Automated Decisions under Scrutiny: Lessons from C-203/22 for Europe's Digital Rule of Law

Georgios Pavlidis
UNESCO Chair & Jean Monnet Chair Associate Professor of International and EU Economic Law
School of Law, Neapolis University Pafos

Ioannis Kastanas
Lecturer of Public Law, School of Law, Neapolis University Pafos
Team Member of the Center of Excellence AI-2-TRACE-CRIME, NUP

Nikoletta Constantinou
Attorney at Law, Special Teaching Staff, School of Law, Neapolis University Pafos
Team Member of the Jean Monnet Centre of Excellence AI-2-TRACE-CRIME

The judgment of the Court of Justice of the European Union in C-203/22, CK v Magistrat der Stadt Wien (Dun & Bradstreet Austria), constitutes an important development in the EU's jurisprudence on automated decision-making and data-subject rights. The Court clarifies the content of the GDPR's requirement to provide meaningful information about the logic involved in profiling and scoring systems. It also attempts to balance transparency obligations and the protection of trade secrets. This article situates the ruling within the broader architecture of Europe's digital rule of law and argues that the Court advances a more accountable model of algorithmic governance. This new model demands intelligibility and contestability when the decisions of automated systems significantly affect individuals. This study was prepared in the context of the Jean Monnet Center of Excellence AI-2-TRACE-CRIME and was funded by the European Union. Views and opinions expressed are however those of the author only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

1. Introduction

Automated decision-making (ADM) and algorithmic scoring systems have become part of modern digital infrastructures. Several types of algorithmic processes, such as creditworthiness assessments, fraud detection, and eligibility screenings in public administration, play an increasingly important role in the economic and social life. These algorithmic processes can determine access to essential goods, services, and opportunities, which raises concerns regarding accountability and the capacity of affected individuals to understand and meaningfully contest the decisions that affect them. At the EU level, the General Data Protection Regulation (GDPR) establishes a series of rights designed to preserve individual autonomy and procedural fairness.[1] Among these rights, we can mention the right of access and the right to obtain meaningful information about the logic involved in automated processing. However, the precise contours of these rights are not always clear, particularly in technologically complex contexts.

The Court of Justice of the European Union (CJEU) has begun to develop its jurisprudence addressing these issues. Following its judgments in C-634/21[2] and C-487/21[3], the Court's more recent decision in C-203/22, CK v Magistrat der Stadt Wien (Dun & Bradstreet Austria)[4], adds doctrinal clarity to rules governing ADM under the GDPR. The case concerns

1. 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), OJ L 119, 4.5.2016, pp. 1–88
2. Judgment of the Court, OQ v Land Hessen (SCHUFA Holding AG),7 December 2023, Case C-634/21, ECLI:EU:C:2023:957
3. Judgment of the Court (First Chamber), 4 May 2023, Case C-487/21, F.F. V Österreichische Datenschutzbehörde (CRIF GmbH), ECLI:EU:C:2023:369
4. Judgment of the Court, 27 February 2025 C-203/22, CK v Magistrat der Stadt Wien (Dun & Bradstreet Austria GmbH), ECLI:EU:C:2025:117

credit-scoring practices, but its implications are broader for the EU's digital rule of law. More specifically, the Court had to examine the extent of a controller's obligation to explain the functioning of an automated scoring model. The Court had also to pronounce on the relationship between access rights and the prohibition of fully automated decisions, as well as the proper balance between transparency obligations and the protection of trade secrets under Directive 2016/943[5].

This article argues that C-203/22 constitutes an important step toward to improve algorithmic accountability within the EU legal order. The judgment appears to advance a more operational understanding of transparency, based on intelligibility and practical contestability, rather than formalistic disclosure. The article examines the implications of the ruling, as well as how C-203/22 contributes to Europe's digital rule of law. Of course, serious challenges remain for ensuring that ADM respects the rights of affected persons.

2. Legal and Regulatory Background

The GDPR is the primary legal framework governing ADM and profiling within the EU. Articles 12–15 GDPR establish the transparency and access obligations owed to data subjects. They require controllers to ensure that information is provided in a concise, intelligible, and easily accessible form. In cases involving profiling or ADM, Article 15(1)(h) specifically grants individuals the right to access "meaningful information about the logic involved" as well as the importance and consequences of such processing. This provision is framed as part of the general right of access, but it also performs a separate function: it enables individuals to understand the basis of a decision that affects them, thereby facilitating the exercise of other rights (rectification, contestation, right to be heard, etc.)[6].

