Chapter 13. Rethinking Algorithmic Explainability Through the Lenses of Intellectual Property and Competition

Lucas Costas dos Anjos

Chapter 13
Rethinking Algorithmic Explainability Through the Lenses of Intellectual Property and Competition

Lucas Costa dos Anjos

Contents

Abstract Algorithmic decision-making is integral to digital platforms, influencing user experiences and societal dynamics. This paper chapter scrutinizes algorithmic opacity, highlighting the inherent biases, the anti-competitive strategies that may result from dominant market power and the potential for discrimination within these systems. Despite the promise of objectivity, algorithms often operate under a veil of opacity, shaping content and information access, with significant implications for individual perspectives and societal functioning. The chapter explores the legal challenges posed by the protection of algorithms through the lenses of intellectual property rights and competition law. It calls for a multifaceted regulatory approach to ensure transparency. The analysis emphasises the need to balance innovation with competition and societal well-being, advocating for a right to explanation in the face of automated decisions within the European Union.

Keywords Algorithmic decision-making · Neutrality · Bias · Transparency · Regulation · Digital platforms

L. C. dos Anjos (✉)
Postdoctoral researcher at École de Droit Sciences Po, 13 rue de l'Université, 75337 Paris, France
e-mail: lucas.costadosanjos@sciencespo.fr

K. Prifti et al. (eds.), *Digital Governance*, Information Technology and Law Series 39,
https://doi.org/10.1007/978-94-6265-639-0_13

13.1 Introduction

Algorithmic decision-making with the help of machine learning has become pervasive in our society, shaping our online experiences and influencing our daily lives. They allow computers to understand patterns and forecast or make judgments based on data without the need for literal and explicit programming. Such is the case of predictive algorithms for personalized advertising, content moderation and matching. However, concerns about bias, discrimination, and lack of transparency have raised significant regulatory challenges. This chapter examines the evolving landscape of algorithmic neutrality and the increasing need for effective rights to explanation in the face of algorithmic decision-making.

While machine learning algorithms promise efficiency and objectivity, their pervasive nature has ushered in a slew of concerns, particularly surrounding their inherent biases and potential for discrimination. The widespread assumption that platforms like Google, Facebook, and Twitter operate under a veil of neutrality is increasingly being challenged.[1]

In reality, these algorithms, often shrouded in opacity, play a pivotal role in shaping the content we are exposed to in a social network such as Twitter, in the information we retrieve in a Google Search results' page, product recommender systems on Amazon and in the societal dynamics of political debates intermediated by public digital discourse. The consequences of algorithmic choices are not neutral and can have profound impacts on our access to information, our perspectives, and the overall functioning of society.

Moreover, the dominance of certain platforms in the digital market presents additional challenges. Market power abuse, anti-competitive strategies, and the lack of transparency in algorithms hinder fair competition and limit users' freedom of choice. The concentration of power in a few platforms raises even more concerns about the implications for market dynamics and the overall diversity of online content.[2]

The legal inscrutability of algorithms further complicates the regulatory landscape. The protection of algorithmic decision-making through trade secrets and intellectual property rights creates barriers to understanding how decisions are made and whether biases are present. As algorithms increasingly drive critical processes in areas such as finance, employment, and criminal justice, the need for transparency and a right to explanation becomes more pressing.[3]

---

[1] Abiteboul and Stoyanovich 2019, p. 9.

[2] Google is one of the main perpetrators of these abuses of dominant position. In the European Union, the company has been scrutinized by competition authorities under several prisms, most noticeably in the Android, Ads and Search cases. Notably, in 2017, it was fined €2.42 billion for abusing its dominant position in the online search market by favoring its own price comparison service. Again in 2018, Google was penalized for restricting competition in the mobile internet sector through its Android operating system. These actions, considered illegal under EU antitrust rules, hindered innovation and competition, leading to reduced choices and potentially higher prices for consumers. Anjos and Leurquin 2021, p. 121–122. See also: Zuboff 2019, p. 112.

[3] O'Neil 2016, p. 78.

In this context, addressing the challenges of algorithmic decision-making requires a multifaceted approach. Regulatory frameworks need to be developed to ensure transparency and mechanisms should be established to challenge biased outcomes and protect user rights. Collaboration among stakeholders, including policymakers, platform operators, and civil society, is essential to develop effective solutions that balance innovation, competition, and societal well-being.

This paper analyses the increasing prominence of algorithmic decision-making, which requires a careful examination of its implications for fairness, transparency, and accountability. This investigation aims to acknowledge the biases inherent in algorithms, address market power concerns, and promote legal and theoretical grounds in favour of a right to explanation of automated decisions in the European Union. The study diverges from the scope of Article 22 of the GDPR, which centres on data protection law, by concentrating on different legal dimensions, specifically intellectual property and competition law. The objective is to scrutinize issues related to market power and broaden the perspective beyond data protection, encompassing the wider legal and market implications of algorithm-driven decision-making processes.

13.2 Technological Neutrality and Determinism

The presumption of neutrality often held by users of digital platforms increases the possible impacts of algorithmic bias when it comes to search results.[4] Since its users primarily assume that, for example, Google's search engine is synonymous with 'research,' and trust that its results are the best possible outputs that can be generated from their queries' inputs, Google can have a strong influence over users' everyday lives. The same can be said about Twitter, Facebook and Instagram's feed: there is nothing neutral about the choices of content a user is exposed to.

In order to better define neutrality as a legal concept, it is possible to extract its meaning from other areas in which this discussion has been progressing for a longer time. For example, the concept of net neutrality involves non-discrimination by internet service providers toward content providers (message source), users (message destination), or the content itself (message).[5] Thus, neutrality is actually defined by its antonym, discrimination.

