their system does not pose a significant risk.[258] To avoid abuse of this potential escape route, the AI Act does provide a

[256] See Smuha and others (n 189) 29. One could also point out the risk that this list is over-inclusive, but the additional exemptive layer that the Parliament and Council introduced when finalising the AI Act significantly decreases that risk.

[257] Admittedly, the Parliament did suggest including a set of general principles that are applicable to all AI systems, regardless of whether they appear on the high-risk list. These principles would have corresponded to the High-Level Expert Group's requirements for Trustworthy AI, whereby all actors falling under the AI Act would have had to 'make their best efforts' to develop and use AI systems in accordance therewith. This suggestion has, however, not been taken up in the final version of the AI Act, except for Recital 27 of the AI Act, which briefly mentions the Expert Group's seven requirements and notes that these "*should be translated, when possible, in the design and use of AI models*" and "*serve as a basis for the drafting of codes of conduct under this Regulation*".

[258] Article 6(3) AI Act. This article, along with Recital 53, further specifies the circumstances that would justify such an exclusion (e.g. the system is used to perform "*a narrow procedural task*",

procedure through which providers should justify their (rebuttable) exclusion from the high-risk requirements, and they still need to register their system in the EU database. Nevertheless, while the aim of this additional layer is to mitigate the over-inclusiveness of the high-risk list (yet not the under-inclusiveness), it will likely only add to the complexity of this Act's regulatory architecture, lead to more red tape, and diminish legal certainty for all those involved.[259]

For the sake of continuing my analysis, let me now, temporarily, bracket these concerns and examine the applications of algorithmic regulation that the AI Act *does* designate as high risk, arguably constituting the most relevant category in this context. To which extent do the requirements imposed on such systems provide protection against their adverse impact, particularly on the rule of law?

5.4.4 *High-Risk Algorithmic Regulation*

5.4.4.a Requirements for High-Risk Systems

Chapter III of the AI Act sets out the requirements that high-risk applications must comply with before being placed on the market or put into service. Article 9 provides that a 'risk management system' be established, implemented, documented and maintained, as part of a continuous iterative process running through the entire lifecycle of the system. This compels AI providers inter alia to identify and analyse the known and reasonably foreseeable risks associated with the system; to estimate and evaluate the risks that may emerge when the system is used in accordance with its intended purpose and 'under conditions of reasonably foreseeable misuse'; and to adopt 'appropriate and targeted risk management measures'.[260] The systems also need to be tested to identify the most appropriate risk management measures, based on their 'intended purpose'.[261]

Reflection on and documentation of those elements is to be welcomed. At the same time, technical developers that are not trained in concepts like fundamental rights and the rule of law will hardly be able to identify risks pertaining thereto. The proper identification of such risks, which enables subsequent measures of

"*to improve the result of a previously completed human activity*" or to "*perform a preparatory task to an assessment relevant for the purposes of the use cases listed in* Annex III").

[259] Unsurprisingly, the European Parliament's Legal Service also issued a 'damning' opinion on this addition, raising inter alia legal certainty as a core concern. This, however, did not stop the AI Act's negotiators from keeping it in. See in this regard Lucca Bertuzzi, 'AI Act: EU Parliament's Legal Office Gives Damning Opinion on High-Risk Classification "Filters"' (*Euractiv*, 19 October 2023) <www.euractiv.com/section/artificial-intelligence/news/ai-act-eu-parliaments-legal-office-gives-damning-opinion-on-high-risk-classification-filters/>

[260] See Article 9(2) AI Act. Such risk-assessments are frequently deployed as a regulatory solution also in other contexts, yet they are not devoid of criticism. For a critical examination thereof in the area of environmental protection, see, e.g., Kathleen Garnett, 'Novelty, Ignorance and the Unknown: Uncertain Science and the Frontiers of Science Doctrine' [2021] elni Review 11.

[261] Article 9(6) AI Act.

mitigation, necessarily requires input from others, including public officials who are trained in the law's application and who will be using the system, people with expertise about the ethical and legal impact of algorithmic systems and, most importantly, those who will be subjected to the system or can be adversely affected thereby. Unfortunately, the AI Act does not foresee the need to seek input and feedback from domain experts or from those who may be adversely impacted.