For its part, Article 22 GDPR complements the access rights by establishing a limited prohibition on decisions "based solely on automated processing" that produce legal or similarly significant effects.[7] Article 22(3) GDPR introduces safeguards (human intervention, right to express one's point of view, right to contest the decision), which presuppose a minimum level of explanation regarding how the automated decision was reached.

The key issue here is that the GDPR does not specify how detailed such information should be. Moreover, it does not specify how controllers should reconcile these obligations with competing interests, such as trade-secret protection or intellectual-property rights.

Directive 2016/943, mentioned previously, introduces an additional layer of complexity regarding the protection of trade secrets. Article 2(1) of the Directive defines a trade secret as information that is secret (not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question), commercially valuable, and subject to reasonable steps to preserve its confidentiality. It can be argued that this definition covers most algorithmic models, proprietary scoring methodologies, and datasets used for automated assessments. Not surprisingly, controllers frequently invoke trade secrets as a basis for refusing to disclose factors, weightings, or methodological details, because they risk revealing commercially sensitive logic underlying ADM systems.

However, the GDPR and Directive 2016/943 do not establish a hierarchy between data-subject rights and the interests of controllers. Instead, they require a balancing exercise, which is specific to the context in each case. Evidently, there is a need to protect trade secrets while ensuring that data-subject rights are not undermined.[8] However, it is difficult to determine the appropriate threshold in practice.[9] On the one hand, giving too much deference to trade secrecy threatens to insulate opaque decision systems from accountability. On the other hand, excessive disclosure may erode legitimate business confidentiality and disincentivise innovation.

Before C-203/22, the CJEU had already begun to clarify some aspects of ADM transparency through the judgments in C-634/21 and C-487/21, mentioned previously. These judgments established, respectively, that credit scoring may constitute a prohibited fully automated decision within Article 22 GDPR and that controllers must provide sufficiently detailed information about profiling to enable meaningful understanding.[10] Together, these cases set the stage for

5. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016, pp. 1–18
6. Case C-203/22, par. 54 "That right of access is necessary to enable the data subject to exercise, depending on the circumstances, his or her right to rectification, right to erasure ('right to be forgotten') or right to restriction of processing, conferred, respectively, by Articles 16, 17 and 18 of the GDPR, as well as the data subject's right to object to his or her personal data being processed, laid down in Article 21 of the GDPR, right of action and right to compensation, laid down in Articles 79 and 82 of the GDPR".
7. *Djeffal, Christian*, "The normative potential of the European rule on automated decisions: A new reading for Art. 22 GDPR", Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, vol. 81 (2020), pp. 847-879.
8. As explained in Recital 63 GDPR, "that right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject."
9. *Malgieri, Gianclaudio*, "Trade Secrets v Personal Data: a possible solution for balancing rights", International Data Privacy Law, vol. 6 (2016), p. 102 ff.
10. *Noguera, Angela Maria*, "Case C-634/21, OQ v. Land Hessen (CJEU)", International Legal Materials, vol. 63 (2024), pp. 946-

C-203/22, in which the Court was asked to determine the scope of explanation required under Article 15 GDPR and to balance transparency of algorithmic assessments against trade-secret claims.

3. Facts and the Questions Referred in C-203/22, CK v Dun & Bradstreet Austria

The dispute originated in Austria, where the data subject, CK, sought to renew or extend an existing mobile phone contract which would have required a monthly payment of EUR 10. The telecommunications provider relied on a creditworthiness score generated by Dun & Bradstreet Austria GmbH (D&B), a private credit information agency. The provider declined to extend the contract on the ground that, according to the automated credit assessment, carried out by D & B, the prospective client did not have sufficient financial creditworthiness. Subsequently, CK exercised her GDPR right of access and requested detailed information regarding how the score had been produced, including the factors, their weightings, and the underlying logic of the process.

D&B provided only limited information. It disclosed broad categories of data and general statements about its scoring methodology. However, it refused to explain the key determinants of the score or the structure of the algorithmic model, invoking trade-secret protection and the confidentiality of third-party data. Dissatisfied, CK lodged a complaint before the Austrian data protection authority. CK argued that D&B had failed to comply with Article 15(1)(h) GDPR and that the refusal prevented her from understanding how the score had been calculated. This also meant that the refusal prevented her from meaningfully contesting the decision.