[4] Newspapers have traditionally relied on outrage and sensationalism, understanding human tendencies that algorithms have also identified. The key distinction is that newspapers can be held legally accountable for their content, and people usually grasp their editorial biases. Algorithms, appearing neutral, escape accountability. Bartlett 2018, p. 80. Janssen 2020, p. 82. Martin 2019, p. 839.

[5] Abiteboul and Stoyanovich 2019, p. 3.

This reasoning can be expanded to other areas where neutrality is key.[6] For example, non-neutral algorithms would be discriminatory algorithms. However, discrimination can be at the core of some algorithmic business models, such as Google's. Discrimination is of the utmost importance to ranking results, determining relevance, and personalizing the outcomes of automated decision-making.

Digital platforms need to exercise some level of discrimination in order to perform well (to curate content in linear timelines, like on Instagram and Twitter, or to match results according to geolocalization, like on Google Search, for example), and it would not be a stretch to affirm that it is precisely its discriminatory abilities, which have been perfected over years, that make it so competitive as business models.[7] Nonetheless, some discriminatory behaviours are unacceptable by law, such as 'discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.'[8]

For this reason, this analysis does not aim to impose neutrality as an absolute value on algorithms. By definition, the ranking algorithm of a search engine or a newsfeed algorithm of a social network needs to evaluate, discriminate, and choose which results and posts are more important than others. Rather than striving to be neutral in every way, the real issue with digital platforms lies in identifying when algorithms are not neutral. This includes situations where they discriminate against protected groups, infringe on fundamental rights, or confuse consumers.

There is the risk of bias. A digital platform perceived as neutral has the chance to significantly influence its users through its algorithm, either by omitting certain content or highlighting others (through higher rankings on the recommendations, for example).[9] Also, altering its design layout may cause confusion concerning what is being commercially sponsored and what are the non-sponsored results.

There is also the possibility of constraints on freedom of communication and expression.[10] Application providers might decide to impede certain forms of speech from appearing high in the ranking of results or keep them from appearing in the

[6] '[N]ew forms of neutrality are emerging such as device neutrality (Is my smart phone blocking certain apps and favoring others?), and platform neutrality (Is this particular web service providing neutral recommendation?). For instance, app stores like Google Play and the Apple App Store, tend to refuse to reference certain services, perhaps because they are competing with the company's own services.' Abiteboul and Stoyanovich 2019, p. 7.

[7] Stinson 2021.

[8] Charter of Fundamental Rights of the European Union 2012, art. 21.

[9] Saurwein et al. 2015, p. 37. Regarding bias Joanna Mazur contends that using artificial intelligence to evaluate current discriminatory practices for making automated decisions about the future can create an illusion of impartiality. The absence of human involvement might seem to make the process more equitable. Yet, it's important to remember who supplies the data and analysis tools. Mazur 2018, pp. 179–180.

[10] Saurwein, Just, and Latzer, p. 37.

results at all due to their nature, tone, and other characteristics contrary to the standards of 'appropriateness,' whether they be political or cultural.[11] Also, due to an increasing quest for intermediate liability in online content nowadays, with concerns regarding fake news and hate speech online, platforms might be overzealous in the removal (or moderation) of content in order to avoid liability in the future.

13.3 Dominant Market Power and Anti-Competitive Strategies

The concept of market power is especially relevant for this analysis.[12] It is worth establishing a precise legal definition of this concept, since market power is not illegal per se, but its abuse and anti-competitive practices stemming from the privileges inherent to a dominant position in a relevant market are.[13] Therefore, to analyse the abuse of power and abusive practices, it is important to determine which market is being considered.

The European Commission Notice on the definition of relevant market for the purposes of Community competition law defines a relevant market according to two main dimensions: product and geography. A relevant product market refers to a set of products and services that are interchangeable or substitutable by consumers due to

[11] This matter of ranking prominence was tackled in the European Commission's decision on the Google Shopping Case. 'The Commission's decision refers to the inducement effect of higher rankings or of adding images, prices and merchant information to product search that result in increases of traffic, as confirmed by eye-tracking studies and similar research on the impact on user behavior and click-through rates. As the Commission concludes, citing Google's own submissions, the rationale for higher rankings and inducement to click is to 'dramatically increase traffic' by leveraging 'universal search initiatives' to 'drive the bulk of increase in traffic to Google's comparison-shopping service'. A form of user-inertia similar to the one identified in Microsoft case seems to be particularly at play for the first three to five generic search results and for results displayed with richer graphic features, which seem to have a major impact on the click rates of a link, irrespective of the relevance of the underlying page.'

Iacobucci and Ducci 2019, pp. 29–30.

[12] In EU competition law, market power entails a company's ability to influence market conditions, which is especially relevant under Article 102 of the Treaty on the Functioning of the European Union (TFEU), that prohibits the abuse of a dominant position. This concept is particularly pertinent in the digital sector, where platforms can rapidly gain significant market influence. Transparency for such platforms is crucial to safeguard consumer rights, ensuring users are informed about data use and to prevent anti-competitive practices. Moreover, it aids regulatory bodies in monitoring compliance with competition laws, fostering fair competition and market efficiency. This is essential in digital markets, where the dominance of a few players and the rapid evolution of technology can significantly impact market dynamics.

[13] Treaty on the Functioning of the European Union 2012, arts. 101 and 102.

their characteristics. A relevant geographic market refers to an area in which conditions for supply and demand of certain products or services are relatively homogenous and distinguishable from other areas.[14]

A staff working document from the European Commission, released on July 12, 2021, suggested that a review of the Market Definition Notice, which is part of EU competition law, showed that the importance of defining the market and its fundamental principles have mostly stayed the same since 1997. This consistency has been largely upheld in decisions made by EU Courts.[15]

For example, in the case of Google, there are concerns regarding its abuse of market power.[16] Since Google currently holds almost 90% of the search engine market share worldwide and more than 93% in Europe,[17] it could, fuelled by the possibility of favouring its own affiliate applications in query results,[18] abuse its dominance through monopolistic practices, stifling consumer choice and reducing competitiveness in other sectors.[19]

Additionally, there is an issue regarding business-to-business relations on digital platforms, as well as a lack of possibilities to compete.[20] Due to business models being generally geared toward generating revenue through advertisements, there is little incentive to include content from direct or secondary competitors. In the Google example, it is extremely important to businesses' relevance nowadays to be well ranked in its search query results. If the criteria used by Google to rank one company higher than another is not transparent and in accordance with users' expectations, this may lead to infringements on users' freedom to conduct business online.[21] One example of a possible way such infringements could be committed, would be setting the parameters of the PageRank algorithm to divert users' traffic away from competitors in unfair ways.