It can also be noted that Article 9(3) limits the risks that must be considered to "*those which may be reasonably mitigated or eliminated through the development or design of the high-risk AI system, or the provision of adequate technical information*". One can wonder what this means for risks that cannot be mitigated through the development and design of the system or by providing technical information. Are those risks simply to be ignored? Furthermore, Article 9(5) provides that any 'relevant residual risk' that cannot be eliminated or mitigated, as well as the 'overall residual risk' of the system, must be judged 'acceptable'. The judgment of whether or not a residual risk is acceptable hence resides solely with the system's coders, not with those who will be subjected thereto. Yet, as noted elsewhere, outsourcing the 'acceptability' of 'residual risks' to high-risk AI providers is hardly acceptable.[262]

As regards the requirement pertaining to data governance, Article 10 requires that the training, validation and testing data sets are subjected to appropriate data governance and management practices, which must include in particular: the relevant design choices; data collection processes; data preparation operations; the formulation of assumptions (with respect to the information that the data are supposed to measure and represent, which can be understood as the 'proxies' that are being used); an assessment of the availability, quantity and suitability of the data sets that are needed; the examination of possible biases as well as measures to detect and mitigate those biases; and the identification of relevant data gaps or shortcomings.[263] Furthermore, data sets must be relevant, sufficiently representative and 'to the best extent possible' free of errors and complete in view of the intended purpose. They should also have 'appropriate statistical properties', including as regards the persons or groups in relation to whom the system is intended to be used.[264] These elements (though not specific to the public sector) could in theory help provide insight into how legal provisions are being translated to code in the context of algorithmic regulation, as they force coders to be explicit about the design choices they make and the relevant assumptions underlying their 'translations'. There is, however, a catch.

First, this information need not be made public. Arguably, providers need to draw up technical documentation pursuant to Article 11 AI Act, which demonstrates that the system complies with the requirements. However, that documentation is only

[262] Smuha and others (n 189) 29. See also Smuha and Yeung (n 221).

[263] Article 10(2) AI act.

[264] Article 10(3) AI act.

meant to provide the relevant supervisory authorities with the necessary information to assess compliance ex post, in case an investigation ever arises. Citizens do not have access thereto, and it is not covered by the (rather minimalistic) information that providers and deployers are meant to include in the 'EU database of stand-alone high-risk systems'.[265] Arguably, if the provider is a public authority rather than a private company to which the system's development is outsourced (and perhaps also in that case), citizens could invoke a *national* right to access to information and submit an 'access to documents' request. However, as various illustrations in Chapter 4 have demonstrated, such a right does not always enable individuals to receive information about the system itself. More generally, the fact that such documentation is not rendered public-by-default whenever it concerns a system deployed to inform or take administrative acts is a missed opportunity. This may in part be due to the fact that the AI Act imposes a single set of requirements both to private and public actors, without acknowledging their crucial differences, particularly as regards the enhanced need of transparency in the public sector, which is meant to *controllably* act in the public interest.

Second, this article still leaves significant discretion to the system's coders. For instance, statistical properties should be 'appropriate', yet what that precisely means is left to the provider, and does not necessarily need to be spelled out or justified. Moreover, the formulation of relevant assumptions and proxies does not in itself prevent reliance on misguided proxies. As noted elsewhere, nothing in the AI Act seems to, for instance "*prevent public authorities from using arrest data as a proxy for crimes committed (while not all arrested persons are charged or convicted, and many crimes occur for which no arrests are made). Given that these assumptions are not publicly accessible, their misguided nature may not easily come to light.*"[266]

In order to enhance traceability and transparency, Article 12 requires record-keeping, while Article 13 imposes certain information obligations, requiring that high-risk systems be designed and developed in such a way to enable deployers to interpret a system's output and use it appropriately.[267] The system should also come with a set of instructions for use that provide, inter alia, information about the 'characteristics, capabilities and limitations of performance of the system'; 'foreseeable circumstances' that may lead to 'risks to the health and safety or fundamental

[265] See in this regard Annex VIII AI Act, which sets out the information that should be provided upon registration in the database, in accordance with Article 71. The AI Act's final version slightly expanded this list, which now includes not only a brief description of the system's intended purpose, but also of "*the components and functions*" it supports, as well as "*a basic and concise description of the information used by the system (data, inputs) and its operating logic*". Usefully, deployers that have a registration obligation must now also include a summary of the findings of their fundamental rights impact assessment pursuant to Article 27 (to which I will come back *infra*) and a summary of their data protection impact assessment pursuant to Article 35 GDPR or Article 27 LED.

[266] Smuha and others (n 189) 34.

[267] Article 13(1) of the AI Act.

rights'; 'when appropriate, its performance regarding specific persons or groups'; and human oversight measures (including technical measures) put in place to facilitate the interpretation out the system's output.[268] Note, however, that all this information is only meant to be provided to *deployers* of the system (*in casu*, the public officials who will be using it) rather than to those subjected to or affected by the system.[269] Once again, individuals adversely affected by algorithmic regulation have a much more limited role in the regulation.