The case was examined by the Vienna Administrative Court (Verwaltungsgericht Wien), which noted the importance of algorithmic scoring models in consumer markets and the uncertainty surrounding the relationship between transparency rights and trade-secret protection. For these reasons, it submitted preliminary questions to the CJEU under Article 267 TFEU.

The key question was how Article 15(1)(h) should be interpreted, i.e. whether "meaningful information about the logic involved" requires disclosure of variables, weightings, thresholds, or other model parameters. Another issue was whether a controller's reliance on trade secrets under Directive 2016/943 could justify withholding such information, and what criteria should guide the balancing of rights. Moreover, the Austrian court sought clarification on the relationship between the right of access and the safeguards in Article 22 GDPR, particularly whether inadequate explanation may affect the determination of whether a decision is "based solely on automated processing."

4. The Court's Judgment and Reasoning

The Court of Justice's judgment in C-203/22 offers an interpretation of Article 15(1)(h) GDPR[11] and its relationship to both Article 22 GDPR[12] and the Directive 2016/943. The ruling examines the "meaningful information" requirement, establishes limits on controllers' claims to confidentiality, and reinforces the transparency architecture of EU data protection law. The Court's reasoning arises in the specific context of credit scoring, but it carries implications for all automated decision-making systems where opaque algorithms influence individual rights.

4.1. The Meaning of "Meaningful Information" under Article 15(1)(h)

The Court begins by interpreting the scope of the right of access in the context of automated decision-making. Article 15(1)(h) GDPR requires disclosure of information sufficient to enable a data subject to understand the "logic involved" in the processing, as well as the significance and envisaged consequences of such processing. The wording of Article 15(1)(h) GDPR covers "all relevant information concerning the procedure and principles relating to the use, by automated means, of personal data with a view to obtaining a specific result".[13] The provision, in the Court's view, is intended to give individuals practical insight into how input variables shape outcomes. It must allow them to assess whether a decision is lawful, accurate, or contestable.

The Court rejects the view that the criterion of "meaningful information" can be satisfied by too generic or too technical descriptions of algorithmic processing.[14] Instead, it requires disclosure of the parameters that determine the outcome. This includes the main factors considered and their relative importance, insofar as such information is necessary for understanding the rationale of the decision. Importantly, the Court clarifies that the GDPR does not mandate disclosure of full algorithmic details, mathematical formulas, or source

961; *Trstenjak, Verica*, "GDPR as a New Consumer Protection Weapon?", European Studies–The Review of European Law, Economics and Politics, vol. 11 (2024), pp. 15-32.

11. On this provision see, *Custers, Bart, and Anne-Sophie Heijne*, "The right of access in automated decision-making: the scope of article 15 (1)(h) GDPR in theory and practice", Computer Law & Security Review, vol. 46 (2022): 105727; see also *Sørum, Hanne, and Wanda Presthus*, "Dude, where's my data? The GDPR in practice, from a consumer's point of view", Information Technology & People, vol. 34 (2021), pp. 912-929.
12. On this provision see, *Roig, Antoni*, "Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR)", European Journal of Law and Technology, vol. 8.3 (2017)
13. Case C-203/22, par. 43.
14. Case C-203/22, par. 59

code.[15] In this approach, the standard is more functional than technical. In other words, information must be comprehensible to an ordinary data subject.

4.2. Transparency Obligations and Their Relationship with Articles 12–14 GDPR

The Court links Article 15(1)(h) GDPR with the transparency obligations under Articles 12–14 GDPR.[16] Controllers must ensure that information is concise, intelligible, and presented in plain language. Transparency obligations operate both *ex ante* and *ex post*: information provided during data collection must align with information later provided upon access request. This interpretation of Article 15 GDPR approximates a form of "right to explanation," even if not explicitly termed as such.

4.3. Trade Secrets and the Limits of Confidentiality

Another significant aspect of C-203/22 concerns the interaction between Article 15 GDPR and Directive 2016/943 on trade secrets. Controllers may have legitimate interests in protecting proprietary scoring models. However, the Court rejects the argument that trade-secret status allows a categorical refusal to disclose meaningful elements of the decision-making logic.[17]

As it is often the case, the Court requires a balancing exercise: national authorities and courts must weigh the interests protected by trade secrecy against the fundamental data-subject rights under the GDPR. The balancing must not be abstract or speculative, but concrete and contextual. Moreover, controllers must demonstrate (i) that the information in question is indeed a trade secret, and (ii) that disclosure would seriously prejudice their legitimate interests. More specifically, the controller is required to provide the allegedly protected information to the competent supervisory authority or court, "which must balance the rights and interests at issue with a view to determining the extent of the data subject's right of access".