If we consider Lawrence Lessig's idea of (computer) code producing 'law' in the sense of shaping and steering societal behaviour, one can assume that algorithms also can shape and steer decision-making processes in the steadily growing online pool of internet users.[22] By influencing consumers' behaviour through the direction of online traffic to specific political content or granting of access to particular information (instead of other information that may be purposefully excluded from its results), search engines, social networks, video streaming and other digital platforms can

[14] Commission Notice on the Definition of Relevant Market for the Purposes of Community Competition Law 1997.

[15] Commission Staff Working Document 2021, p. 67.

[16] Saurwein et al. 2015, p. 37. See also: Iacobucci and Ducci 2019, pp. 20–21.

[17] StatCounter Global Stats 2020.

[18] Case AT.39740, Google Search (Shopping), 2017 E.C.

[19] 'The battle against the accumulation of data operated by PageRank reminds the social struggles against the traditional forms of monopoly and accumulation of capitals. PageRank is to the internet, as primitive accumulation and rent are to early capitalism.' Pasquinelli, 'Google's PageRank,' p. 12.

[20] Saurwein et al. 2015, p. 37.

[21] Strader, 2019, p. 560.

[22] Hildebrandt, 'Code Driven Law,' pp. 67–84.

actually precipitate certain behaviours in the same way social norms, nature, and the market do.[23] Thus, the theory that 'code is law' has its merits.

Lawrence Lessig's 'code is law' theory fundamentally impacts market power and transparency in digital markets by highlighting how algorithms, akin to legal codes, can shape consumer behaviour and decision-making. This perspective emphasizes the control digital platforms have over market dynamics, extending beyond traditional market dominance to influencing market conditions themselves. Consequently, greater transparency of algorithmic processes ensures fairness and further protects consumers. This theory calls for a regulatory approach that considers the influence of algorithmic control on competitive practices and consumer choices, highlighting the need for policies that address both traditional aspects of market power and the newer, more nuanced forms of influence in the digital economy.

The main conclusion to be drawn from all this is that these concerns call attention to a lack of transparency surrounding digital platforms. The various conceptions of transparency can be considered in relation to three actors. First, the end-user of platform provides personal data and is subjected to its content. Second, the business user wishes to see its content (website, blog, service, product, etc.) displayed and well-ranked on the platform. Third, regulators in a broad sense, which encompasses competition and data protection authorities, magistrates, superior courts, and members of legislative branches of government, that have mandates to scrutinize, understand analyse and enforce current legislation with regards to these platforms.

Due to a series of contextual circumstances surrounding the conception of most digital platforms' business model, their algorithm is created and developed in a manner that is highly dependent on users' personal data, less prone to regulation, and extremely fierce toward its competitors.[24] Over the years, this business strategy has continued to be employed and perfected, in addition to being appropriated by other tech startups, establishing surveillance capitalism as a standard practice.[25]

Nonetheless, the issues at hand have led to a growing predicament with regard to the unique convergence of issues surrounding this platform. Users, businesses, and governmental bodies alike have a significant stake in the regulation of the mechanism essential to its operations: the algorithm. Therefore, better transparency standards are essential in order to meet the expectations of its users (both individuals and businesses).

[23] Ribeiro et al. 2019.

[24] There are many challenges that regulatory frameworks face in effectively governing the complex, rapidly evolving, and data-centric business models of these platforms. This difficulty stems from the technological complexity of algorithms, the fast pace of digital innovation, the global reach of platforms versus local regulatory powers, the intricacies of data privacy, and the resistance of business models centered on surveillance capitalism. Consequently, there often exists a gap between the development of digital technologies and the ability of regulations to adapt and address emerging concerns effectively.

[25] Zuboff, 2019, p. 369.

13.4 Legal Inscrutability of Algorithms

Broadly speaking, one may contend that there is a tendency for the importance of behavioural data to grow even more over the next years and decades. This overflow of data into the digital economy also feeds the artificial intelligences behind automated systems, most of them proprietary. Companies collect, process, and create value out of data, especially to feed predictive models for advertisers and consumers. In essence, the key to success lies in identifying patterns; by analysing past behaviours, companies can forecast future trends.[26]

The data processor is not always the data collector. Since consent, legitimate interest, and other legal bases are understood as the requirements for the processing of personal data, users may be startled to find out about the cross-referencing of data between original collectors and data brokers or even between different applications of the same company.[27] For example, Alphabet Inc. (Google's parent company) invests its efforts into numerous services, but an important asset is the large number of users (and, therefore, their data) of the services offered by their core businesses, like Google Search, Gmail, and YouTube. Unbeknownst to most users, a combination of different data sources might be what determines the logic behind the profiling activities of certain algorithmic decisions.[28]

Because generating extra behavioural data was crucial for income, and keeping it secret was essential for continuously gathering more of this data, the reasoning that directs this processing of data would also remain, for the most part, protected by black boxes sustained by the justification of safeguarding trade secrets.[29] Unaware of how their data is being processed, as this is obscured by the rationale of trade secrets, users remain oblivious to how decisions are being made for them in crucial areas, such as insurance, finance, employment, credit-scoring, policing, and criminal justice, among other vital fields that can profoundly impact their lives.[30]

These areas connect with platforms through the mechanisms used to collect, process, and exploit user data. Digital platforms, ranging from social media networks

[26] Pasquale 2015, p. 20.