Besides requirements around the accuracy, robustness and cybersecurity of the system in Article 15, and requirements of record-keeping and automatic logging in Article 12, the AI Act also contains a requirement on human oversight. Article 14 provides that high-risk systems should be designed and developed in a way that they can be effectively overseen by natural persons, and that such oversight should aim to "*prevent or minimise the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse*".[270] The oversight measures must be commensurate to the risks, autonomy level and context of the system's use, and should either be put in place by the provider or by the deployer (or both) depending on what is most appropriate. [271] Pursuant to Article 14(4) of the AI Act, the system's deployers must be enabled to understand the system's relevant capacities and limitations; to monitor its operation so as to detect and address anomalies and dysfunctions; to remain aware of their possible tendency of automation bias; to 'correctly' interpret the system's output; to decide not to use the system or to otherwise disregard, override or reverse its output; and to intervene in its operation or interrupt it through "a 'stop' button or a similar procedure that allows the system to come to a halt in a safe state".

The intention behind this provision is certainly to be applauded, as it is aimed at mitigating the risk of 'mindless rule-following' identified under Chapter 4. As such, it could help public officials maintain their agency and hence their sense of responsibility for the administrative acts taken or informed by algorithmic systems. However, in many instances, a meaningful failsafe is impossible to secure in practice, given that the entire premise of data mining is aimed at generating insight that is beyond the capacity of human cognition. This inevitably also means that the human being who needs to exercise oversight over the system will often not be able to second-guess the validity of the system's outputs, except in limited cases where human intuition may detect obvious failures or outliers. Moreover, the problem of automation bias is unlikely to be overcome through this provision, despite the laudable intentions.[272]

[268] Article 13(3) AI Act.

[269] See in this regard also Smuha and others (n 189) 34.

[270] Article 14(2) AI Act.

[271] Article 14(3) AI Act.

[272] Smuha and others (n 189) 35.

It would therefore be important to ensure that this provision does not remain a dead letter, and that besides 'technical measures', deployers also implement 'non-technical' oversight measures, such as adequate education and training for public officials,[273] logging oversight activities and easily accessible review and redress mechanisms. While much will depend on the internal organisation of public authorities (and the importance they attach to speed and efficiency KPIs), it is to be hoped that this provision can nevertheless contribute to a more responsible use of algorithmic regulation by providing some friction and a much-needed opportunity for critical internal reflection.

5.4.4.b Additional Obligations for Deployers

In the original proposal, most of the responsibilities for high-risk AI systems fell on system *providers*.[274] In the final version of the AI Act, this has been somewhat rebalanced to also include obligations for system *deployers*.[275] The former are chiefly responsible for the conformity assessment of their system with the above high-risk requirements (and the concomitant affixation of the CE marking),[276] setting up a quality management[277] and ensuring documentation keeping and automated logs,[278] while the latter must take technical and organisational measures to use the

[273] During the negotiations, the drafters of the AI Act included a new article on 'AI literacy', which survived the final text. Article 4 of the AI Act now states that

> providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

The Act also goes on to define AI literacy in Article 3(56) as "*skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause*".

[274] Pursuant to Article 3(3) AI Act, a provider is defined as "*a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge*".

[275] One of the main criticisms of the Commission's original proposal (especially made by large tech companies) was the 'unbalanced' imposition of obligation on providers of AI systems, who may not always be able to know or control in which (potentially problematic ways) the systems are subsequently used by deployers of the system. Article 3(4) AI Act defines a deployer as "*a natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity*".

[276] Providers must draw up a declaration of conformity in accordance with Article 47 AI Act and affix a CE marking to their high-risk system to indicate conformity with the regulation. See Articles 16 and 43 AI Act.

[277] Article 17 AI Act.

[278] Articles 18 and 19 AI Act.

system in accordance with the provider's instructions for use, ensure human oversight, monitor the system, and keep the system's logs.[279]

Interestingly, certain deployers have a few additional obligations.[280] First, all deployers of high-risk AI systems referred to in Annex III "*that make decisions or assist in making decisions related to natural persons*" shall inform those persons that they are subject to the use of such system.[281] This is a highly important (new) obligation, especially when coupled with two rights introduced in the AI Act: the right for individuals to lodge a complaint with a market surveillance authority if they believe the AI Act is not complied with,[282] and the right for individuals to receive an explanation of a decision taken about them,[283] of which the combination could facilitate redress. Second, deployers of a post-remote biometric identification in the context of a criminal investigation must obtain ex ante judicial or administrative authorisation to do so.[284] Third, deployers of high-risk systems who are public authorities must register their use of a high-risk system in the EU database to make such use known.[285]

Finally, public authorities that deploy high-risk AI systems must also undertake a fundamental rights impact assessment (FRIA).[286] This obligation was fiercely advocated for by civil society organisations throughout the AI Act's negotiations, and the Parliament ultimately managed to push it through in Article 27.[287] Inspired by the

[279] Article 26 AI Act.

[280] When a high-risk system is deployed at the workplace, deployers who are employers shall inform workers' representatives and the affected workers that they will be subject to the use of the high-risk AI system. See specifically Article 26(7) AI Act.

[281] Article 26(11) AI Act.

[282] Article 85 AI Act.