4.4. Relationship with Article 22 GDPR and the Nature of the Decision

Another important issue concerns the relationship between Article 15 and Article 22 GDPR. Article 22(1) GDPR prohibits decisions based solely on automated processing that produce legal or similarly significant effects unless specific safeguards are provided. The Court does not fully revisit its earlier jurisprudence, but it affirms that meaningful access information is essential for assessing whether a decision falls within the scope of Article 22 GDPR. In other words, insufficient explanation may impede the ability of data subjects to determine whether they were subject to a prohibited automated decision and to assert their rights under Article 22(3) GDPR.[18]

5. Lessons for Europe's Digital Rule of Law

The Court's judgment in C-203/22 extends beyond the specific context of credit scoring; it contributes to the wider process of building a digital rule of law in the EU.[19] The reasoning clarifies how transparency, accountability, and the balancing of competing interests should operate when automated systems affect individual rights.

Several key lessons emerge from the decision.

First, the judgment reaffirms the importance of transparency for algorithmic accountability.[20] The Court rejects overly generic or complex disclosures and confirms that individuals must be able to understand why a particular outcome arose. Therefore, the focus is on functional comprehensibility, non on formalistic compliance. Regarding the procedural dimension of the GDPR, the Court views explanation not as an end, but as condition for enabling other rights (contestation, rectification, and Article 22 GDPR safeguards).

Second, controllers (public and private) must rethink their internal governance practices.[21] The requirement to disclose the principal parameters of automated models has practical implications. It necessitates structured documentation of how systems function, which factors determine outcomes, and how weightings or thresholds operate. This requires an "explainability by design" model[22], where explanations are not assembled retroactively but form part of system

15. Case C-203/22, par. 60
16. Case C-203/22, par. 46
17. Case C-203/22, par. 70-72.
18. Case C-203/22, par. 55.
19. *Sun, Xiaoxia, and Yang Xiao*, "How digital power shapes the rule of law: The logic and mission of digital rule of law", International Journal of Digital Law and Governance, vol. 1.2 (2024), pp. 207-243; *Shaelou, Stéphanie Laulhé, and Yulia Razmetaeva*, "Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems: shaping the digital legal order while upholding Rule of Law principles and European values", ERA Forum, vol. 24 (2023).
20. *Kossow, Niklas, Svea Windwehr, and Matthew Jenkins*, Algorithmic transparency and accountability, Transparency International, 2022; *Ananny, Mike, and Kate Crawford*, "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability", New Media & Society, Vol. 20.3 (2018), pp. 973-989
21. *Sayles, James*, "Aligning AI Governance with Other Internal Governance Models for Trustworthy AI: The Convergence of Governance Frameworks", in: Principles of AI Governance and Model Risk Management, Berkeley 2024, pp. 113-172.
22. *Hamon, Ronan, et al.*, "Bridging the gap between AI and explainability in the GDPR: towards trustworthiness-by-design in automated decision-making", IEEE Computational Intelligence Magazine, vol. 17.1 (2022), pp. 72-85.

development. This also requires standardised templates, records of processing, and training of staff to respond meaningfully to access requests. Therefore, organisational models must anticipate scrutiny and embed accountability mechanisms within algorithmic systems.

Third, the judgment narrows the defensive use of trade-secret claims.[23] Indeed, reliance on confidentiality has often been a barrier to understanding algorithmic processes. The Court requires a concrete balancing exercise, rather than blanket deference. This shifts the regulatory burden: controllers must now justify, with specificity, why particular disclosures would genuinely harm their commercial interests. This recalibration of trade-secret protection demonstrates the primacy of fundamental rights. It also signals that economic interests cannot be used to circumvent key transparency obligations.