[27] Pasquale 2015, p. 32.

[28] The Article 29 Data Protection Working Party highlights the statistical deduction nature of profiling and defines it according to three essential elements: '[I]t has to be an automated form of processing; it has to be carried out on personal data; and the objective of the profiling must be to evaluate personal aspects about a natural person.' Therefore, profiling involves a higher legal threshold rather than a simple classification of data subjects. Article 29 Data Protection Working Party 2017, pp. 6–7. See also: Oostveen and Irion, 'Golden Age of Personal Data,' p. 16; Büchi et al. 2020, p. 2.

[29] O'Neil 2016, p. 173. See also: Schneier 2015, p. 230; Guidotti et al. 2019, p. 36.

[30] An algorithm analyzes various statistics to predict the likelihood of an individual being an unsuitable employee, a high-risk borrower, a terrorist, or a poor teacher. This prediction is then converted into a score that has the potential to drastically alter someone's life. However, if the individual attempts to contest this, merely presenting suggestive counter evidence is insufficient. Their argument must be exceptionally strong. As we'll repeatedly observe, individuals affected by these 'Weapons of Math Destruction' are subjected to much stricter evidence requirements than the algorithms are. O'Neil 2016, p. 10. See also: Smith 2019, pp. 7–15.

to search engines and e-commerce websites, are at the forefront of accumulating behavioural surplus because they are integral to users' online activities. These platforms are the primary sites for the generation and collection of behavioural surpluses. Also, they embody the challenges associated with data privacy, algorithmic decision-making, and the lack of transparency, all of which have significant implications for individual autonomy and societal norms. The concerns extend beyond the mere presence of platforms to encompass the broader implications of how data-centric business models influence crucial aspects of our lives, often without clear accountability or oversight.

The case of Google Street View in Germany and other European countries is remarkable and exemplifies this issue. After an audit by the German data protection authority, Google admitted it had 'been accidentally gathering extracts of personal web activity from domestic Wi-Fi networks through the Street View cars it has used since 2007.'[31] Moreover, the company's automobiles were equipped with antennas that scanned and analysed Wi-Fi networks throughout the routes they travelled, collecting information. There was no consent for such data collection nor any apparent legitimate interest that justified a street mapping service engaging in this activity.

To help address this matter, it is worth inquiring into the purported technical challenges to scrutinizing an algorithm.[32] The rendering of data collected from users into something useful, and not just the data in and of itself, is what comprises the function of the algorithm. These probability calculations,[33] as well as profiling and pattern recognition, inform the decisions of platforms, and are directly related to how efficient, user-friendly, and potent the platforms are perceived to be. According to Cathy O'Neil, this is a feature of digital platforms that steers them both towards secrecy and competitiveness.[34]

---

[31] Kiss 2010.

[32] Bayamlıoğlu 2021, p. 15.

[33] Automated decisions consist of a statistical calculation of probability. Depending on certain criteria previously set by algorithm designers, data subjects can be classified into different categories. The more data there is on a subject, the more likely it is for him or her to be adequately classified.

[34] 'And yet many companies go out of their way to hide results of their models or even their existence. One common justification is that the algorithm constitutes a 'secret sauce' crucial to their business. It's *intellectual property*, and it must be defended, if need be, with legions of lawyers and lobbyists. In the case of web giants like Google, Amazon and Facebook, these precisely tailored algorithms alone are worth hundreds of billions of dollars. WMD [Weapons of Math Destruction] are, by design, inscrutable black boxes. That makes it extra hard to definitively answer the second question: Does the model work against the subject's interest? In short, is it unfair? Does it damage or destroy lives?' Note that Cathy O'Neil, an American data scientist and author, treats trade secrets as equivalent to an intellectual property right, which is a concept in dispute. This also has to do with her American practical background and research, a jurisdiction in which the tradition of intellectual property rights assumes a usually excessively protective stance of the right of owners, encompassing a myriad of IP categories to inhibit infringement and protect service providers. Even from a competition standpoint, American authorities such as the Federal Trade Commission are frequently more lenient to companies that ensure lower prices to consumers. O'Neil 2016, p. 29.

It is important to understand that biases and errors are not just technical problems, or things that can be solely managed by means of simple adjustments to the code. Some of these predictive models rely upon choices about what data is used and what is not.[35] These decisions also imbue algorithms with designers' biases, prejudices, priorities, judgments, and misunderstandings. Often, these human shortcomings are passed onto algorithms, which perpetuate injustices and define individuals' realities significantly. Hence, this issue also happens to be a matter of justice, fairness, and morality. Possible solutions will neither be only technical nor solely regulatory or governance related. They will have to take into consideration a legal balancing of rights, a juxtaposition of values, and a counterweighting of political forces.

13.5 The Clash Between Intellectual Property Rights and Societal Well-Being

To understand the role of intellectual property rights and trade secrets in the transparency of algorithms, it is essential to recognise how these legal tools are used to safeguard computer programs. Trade secrets differ from copyrights and patents in that they are not formal intellectual property rights requiring registration or public disclosure. Instead, they protect confidential business information (such as the algorithms performing automated decision-making) that provides a competitive edge, based on secrecy. Unlike the fixed-term protection offered by copyrights (for original works) and patents (for inventions, including in some cases software algorithms), trade secrets can offer indefinite protection as long as the information remains undisclosed. This contrasts with the public disclosure required for patents and the automatic protection copyrights provide. That is why trade secrets contribute to the opacity of algorithms, as they inherently limit transparency by relying on the information's confidentiality.