[283] Article 86 AI Act. It should, however, be pointed out that "*the right to obtain from the deployer clear and meaningful explanations of the role of the AI system in the decision-making procedure and the main elements of the decision taken*", only applies for a decision "*which produces legal effects or similarly significantly affects that person in a way that they consider to have an adverse impact on their health, safety or fundamental rights*". In theory, it is thus possible that a deployer has the obligation to inform individuals of the fact that they take a decision concerning them based on a high-risk system, without those individuals having the right to receive an explanation thereof if it cannot be said to produce legal effects or similarly affects them. Furthermore, Article 86(2) in any case precludes the right's application when exceptions are provided based on Union law or national law in compliance with Union law.

[284] The additional safeguards concerning post-remote biometric identification used in the area of criminal investigations can be found in Article 26(8) AI Act.

[285] The information they must provide is described in Annex VIII, section C. Apart from the deployer's contact details, it includes a summary of the findings of the fundamental rights impact assessment carried out under Article 27 of the AI Act and – where applicable – a summary of their data protection impact assessment.

[286] See Article 27 AI Act.

[287] See for instance European Center for Not-for-Profit Law (ECNL), 'Big Win for Fundamental Rights, as the European Parliament Adopts the AI Act' (ECNL 14 June 2023) <https://ecnl.org/news/big-win-fundamental-rights-european-parliament-adopts-ai-act>; Brussels Privacy Hub, 'More Than 150 University Professors from All Over Europe and Beyond Are Calling on the European Institutions to Include a Fundamental Rights Impact Assessment in the Future

concept of data protection impact assessments,[288] it is meant to force deployers to reflect on how their system can affect people's rights prior to its use, as well as to document and mitigate those effects. While this could constitute an important safeguard, the feedback gathered during the piloting phase of the Ethics Guidelines for Trustworthy AI revealed that most organisations, private or public, have no clue what such an assessment entails. Even for trained lawyers, assessing the impact of an AI system on all fundamental rights is not an easy task.

There are hence fears that this obligation will either be too difficult to comply with or, if interpretative guidance is provided, could turn into an empty box-ticking exercise leading to yet another façade of legality without any substantive protection. The latter unfortunately seems rather likely, since Article 27 provides a relatively rigid list of elements that the assessment should describe, and tasked the AI Office with developing "*a template for a questionnaire, including through an automated tool, to facilitate deployers in complying with their obligations under this Article in a simplified manner*". This reflects the legislator's desire to ensure the AI Act's measures can be implemented in an easy and straightforward manner, ideally with the help of some technical tools – even if there is nothing easy and straightforward about carrying out a proper assessment of the ways in which those systems can affect people's rights. This is an inevitably complex matter that requires the balancing of various interests and considerations, which cannot be bypassed through a simple checklist. Furthermore, the obligation's narrow focus on individual rights also neglects the societal interests that can be affected by such systems, especially by virtue of the systemic effects they can have on values like democracy and the rule of law.

5.4.5 *A Low Ceiling*

Considering these shortcomings, it is worth asking whether Member States can still remedy these gaps by adopting stronger safeguards through national legislation. In essence, this question comes down to whether the AI Act, and its aim to harmonise rules on algorithmic systems across the EU to establish an internal AI market, aspires a form of minimum or maximum harmonisation. Minimum harmonisation "*sets a common floor of regulation, which all Member States must respect, but it does not set a ceiling*", whereas maximum harmonisation "*serves as both floor and ceiling*".[289] The AI Act is directly applicable in national legal orders and

Regulation on Artificial Intelligence' (12 September 2023) <https://brusselsprivacyhub.com/2023/09/12/brussels-privacy-hub-and-other-academic-institutions-ask-to-approve-a-fundamental-rights-impact-assessment-in-the-eu-artificial-intelligence-act/>.

[288] Such an obligation was also already suggested by the High-Level Expert Group on AI in its Policy and Investment Recommendations (n 176) 40.

[289] Stephen Weatherill, 'Maximum versus Minimum Harmonization: Choosing between Unity and Diversity in the Search for the Soul of the Internal Market' in Niamh Nic Shuibhne and

Member States will need to ensure that individuals can benefit from the protection it affords.

However, can Member States go further than what the regulation requires and provide stronger safeguards against AI's adverse impact? If the AI Act seeks to ensure the maximum harmonisation of national rules, this would effectively prevent a Member State from addressing the AI Act's shortcomings, as that would be contrary to the regulation's objective and hence contrary to EU law.[290] As observed by Weatherill, this question thus expresses "*a battle for the soul of the internal market*",[291] as it essentially determines at which level regulatory power is held, and how much regulatory diversity the EU internal market can tolerate.