Fourth, although the case arises from a private-sector context, its reasoning also applies to public-sector ADM, maybe with greater force.[24] Increasingly, public authorities rely on automated scoring, eligibility assessments, risk evaluations, prioritisation tools and other AI applications that directly affect rights and entitlements. The Court reaffirms the importance of intelligibility and contestability, which resonates with core principles of administrative law (duty to give reasons, right to be heard, proportionality, and effective judicial protection). As algorithmic administration expands, C-203/22 can serve as a doctrinal foundation for public authorities to disclose the operative logic of ADM systems and ensure that individuals can challenge automated outcomes.

Finally, the decision complements the new regulatory framework under the EU Artificial Intelligence Act.[25] The AI Act imposes transparency, documentation, traceability, and human-oversight obligations on high-risk systems.[26] Many of these obligations mirror the Court's interpretation of GDPR rights. C-203/22 appears to pre-figure the demand for explainability under the AI Act and supports the idea of risk-based governance. Once the AI Act is fully implemented, controllers will face a dual compliance regime: algorithmic systems must satisfy GDPR rights and meet the AI Act's requirements. These legal instruments are not competing but mutually reinforcing components of a broader European strategy for responsible digital transformation.

6. Remaining Ambiguities, Future Challenges, and Concluding Reflections

The judgment in C-203/22 represents an important step for determining the contours of algorithmic accountability within EU law. Yet even as the Court clarifies the notion of "meaningful information," some important questions remain unresolved. The functional standard set out by the Court, as discussed previously, advances transparency, but it remains contextual and it can be uncertain. This will be particularly problematic for complex AI systems whose inner logic cannot easily be translated into human-readable terms. As AI models grow more sophisticated, controllers may find it difficult to provide explanations that satisfy the intelligibility requirements of Article 15 GDPR.

Moreover, the fact that the Court insists on a concrete balancing of trade-secret claims may lead to divergent national approaches. Supervisory authorities and courts may vary in how they evaluate the commercial sensitivity of an algorithm. They may also vary in the extent to which they require partial, anonymised, or safeguarded disclosures. Without further harmonisation, this doctrinal flexibility could lead to uneven protection of data-subject rights across the Union. The need for technical and legal expertise also raises concerns about the capacity of national authorities to assess complex algorithmic evidence.

In public-sector contexts, the implications of C-203/22 are more profound. Automated scoring and eligibility systems can be used in areas such as welfare assessments, fraud detection, tax administration, and migration control. The judgment reinforces that such systems must satisfy transparency and explanation duties consistent with the principles of good administration and effective judicial protection. However, public authorities may rely on proprietary systems supplied by private vendors, which creates an accountability gap when governments cannot fully disclose the logic of the tools they deploy.

There are also challenges regarding the interaction between the GDPR and the EU AI Act. The two instruments share normative objectives (traceability, human oversight, and risk management), but there is a certain risk of fragmentation. Indeed, the AI Act's technical standards may not always

23. *Matulionyte, Rita, and Tatiana Aranovich*, "Trade secrets versus the AI explainability principle", in: Research handbook on intellectual property and artificial intelligence, Edward Elgar Publishing, 2022, pp. 405-422.
24. *Kastanas, Ioannis, and Pavlidis, Georgios*, "Algorithmic Administration and the EU AI Act: Legal Principles for Public Sector Use of AI", Journal of Ethics and Legal Technologies, Vol. 7(2), pp. 59-79; Wirtz, Bernd W., Jan C. Weyerer, and Carolin Geyer. "Artificial intelligence and the public sector—applications and challenges." International Journal of Public Administration 42.7 (2019): 596-615.
25. 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), OJ L, 2024/1689, 12.7.2024
26. *Pavlidis, Georgios*, "From the AI Act to a European AI Agency: Completing the Union's Regulatory Architecture", Croatian Yearbook of European Law and Policy, Vol. 21 (2025), pp. 125–144.

map neatly onto the GDPR's rights-based obligations, and controllers will need to navigate a dual compliance landscape.

Despite these ambiguities, the lesson of C-203/22 is that the EU is steadily constructing a digital rule of law, promoting transparency and the protection of fundamental rights.[27] The Court's reasoning confirms that algorithmic systems cannot operate as "black boxes"[28] and that commercial confidentiality cannot be used to negate data-subject rights. Therefore, explanation constitutes a safeguard, enabling individuals to understand, challenge, and ultimately resist decisions that shape their social and economic opportunities. C-203/22 does not resolve every tension inherent in regulating ADM, but it advances the principle of accountability in the EU. The next phase of legal development will likely concern seeking the right balance between transparency and confidentiality, ensuring consistent implementation across Member States, and adapting the law to increasingly complex AI systems.