According to Article 2(1) of the EU's Directive 2016/943, regarding the protection of undisclosed know-how and business information, trade secrets are defined as follows:

> 'Trade secret' means information which meets all of the following requirements: a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; b) it has commercial value because it is secret; c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.[36]

Since there is some room for state-by-state interpretation of directives in the European Union, a broad analysis of the practical implementation of the Trade Secrets Directive reveals that it is used to provide legal protection to many types of information: 'technical or non-technical data, patterns, compilations, programs, devices,

[35] O'Neil 2016, pp. 3–218. See also: Graef 2018, p. 131.

[36] Directive (EU) 2016/943 2016, art. 2.1.

methods, techniques, financial data, customer lists, or supplies that have economic value.'[37]

Companies typically employ a dual approach: utilizing trade secrets, which are intangible assets rooted in competition law, alongside either copyright or patent protections, both forms of IP rights. The visible aspects of computer programs, like the user interface, are often shielded by copyright or patents. These protections are robust against reverse engineering and facilitate interoperability.[38] Additionally, companies might consider patenting the algorithm itself, especially in jurisdictions like the United States where the scope of patent protection is broader than in the EU.[39] This legal strategy, while protecting proprietary interests, inherently contributes to the opacity of algorithms, as it limits the disclosure and scrutiny of the underlying code and operational logic.

Another type of right involved in business models that are based on computer processing is database rights. According to Directive 96/9/EC, a database consists of 'a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means.'[40] Very similar to the logic of copyrights, database rights encompass the concept of authorship and a limited timeframe for protection of exclusive use.

Although a variety of intellectual assets can overlap in legal strategies of algorithmic business models, including intellectual property and *sui generis* rights such as database rights, the present analysis is focused on the aspects related to the trade secret protection of algorithms performing automated decisions. Therefore, though many layers of legal protection can shield the different processes of a company, the black box surrounding the performance of algorithms is of particular interest in a systemic approach.

---

[37] Desai 2018, p. 490. It is particularly interesting to observe the actual wording of the Trade Secrets Directive, since it distinctively separates trade secrets from intellectual property. Recitals 1 and 2 of Directive 2016/943 refer to trade secrets as 'intellectual capital' and as an alternative to a list of intellectual property rights. Therefore, a noticeable distinction is drawn between trade secrets and intellectual property rights. Internationally and within the European Union, the matter of trade secrets is treated in a parallel manner as intellectual property rights. Recital 39 of the Trade Secrets Directive makes it clear that there is a legal distinction between them. It should be noted that this directive also establishes that member states of the EU are still allowed to apply rules that require disclosures to either the public or to public authorities, if necessary. Moreover, other limitations are set in Article 9 of the same statute regarding the confidentiality of trade secrets during the course of judicial proceedings. These limitations provide an additional layer of protection for companies when providing documents and testimonies to hearings regarding such competitive assets and even provide for the possibility of a confidential version of the decision to be rendered as an exceptional measure to protect trade secrets. See also: Arcidiacono 2016, pp. 1073–1085.

[38] Lu 2020, p. 117.

[39] According to Article 8 of the Directive 2009/24/EC: 'The provisions of this Directive shall be without prejudice to any other legal provisions such as those concerning patent rights, trademarks, unfair competition, trade secrets, protection of semi-conductor products or the law of contract.' This allows for additional intellectual property protection to computer programs' functionalities, not just copyright, or at least a systematic interpretation of those rights within the intellectual property protection realm of possibilities. Directive 2009/24/EC 2009, art. 8.

[40] Directive 96/9/EC 1996, art. 1.2.

There is also a distinction between algorithms and the source code of computer programs, which is of the utmost importance for our analysis, considering it reveals the reasons why copyright does not provide enough protection in the tech industry.[41] A source code is the tangible support (0's and 1's, or other code forms that a literal programming language may entail) by which an algorithm performs its task. According to Directive 2009/24/CE, Recital 11, algorithms resemble programming languages in the logic through which ideas are expressed (computer codes).[42]

The ideas and logic behind an algorithm are not subject to copyright protection, unlike the actual form by which they are expressed (sequence of codes). Thus, if a creator of an algorithm were to protect its creation only through copyright, competitors would be able to base new creations on the underlying ideas and methods of the original, as long as they expressed it in a different way (original code). It is for this reason that trade secrets then become a more advantageous way of protecting the property of the algorithms' creators. Trade secrets, however, tend to be used to protect 'deeper' parts of the provision of software, where it is possible to maintain control of the rationale behind input to output transformation.

There are also significant procedural differences between cases discussing trade secrets and intellectual property rights. While the European Union provides specific pre-litigation evidence collection provisions under the Intellectual Property Enforcement Directive,[43] such provisions have been purposefully avoided by national legislators when regulating the protection of trade secrets in the Union.[44]

The fact that trade secrets, contrary to patents and copyright, are required to meet minimum bureaucratic standards or none at all (such as administrative registration), makes them an interesting option for companies that follow flexible business models with rapidly adaptable characteristics. For this reason, startups and companies seeking to protect proprietary algorithms often opt to protect them under the banner of trade secrets. However, the very characteristics that define trade secrets could also enable them to continue and intensify 'pre-existing biased social frameworks, especially when these systems are left unmonitored and uncontrolled.[45]

Unlike other intangible intellectual assets, the right to trade secrets does not require public disclosure of the object of protection.[46] Pointing this out may seem like a

[41] Marty 2019, p. 222.

[42] For the avoidance of doubt, it has to be made clear that only the expression of a computer program is protected and that ideas and principles which underlie any element of a program, including those which underlie its interfaces, are not protected by copyright under this Directive. In accordance with this principle of copyright, to the extent that logic, algorithms and programming languages comprise ideas and principles, those ideas and principles are not protected under this Directive. In accordance with the legislation and case-law of the Member States and the international copyright conventions, the expression of those ideas and principles is to be protected by copyright. Directive 2009/24/EC 2009, Recital 11.