While the initial proposal of the AI Act still left the answer to this question somewhat ambiguous, the final version is more clear: "*This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation*".[292] It hence appears that the AI Act is targeting the maximum harmonisation of national legislation, and that Member States cannot provide a higher level of protection by adopting stricter rules, as this may cause unwanted 'market fragmentation'. There are only few exceptions such as the protection of workers, for which the regulation states that it "*does not preclude the Union or Member States from maintaining or introducing laws, regulations or administrative provisions which are more favourable to workers in terms of protecting their rights in respect of the use of AI systems by employers*".[293] This explicit exception only seems to confirm the regulation's ceiling-imposing nature.

In theory, a maximum harmonisation approach is meant to ensure an *equal* level of protection in all Member States. Yet in practice, given the AI Act's deficiencies, this may in fact come down to an *equally low* level of protection of the rule of law. Certainly, the AI Act establishes EU law provisions that public authorities must comply with. It could thereby also serve as a basis to invoke EU remedies aimed at ensuring Member States' compliance with their EU law obligations.[294] However, the fact that it does not impose stronger obligations on Member States to ensure their use of algorithmic regulation does not lead to *algorithmic rule by law*,

Laurence W Gormley (eds), *From Single Market to Economic Union* (Oxford University Press 2012) 176.

[290] In the past, the CJEU has frequently been asked to offer guidance to national courts regarding Member State legislation that imposed stricter requirements on providers of goods and services than those imposed by EU law (a practice sometimes referred to as 'goldplating'), which in some cases also resulted in the national legislation's incompatibility with EU law precisely because it was aimed at maximum harmonisation. See, e.g., Joined Cases C-261/07 and C-299/07, VTB-VAB NV, 23 April 2009, ECLI:EU:C:2009:244.

[291] Weatherill, 'Maximum versus Minimum Harmonization' (n 289) 177.

[292] Recital 1 AI Act.

[293] Article 2(11) AI Act. This also includes encouraging and allowing the application of collective agreements that are more favourable to workers.

[294] See *supra*, Section 5.2.3.

inadvertently or intentionally, is a missed opportunity. And the fact that Member States may be legally unable to level this protection up through national legislation, unless they can argue it falls outside its scope, only makes this problem worse.

Admittedly, the AI Act does state that the harmonised rules it provides "*should be without prejudice to existing Union law, in particular on data protection, consumer protection, fundamental rights, employment, and protection of workers, and product safety, to which this Regulation is complementary*."[295] It also mentions that a system's classification as 'high-risk' should not be interpreted as indicating the lawfulness of its use under other Acts of Union law or national law implementing Union law, "*such as on the protection of personal data, the use of polygraphs or the use of emotion recognition systems*".[296] However, the AI Act's clear intention to comprehensively regulate systems that pose a risk to fundamental rights makes it difficult to argue that an application listed in Annex III is nevertheless unlawful. While not excluded in principle, the person claiming such unlawfulness (for instance due to an incompatibility with a fundamental right) would have to surmount a significant burden of proof, which may only be met in the case where a national law exists that explicitly sets out the system's unlawfulness.[297] Moreover, in that case too, the risk still exists that an AI provider or deployer challenges the national law on internal market-based grounds, by claiming it constitutes an illegal market restriction for the very product the AI Act is meant to promote.[298]

Finally, the maximum ceiling imposed by the AI Act also has repercussions for Member States' participation in negotiations on AI regulation at the international level. For instance, during the Council of Europe's negotiations of a new Convention on AI and human rights, democracy and the rule of law,[299] which largely took place in parallel with the negotiations of the AI Act,[300] the Commission requested and

[295] See Recital 9 AI Act.

[296] See Recital 63 AI Act.

[297] I also made this point in Smuha (n 166).

[298] For a discussion of the relationship between internal market law and fundamental rights law, see also Stephanie Reynolds, 'Explaining the Constitutional Drivers behind a Perceived Judicial Preference for Free Movement over Fundamental Rights' (2016) 53 Common Market Law Review 643.

[299] This work was started by the Council of Europe's Ad Hoc Committee on AI (CAHAI) and continued by its Committee on AI (CAI). In Spring 2024, the CAI approved the 'draft Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law', along with a draft Explanatory Report. See also *supra*, Section 1.2.3.

[300] See Council Decision 2022/2349 of 21 November 2022 authorising the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence, human rights, democracy and the rule of law, ST/14173/2022/INIT, OJ L 311, 2 December 2022. When the Commission realised how fast the CAI's negotiations were advancing, and that the Convention could even be concluded before the finalisation of the AI Act, it quickly sought to postpone the Convention's negotiations. Officially, it requested its negotiation mandate to "*protect the integrity of Union law and to ensure that the rules of international law and Union law remain consistent*" (pursuant to Recital 7 of the Mandate). One could, however, also wonder to which extent the importance of being the *first* global

obtained a mandate to be the sole negotiator on behalf of EU Member States, rather than having Member States negotiating their own position.[301] From its request, it was evident that the Commission considers that matters related to the Council of Europe's Convention (meaning, matters related to AI's impact on human rights, democracy and the rule of law) to already be comprehensively dealt with under the AI Act. This assumption is, however, fanciful considering the inadequate attention to the rule of law in the AI Act, as well as its underwhelming protection of fundamental rights and democratic participation in decisions on AI's use. Nevertheless, the Commission wanted to ensure the Convention's alignment with the AI Act, thereby also precluding Member States to advocate for stronger protection. This is despite the fact that, as already hinted at, one could legitimately wonder whether the EU can claim the competence to exhaustively regulate aspects pertaining to algorithmic regulation in public administration on an internal market legal basis.