References

- *Ananny, Mike, and Kate Crawford*, "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability", New Media & Society, Vol. 20.3 (2018), pp. 973-989.
- *Custers, Bart, and Anne-Sophie Heijne*, "The right of access in automated decision-making: the scope of article 15 (1) (h) GDPR in theory and practice", Computer Law & Security Review, vol. 46 (2022): 105727.
- *Djeffal, Christian*, "The normative potential of the European rule on automated decisions: A new reading for Art. 22 GDPR", Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, vol. 81 (2020), pp. 847-879.
- *Hamon, Ronan, et al.*, "Bridging the gap between AI and explainability in the GDPR: towards trustworthiness-by-design in automated decision-making", IEEE Computational Intelligence Magazine, vol. 17.1 (2022), pp. 72-85.
- *Kastanas, Ioannis, and Pavlidis, Georgios*, "Algorithmic Administration and the EU AI Act: Legal Principles for Public Sector Use of AI", Journal of Ethics and Legal Technologies (forthcoming).
- *Kossow, Niklas, Svea Windwehr, and Matthew Jenkins*, Algorithmic transparency and accountability, Transparency International, 2022.
- *Malgieri, Gianclaudio*, "Trade Secrets v Personal Data: a possible solution for balancing rights", International Data Privacy Law, vol. 6 (2016), p. 102 ff.
- *Matulionyte, Rita, and Tatiana Aranovich*, "Trade secrets versus the AI explainability principle", in: Research handbook on intellectual property and artificial intelligence, Edward Elgar Publishing, 2022, pp. 405-422.
- *Noguera, Angela Maria*, "Case C-634/21, OQ v. Land Hessen (CJEU)", International Legal Materials, vol. 63 (2024), pp. 946-961.
- *Papanastasiou, T. N. and Pavlidis, G.*, "The European Court of Human Rights and the Age of Artificial Intelligence: Jurisprudential Foundations for Future Adjudications", Cyprus Law Review (KYNE), vol. 2-3/2024, pp. 183-187.
- *Pavlidis, Georgios, "*From the AI Act to a European AI Agency: Completing the Union's Regulatory Architecture", Croatian Yearbook of European Law and Policy, Vol. 21 (2025), pp. 125–144.
- *Pavlidis, Georgios*, "Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI", Law, Innovation and Technology, vol. 16.1 (2024), pp. 293-308.
- *Roig, Antoni*, "Safeguards for the right not to be subject to a decision based solely on automated processing (Article 22 GDPR)", European Journal of Law and Technology, vol. 8.3 (2017).
- *Savin, Andrej*, "Designing EU digital laws" in: Research Handbook on EU Internet Law, Edward Elgar Publishing, 2023, pp. 63-79.
- *Sayles, James*, "Aligning AI Governance with Other Internal Governance Models for Trustworthy AI: The Convergence of Governance Frameworks", in: Principles of AI Governance and Model Risk Management, Berkeley 2024, pp. 113-172.
- *Shaelou, Stéphanie Laulhé, and Yulia Razmetaeva*, "Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems: shaping the digital legal order while upholding Rule of Law principles and European values", ERA Forum, vol. 24 (2023).
- *Sørum, Hanne, and Wanda Presthus*, "Dude, where's my data? The GDPR in practice, from a consumer's point of view", Information Technology & People, vol. 34 (2021), pp. 912-929.
- *Sun, Xiaoxia, and Yang Xiao*, "How digital power shapes the rule of law: The logic and mission of digital rule of law", International Journal of Digital Law and Governance, vol. 1.2 (2024), pp. 207-243.
- *Trstenjak, Verica*, "GDPR as a New Consumer Protection Weapon?", European Studies–The Review of European Law, Economics and Politics, vol. 11 (2024), pp. 15-32.

27. *Savin, Andrej*, "Designing EU digital laws" in: Research Handbook on EU Internet Law, Edward Elgar Publishing, 2023, pp. 63-79; see also *Papanastasiou, T. N. and Pavlidis, G.*, "The European Court of Human Rights and the Age of Artificial Intelligence: Jurisprudential Foundations for Future Adjudications", Cyprus Law Review (KYNE), vol. 2-3/2024, pp. 183-187.
28. *Pavlidis, Georgios*, "Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI", Law, Innovation and Technology, vol. 16.1 (2024), pp. 293-308.