[43] Corrigendum to Directive 2004/48/EC 2004.

[44] Niebel et al. 2018, p. 447.

[45] Moore 2017, p. 6.

[46] Patents offer exclusive rights to new inventions at the cost of revealing them to the public. Conversely, trade secrets don't grant such exclusive rights, but their protection can last indefinitely

tautology, but it is relevant to grasp the effects it may have on digital innovation. Since the object of trade secret protection will not be eventually available to society after a period of time (most importantly, to competitors, which is the case with patents), this creates greater barriers to entry to newcomers in specific markets and, thus, less competition in the medium to long term.[47] Other intangible intellectual rights, such as intellectual property rights, enjoy somewhat limited protection in terms of time (expiration of patents, for example), scope (jurisdiction), and object (some are specifically excluded from intellectual property protection).[48]

Furthermore, companies that envisage worldwide provision of services, which is the case with GAFA (Google, Apple, Facebook, and Amazon), for instance, do not wish to be bound by local jurisdictional, temporal, or object scope. These legal hurdles increase the cost of doing business, especially opportunity costs, i.e., the costs of losing opportunities to launch new products.[49] Thus, trade secrets become an appealing option in the digital realm.[50]

If we systematically interpret these provisions with Article 23(1)(i) of the GDPR, one can see that restrictions to data controllers and processors' rights apply 'when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the protection of the data subject or the rights and freedoms of others.'[51] Thus, limitations to intangible intellectual assets such as trade secrets may be not only possible but also necessary in order to safeguard users' fundamental rights.[52]

In the context of the European Union, trade secrets are intimately connected to the principle of competition. Even its definition is relational, since the element of market value, a requirement for its characterization, is extracted precisely from

as long as they are not disclosed against the owner's will. This might be seen as a benefit compared to intellectual property rights that expire after a certain period. Niebel et al. 2018, p. 447.

[47] Marty 2019, p. 217.

[48] Hrdy and Lemley 2021, pp. 10–11. Also, patent law's demand for public disclosure of inventions aimed to foster transparency by conditioning intellectual property protection on detailed public descriptions of the inventions. Over time, however, this open system was overlooked as savvy, but unethical people figured out how to exploit these transparent systems. The lure of gaining profits through exclusive information proved too tempting to ignore. See: Pasquale 2015, p. 193.

[49] Svantesson 2017, pp. 65, 109, 117.

[50] Globally, the recommendation system of Amazon, Instagram's algorithm for spreading posts, and Google's search algorithms stand out as famous trade secrets. The specific methods Google uses to assess links between pages, improvements in its search system, and criteria to identify manipulations are kept secret. For instance, it's unclear how Google weighs various factors, like the number of links, page traffic, or the organization of a page's source code. See: Brkan and Bonnet 2020, p. 40.

[51] Regulation (EU) 2016/679 2016.

[52] Ideally, this is a theoretical and legal framework applied through casuistry, not necessarily a hierarchical structure of data protection rights over algorithmic intellectual assets. According to Brkan and Bonnet: '[I]f GDPR always prevailed over trade secrets, the latter could never be protected when providing an explanation of an algorithmic decision to the data subject.' Brkan and Bonnet 2020, p. 40.

a competitive advantage.[53] Frédéric Marty defines it as 'information known by a restricted number of people, with commercial value, effective or potential, due to its secretive character and that is subject to reasonable measures of protection to maintain its secretive character' (my translation).[54]

If it were the case that competitors obtained the information subject to protection by legitimate methods, such as technological advancements, research and development, or reverse engineering, there would be no issue at hand. However, what is considered illicit are anti-competitive practices, such as unlawful disclosure by former employees or business espionage.[55] Both these situations are foreseen by Articles 3 and 4 of the EU directive on the protection of trade secrets.[56]

Thus, unfair competition is a primary concern with regard to this category of intangible business assets and must be considered as a factor of analysis. Nevertheless, how does one compete and innovate in markets based on algorithmic business models? Intellectual property, such as patents and copyrights, are usually characterized by incremental innovations in their respective markets, whereas a scenario widely based on trade secrets requires that competitors invest a similar number of resources into research and development (which can be quite significant in the tech industry) in order to attempt to compete. Trade-secret law uniquely permits owners to withhold information, in contrast to intellectual property rights.[57]

In markets where digital platforms use algorithms to make decisions, new companies often try not to compete directly with dominant players. Instead, they aim to offer products and services that complement those of the established companies. This approach strengthens the leading position of well-established companies in the main market.[58] Hence, trade secrets tend to stifle competition in primary markets, which may not be ideal, depending on the objectives one considers in regulating competition. Its negative externalities might outweigh its positive ones, strengthening oligopolies, for example.

Once again, focusing on the usual business models of this analysis, digital platforms based on behavioural advertising, it is important to note that its putative neutrality is, in fact, also a product of a business model that relies on secrecy in order to thrive.[59] An erroneous assumption by the public, although widespread among its users, is that timelines, recommendations, rankings and results are objective.[60]

---

[53] Hrdy and Lemley 2021, pp. 31–32. See also: Banterle 2018, p. 420.

[54] Marty 2019, p. 214.

[55] Marty 2019, p. 215.

[56] It defines lawful acquisition as that achieved by means of independent discovery, creation, observation, study, and reverse engineering, among other means. Guidotti et al. 2019, pp. 10–11.

[57] Scotchmer 2004, p. 81.

[58] Marty 2019, p. 220.

[59] '[…] Google is not a neutral tool or a non-distorting lens: it is an actor and a stakeholder in itself. And, more important, as a publicly traded company, it must act in its shareholders' short-term interests, despite its altruistic proclamations.' Vaidhyanathan 2011, p. 9. See also: Martin 2019, p. 839.