It hence appears that the EU legislator not only left open important legal gaps in the AI Act, but that it is also preventing Member States to fill these gaps, in the name of countering market fragmentation. This begs the question whether the Union's interest in being 'the first' AI legislator to reap the economic benefits of an internal market for AI are deemed more important than safeguarding its core values.

5.4.6 *Evaluation: The Return of Techno-supremacy*

Considering the above analysis, what should we now make of the AI Act in the context of the concerns identified in Chapter 4? Can it offer any help in countering the threat of algorithmic rule by law? Undoubtedly, the new regulation does introduce important legal safeguards to better protect individuals against the risks that *some* AI systems pose to their health, safety and fundamental rights. The establishment of a public enforcement mechanism; the introduction of prohibitions and requirements that must be met ex ante; as well as the inclusion of several rights for individuals that can fortify private enforcement channels are all to be welcomed. Furthermore, by imposing documentation and logging obligations that should facilitate ex post review, and by setting up an EU database to register the use of

legislator in this field played a role. See also Luca Bertuzzi, 'EU Commission postponed AI treaty negotiations with further delays in sight' *Euractiv* (5 October 2022), <www.euractiv.com/section/digital/news/eu-commission-postponed-ai-treaty-negotiations-with-further-delays-in-sight/>.

[301] This mandate was formally sought for matters falling within the exclusive competence of the Union, yet Article 2 of the Mandate also stated that "*to the extent that the subject matter of the negotiations falls partially within the competence of the Union and partially within the competence of its Member States, the Commission and the Member States shall cooperate closely during the negotiating process, with a view to ensuring unity in the external representation of the Union*".

high-risk systems by public authorities, the AI Act also enhances transparency around algorithmic regulation.[302]

However, overall, the protection the AI Act provides remains insufficient to meet the identified concerns. Its process is primarily based on self-assessments, and is not tailored to the specific risks arising in the context of algorithmic regulation. There are no proper mechanisms for public participation and input (for instance regarding the decision to deploy algorithmic regulation in the first place, or even just to help identify and assess the risks attached thereto); there are only limited transparency obligations towards those potentially affected by the systems; there is no obligation to make the extensive documentation of the system's functioning accessible to researchers, civil society organisations or the public at large; there are no provisions around the procurement of systems, or limitations as regards who should be able to undertake translations from law to code, with which training, and with which constitutional checks and balances; there are no ex ante independent oversight mechanisms, nor mandatory periodic audits that can help ensure continuous oversight; and there are no provisions that enable *systemic* review.

These substantive shortcomings are coupled with concerns around the AI Act's regulatory architecture. First, despite the role of the European AI Office, when it comes to public authorities' use of AI, oversight is primarily organised at the national level, which means the extent to which people can enjoy the AI Act's protection depends on the resources and skills of Member States. As the enforcement practice of the GDPR has shown, these vary significantly from one state to another.[303] And while national supervisory authorities ought to be independent, especially given their task to also review the actions of public authorities, experience with national data protection authorities has likewise indicated that such independence may not always be straightforward, even in countries that are not yet considered as undergoing 'an autocratic turn'.[304]

[302] In addition, geopolitically speaking, the regulation could act as a catalyst for others in the global regulatory arena for AI, as well as potentially offering the EU a first-mover advantage by setting the standard and aspiring to a 'Brussels effect' as described in Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020); *Digital Empires: The Global Battle to Regulate Technology* (Oxford University Press 2023). See also Charlotte Siegmann and Markus Anderljung, 'The Brussels Effect and Artificial Intelligence' (Centre for the Governance of AI 2022). On the first mover advantage to regulate AI, see also Nathalie A Smuha, 'From a "Race to AI" to a "Race to AI Regulation": Regulatory Competition for Artificial Intelligence' (2021) 13 Law, Innovation and Technology 57.

[303] See, for instance, Johnny Ryan and Alan Toner, 'Europe's Enforcement Paralysis – ICCL's 2021 Report on the Enforcement Capacity of Data Protection Authorities' (Irish Council for Civil Liberties 2022) <www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf>.