[60] For example, the automated decisions of Google Search derive from a combination of the mathematics related to the algorithmic relevance of certain content and of the editorial decisions of the

However, this perception actually stems from a highly effective personalization algorithm, as we have seen, and from companies' savvy strategies to characterize its business model as exempt from scrutiny.[61]

Digital platforms, particularly those using algorithms for automated decision-making, have trade secrets play as a key component that shapes (the lack of) transparency and competition. They offer indefinite protection to the more covert elements, creating opacity around algorithms. This legal framework, while protecting proprietary interests, potentially stifles competition and innovation in the market by creating barriers to entry and perpetuating existing market dominance, as newcomers often find it challenging to compete with or innovate beyond the established players. The EU recognizes the delicate balance between protecting trade secrets and ensuring fair competition, indicating the need for regulation that considers the broader impacts on market dynamics and user rights.

Thus, this analysis on the nature of trade secrets brings forward a correlation between Google's opaque algorithm and the core role of its data extraction imperatives, which have been replicated by Facebook and other emerging data-driven companies.[62] The same predilection of these companies for trade secrets over patents and copyrights justifies the need to make the right to protect trade secrets dependent on the guarantee of an effective explanation of algorithmic decision-making.

company itself, which chooses not to show results that violate copyrights, contain pornographic content, encourage violence etc. Therefore, even subjective factors influence the ranking of results provided by the search engine. According to Google's Code of Conduct, which interestingly abandoned its quite literal 'don't be evil' motto in 2018, 'Google's intellectual property rights (our trademarks, logos, copyrights, trade secrets, 'know-how,' and patents) are among our most valuable assets.' 'Alphabet Investor Relations: Google Code of Conduct,' Alphabet Inc., accessed July 31, 2018, https://abc.xyz/investor/other/code-of-conduct.

[61] Many people believe that searching for a term on Google yields the same results for everyone, ranked by the company's well-known Page Rank algorithm according to the authority of links from other pages. However, since December 2009, this assumption has become outdated. Currently, Google's algorithm tailors search results to what it deems most relevant for each individual user, meaning different people may see completely different results. Essentially, there's no longer a one-size-fits-all version of Google. See: Pariser 2011, p. 2.

[62] Today's trade secrets, such as Google's search engine algorithm, are often more secure against being revealed. They are usually difficult to reverse engineer, and there are fewer employees who could potentially leave and share their knowledge with a competing company. Hrdy and Lemley 2021, p. 13. See also: Lu 2020, p. 114.

13.6 Market Power and Algorithms: The Digital Markets Act and the Digital Services Act

The Digital Single Market Strategy launched two significant regulations in this field: The Digital Services Act (DSA)[63] and Digital Markets Act (DMA).[64] The DSA is focused on the fact that online intermediaries share responsibilities in ensuring predictability, safety, and protection of fundamental rights within the European Union's digital environment. Thus, many of the provisions it sets out focus on transparency, liability, and risk mitigation (against fundamental rights violations). It particularly applies to recommender systems, a definition which can be applied to Amazon's or Google's results page, for example.[65]

Article 27 of the DSA (recommender system transparency) is of the utmost relevance, since it encompasses the reasoning behind automated decisions, the need for explanations comprehensible to users regarding such reasoning, and finally, the possibility to provide more autonomy to users through the individual personalization of these platforms. It requires platforms to implement explainability tools for its users, in addition to providing them with the choice to adhere or not to these criteria or personalization.

The DSA foresees the need for 'very large platforms' to execute audits in order to conduct 'risk assessments and design their risk mitigation measures with the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations.'[66] The Act mentions specific algorithmic audits which should ensure the confidentiality, security, and integrity of the information gathered, such as trade secrets.[67] Even though the DSA is not a competition mechanism, it does provide transparency tools that might increase scrutiny of online platforms, especially larger platforms with recommender systems.

The DMA focuses on *ex ante* rules to ensure contestable, interoperable, and fairer markets in the digital sector where gatekeepers are present. It defines gatekeepers (providers of core platform services when they have a significant impact on the internal market) to raise core issues related to their opaqueness and complexity. And, again, like the Digital Services Act, this central legal definition in the regulation has the potential to profoundly change and influence the realm of digital platform regulation, because it creates additional obligations for these core platform services, based on contestability mechanisms, transparency, and market monitoring investigations.

---

[63] Regulation (EU) 2022/2065.

[64] Regulation (EU) 2022/1925.

[65] 'A fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service, including as a result of a search initiated by the recipient or otherwise determining the relative order or prominence of information displayed.' Article 2, (o), of the DMA.

[66] Recital 90, Digital Services Act, 2022.

[67] Recital 92, Digital Services Act, 2022.

Furthermore, the concept of transparency with regard to users' data is directly linked to a more fertile and competitive market for newcomers.[68]

Another provision requires gatekeepers to allow business users to offer the same products or services to end users through third party online intermediation services at prices or conditions that are different from those offered through the online intermediation services of the gatekeeper.[69] Also, they must provide to any third party providers of online search engines, upon their request, access on fair, reasonable and non-discriminatory terms to ranking, query, click and view data in relation to free and paid search generated by end users on online search engines of the gatekeeper, subject to anonymisation for the query, click and view data that constitutes personal data.[70] These are provisions that directly respond to issues raised against Google in previous antitrust cases, such as those concerned with Google Android and Google Shopping, and that would foster competition in their markets. There is no question that this is part of the European Union's institutional response to the anticompetitive practices in which Google has engaged in the past.

Reflecting on the provisions of the DSA and the DMA reveals both their strengths and limitations in ensuring platform accountability and transparency. While these regulatory frameworks aim to safeguard fundamental rights within the EU's digital environment and ensure fairer digital markets, their effectiveness hinges on its transparency and liability provisions' effectiveness in practice. What will be the depth of explanations provided and will they truly enhance users' autonomy, or merely serve as superficial compliance measures? The complex nature of algorithms might render explainability insufficient for the average user to grasp, limiting its intended empowerment effect.