[304] In this regard, reference can, for instance, be made to the perceived concerns around the (lack of the) independence of the Belgian data protection authority. See Paul De Hert, 'Complete Independence of National Data Protection Supervisory Authorities: About Persons, Czars and Data Governance in Belgian Debates' (*European Law Blog*, 24 December 2021) <https://europeanlawblog.eu/2021/12/24/complete-independence-of-national-data-protection-supervisory-authorities-about-persons-czars-and-data-governance-in-belgian-debates/>. See also Belgian Data Protection Authority, 'A New Draft Law Threatens the Independence and Functioning of the BE

Second, the AI Act's reliance on conformity assessment and technical standardisation, as part of the New Legislative Framework (NLF) approach, is inadequate to deal with the rule of law risks posed by algorithmic regulation. As briefly noted above, this is an approach the Commission typically uses in the context of EU product regulation and safety standards. As such, it makes sense to subject high-risk systems that are already part of NLF legislation (listed in Annex I, including machinery, medical devices and toys), to the same compliance mechanisms as before, with the addition of the new requirements of the AI Act. However, applying the same model of safety legislation to the high-risk systems listed in Annex III is problematic, as the risks they pose – not only to fundamental rights, but also to societal interests such as the rule of law – are not comparable. AI systems are treated as tangible products which simply need to conform to technical requirements and have a 'CE' marking affixed to them, rather than socio-technological systems. This approach might work reasonably well for fridges and dishwashers, yet "*it is hardly appropriate for a digital technology which, on the Commission's own account, may pose significant risk to the protection of nontangible values*".[305] As noted elsewhere, while the "*text is infused with fundamental rights-language, it seems to take an overly technocratic approach to the protection of fundamental rights*",[306] by essentially translating those rights into a set of prescriptive rules, exhaustive lists, detailed technical safety standards, as well as handy templates and checklists. In addition, the reliance on harmonised standards that provide a 'presumption of conformity' in fact implies that the interpretation of the AI Act's requirements is outsourced to the (primarily technical experts of) standardisation organisations,[307] despite their lack of representativeness and democratic accountability.[308]

DPA' (March 2022) <www.dataprotectionauthority.be/citizen/a-new-draft-law-threatens-the-independence-and-functioning-of-the-be-dpa>; Belgian Data Protection Authority, 'Opinion on Preliminary Draft Law Amending the Act of 3 December 2017 Establishing the Data Protection Authority (AH-2022-0020)' (February 2022) <www.autoriteprotectiondonnees.be/publications/opinion-on-preliminary-draft-law-amending-the-act-of-3-december-2017-establishing-the-data-protection-authority.pdf>.

[305] Jeremias Adams-Prassl, 'Regulating Algorithms at Work: Lessons for a "European Approach to Artificial Intelligence"' (2022) 13 European Labour Law Journal 30, 49. See also Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 22 Computer Law Review International 97, 102; Smuha and others (n 189) 39. See also Jérôme De Cooman, 'Humpty Dumpty and High-Risk AI Systems: The Ratione Materiae Dimension of the Proposal for an EU Artificial Intelligence Act' [2022] Market and Competition Law Review 49.

[306] Smuha and others (n 189) 9.

[307] While efforts are made to include civil society organisations in the discussions, they are not only a minority in these discussions, but they also have far less resources to take part therein, as well as less knowledge about the procedures of such standardisation organisations. See also Luca Bertuzzi, 'AI Standards Set for Joint Drafting among European Standardisation Bodies' *Euractiv* (30 May 2022) <www.euractiv.com/section/digital/news/ai-standards-set-for-joint-drafting-among-european-standardisation-bodies/>.

[308] See the critique thereon by Smuha and Yeung (n 221). See also Veale and Borgesius (n 305) 105.

Interestingly, and sadly, parallels can hence be drawn with one of the risks pointed out in Chapter 4, namely that reliance on algorithmic regulation may exacerbate a techno-scientific approach to the law.[309] As noted previously, the danger associated with *algorithmic rule by law* is that the legal protection of individuals and the translation from open-ended legal rules to code is seen as a mere techno-scientific enterprise, to the detriment of human rights, the rule of law, and other essential values. When the regulated risk concerns the safety of machines, food or pharmaceuticals, a techno-scientific approach is neither new nor surprising. In those areas, it is common for the legislator to set out broad norms stating the objective of protecting the health and safety of individuals, which are subsequently elaborated and complemented with detailed technical requirements by domain experts who translate the objective of 'safety' into quantifiable, measurable and demonstrable safety standards that need to be complied with.[310]

Yet when it comes to protecting fundamental rights or the rule of law, this type of approach falls woefully short, as it is unable to do justice to the intricate contextual assessment and balance it requires between various interests. Nevertheless, this is precisely the AI Act's approach, as it erroneously reduces "*the careful balancing exercise between fundamental rights to a technocratic process, thus rendering the need for such balancing invisible*".[311] In this way, legal concepts such as the right to non-discrimination and the principle of equality are considered as elements that can be embodied by technical standards expressed in quantifiable and measurable specifications, checked by an internal 'quality management process', and algorithmically programmed, thereby maintaining the primacy of techno-rationality.[312] Worse still, the fact that this assessment and quality management occurs entirely in-house, without external oversight or ex ante accountability mechanisms, leaves these translation decisions entirely in the hands of technical experts, thus maintaining the supremacy of coders set out above.[313]

Lastly, the ceiling imposed by the AI Act's maximum harmonisation means that Member States who want to offer a higher level of protection than the AI Act currently provides are practically unable to do so. Despite the regulation's laudable intentions, and despite its introduction of valuable new safeguards, the overall picture that results from this analysis is therefore still rather bleak when it comes to the AI Act's ability to counter the threat of algorithmic rule by law.

5.5 CONCLUDING REMARKS

In Chapter 4, I conducted a systematic analysis of the way in which algorithmic regulation can impact the core principles of the rule of law, and conceptualised the

[309] Just like in other regulatory domains, see e.g. Garnett (n 260).

[310] See also *supra*, Section 2.3.3.

[311] Smuha and others (n 189) 12.

[312] See *supra*, Section 4.2.1.

[313] See *supra*, Section 4.2.2.

threat emanating therefrom as *algorithmic rule by law*. I noted that this threat needs to be counter-balanced by appropriate legal safeguards, apt to address the challenges raised by public authorities' increased reliance on algorithmic regulation. In this chapter, I therefore critically assessed whether the current EU legal framework is up to this task, and respectively analysed legislation pertaining to the rule of law, and legislation pertaining to the risks posed by (personal) data processing activities and by algorithmic systems. Although various protection mechanisms exist, and while the AI Act should be able to make a relevant contribution in this regard, my evaluation leads me to conclude that these are insufficient to address the adverse impact of algorithmic regulation on the rule of law.

On the one hand, the legal domain pertaining to the rule of law does not consider algorithmic regulation to be a particular threat, and rule of law monitoring initiatives that can help trigger such legislation do not pay attention to it. Moreover, the legal mechanisms to protect the rule of law currently seem unable to tackle more than individual infringements or budget-related concerns, whereas the deployment of algorithmic regulation without adequate safeguards can result in, or exacerbate, systemic deficiencies. On the other hand, the legal domain pertaining to algorithmic systems does not consider the rule of law to be a particularly impacted value. It hence does not pay specific attention to the fact that algorithmic regulation can increase the executive's power, erode the protective role of the law and, given its systemic effects, undermine the normative pillars of liberal democracy. In other words, these two legal domains are currently not on speaking terms, despite the urgent need for them to enter into a serious dialogue.

This urgency is only exacerbated by the new AI Act, which aims to be future proof and on which hope has now been vested for years to come. Yet by seeking to put forward a comprehensive piece of legislation to deal with the risks of algorithmic systems in an exhaustive manner, the EU legislator's ambition, though praiseworthy in itself, undermines its own purpose. First, there is no such thing as an *exhaustive* way to tackle the risks posed by algorithmic systems, even if we would assume the EU would have such competences,[314] and the many gaps in the complex and legalistic list-based approach of the AI Act testify to that. Second, the Act appears to pre-empt stronger safeguards at Member State level, due to its objective to counter market fragmentation and ensure harmonised member state legislation. Third, it approaches the protection of fundamental rights and, to the extent these are on the radar, other values, as a technocratic endeavour, which can be solved by identifying the right technical standard that providers should implement, crowned by a CE marking. Fourth, the combination of a single set of requirements for applications

[314] Recall the fact that the EU, for instance, does not have a general competence to regulate matters pertaining to the rule of law – or pertaining to national public administrations – but instead needs to rely on specific competences that are indirectly linked thereto. See *supra*, Section 5.1.

used in the public sector and the private sector, with a few useful yet tailored exceptions, overlooks the particular rule of law-related risks that are associated with the former, and might explain the AI Act's disregard thereof. Instead, the regulation approaches the harm caused by algorithmic systems in an isolated fashion, assessing for each individual application which risks it can pose to each individual interest. Yet by looking at the trees, it risks overlooking the forest: the systemic, networked, long-term, widespread impact of algorithmic regulation on societal interests, including the preservation of the protective role of the law, and the integrity of the legal system as a whole.

Unfortunately, despite these flaws, the existence of the AI Act may nevertheless provide a false sense of security that the risks raised by algorithmic regulation are aptly dealt with, and that their use by public authorities can now be further promoted and sponsored in the name of efficiency and innovation. Some commentators even claimed that the AI Act is in fact overprotective, and "*may come at the price of digital innovation*",[315] seemingly forgetting that innovation is not an end in and of itself, but that the aim of regulating the risks of this technology is to delineate the contours in which socially beneficial innovation can thrive. Finally, it must be recalled that these developments occur against a background in which illiberal and authoritarian practices are on the rise, and in which the implementation of the law – whether in textual or algorithmic form – is already being used, inadvertently or deliberately, to further those problematic ends.

[315] Raposo (n 187) 88.