Moreover, the requirement for algorithmic audits and risk assessments under the DSA points towards a proactive approach in identifying and mitigating risks associated with digital platforms. Yet, the effectiveness of these measures largely depends on the rigor of the audits, the independence of the auditors, and the transparency of the audit process itself. Without stringent enforcement mechanisms and clear standards for these audits, there's a risk that these processes become tick-box exercises rather than substantive evaluations of platforms' impact on fundamental rights and societal values.

The DMA's focus on contestability and fairness through *ex ante* rules for gatekeepers highlights the EU's commitment to curbing anti-competitive practices in digital markets. While the provisions aimed at ensuring interoperability and preventing unfair conditions are vital steps towards a more competitive digital

[68] The data protection and privacy interests of end users are relevant to any assessment of potential negative effects of the observed practice of gatekeepers to collect and accumulate large amounts of data from end users. Ensuring an adequate level of transparency of profiling practices employed by gatekeepers facilitates contestability of core platform services, by putting external pressure on gatekeepers to prevent making deep consumer profiling the industry standard, given that potential entrants or start-up providers cannot access data to the same extent and depth, and at a similar scale. Recital 72, Digital Markets Act, 2022.

[69] Article 5.3, Digital Markets Act, 2022.

[70] Article 6.11, Digital Markets Act, 2022.

economy, the challenge lies in their enforcement. The dynamic nature of digital markets and the sophisticated strategies employed by gatekeepers to maintain their dominance demand agile and robust regulatory responses. The current provisions may not fully account for the evolving tactics of gatekeepers, or the complexities involved in implementing and enforcing interoperability requirements.

Furthermore, both the DSA and DMA could benefit from integrating insights and provisions from the recently approved AI Act, particularly concerning advanced AI systems used by digital platforms. The AI Act's focus on high-risk AI applications provides a framework that could complement the DSA and DMA by offering specific guidelines and standards for the ethical and responsible use of AI in digital platforms. This integration could address potential gaps in dealing with AI-driven practices that impact market dynamics and fundamental rights.

While the DSA and DMA represent significant advancements towards regulating digital platforms, their success in ensuring platform accountability, transparency, and contestability is contingent upon robust enforcement, clear standards for algorithmic transparency and audits, and the integration of comprehensive legal reasoning that includes considerations from the AI Act. Addressing these challenges requires an approach that combines regulatory oversight with stakeholder engagement and continuous evaluation of the regulatory frameworks' effectiveness in the face of rapidly evolving digital technologies.

13.7 Conclusion

As we navigate the intricacies of the digital era, the role and influence of algorithmic decision-making systems have become undeniably central to our societal fabric. These algorithms, once heralded as harbingers of objectivity and efficiency, are now under increased scrutiny for their latent biases and potential to perpetuate discrimination.

The once-held belief in the unerring neutrality of platforms like Google, Facebook, and Twitter is being systematically deconstructed, revealing a landscape where content is not merely presented but is actively shaped, often in ways that serve the platforms' interests. The monopolistic dominance of a few digital behemoths further exacerbates these concerns, raising pressing questions about market dynamics, competition, and the very essence of user choice in the digital realm. Addressing these multifaceted challenges necessitates a comprehensive approach, one that fosters collaboration among diverse stakeholders, from policymakers to platform operators. As we stand at this pivotal juncture, the call for transparency, accountability, and a rights-centric approach to algorithmic decision-making has never been more urgent. Only through such concerted efforts can we hope to strike a balance between technological innovation, market competition, and the broader well-being of society in an age defined by algorithms.

In the rapidly evolving digital landscape, the prominence of algorithmic decision-making has raised significant concerns regarding transparency. This chapter has

explored the challenges posed by putative neutrality, market power, and the (supposed) legal inscrutability of algorithms. It has also highlighted the increasing necessity of a right to explanation for automated decisions, particularly in the context of personal data processing.

The analysis underscores the inherent biases embedded in algorithms used by digital platforms, challenging the assumption of neutrality. The concentration of market power among dominant platforms further exacerbates the need for regulatory interventions to ensure fair competition and protect user rights. The legal protection afforded to algorithms through trade secrets and intellectual property rights creates barriers to understanding their functioning and potential biases.

To address these challenges, there is a growing call for transparency and accountability in algorithmic decision-making. The notion of a right to explanation has gained traction, emphasizing the need for individuals to understand the logic and consequences of automated decisions that affect their lives. This right should be complemented by robust regulatory frameworks that promote fairness, protect user data, and mitigate the risks of algorithmic discrimination.

Recent developments in the European Union have led to the adoption of the Digital Services Act and the Digital Markets Act, which aim to address issues of transparency and explainability of very large online platforms and of gatekeepers, respectively. The regulations recognize the need for explainability and set requirements for transparency in the provision of platform services online. What is certain is that the challenges posed by algorithmic decision-making call for a multifaceted approach that prioritizes transparency and the protection of individual rights.

Acknowledgements The author would like to acknowledge the support received from Sciences Po's Law School and the McCourt Institute in facilitating the research and development of this chapter. The author would also like to disclose that the views expressed in this chapter are solely those of the author and do not necessarily reflect the opinions or positions of Sciences Po's Law School, the McCourt Institute, or any funding entities.

References

"Alphabet Investor Relations: Google Code of Conduct," Alphabet Inc., accessed July 31, 2018, https://abc.xyz/investor/other/code-of-conduct.

Article 29 Data Protection Working Party, "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679" (WP251rev.01, 3 October, 2017), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

Bilel Benbouzid, "Values and Consequences in Predictive Machine Evaluation. A Sociology of Predictive Policing," Science & Technology Studies 32, no. 4 (2019), https://sciencetechnologystudies.journal.fi/article/view/66156.

Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (New York: W.W. Norton & Company Inc, 2015).

Camilla A. Hrdy and Mark A. Lemley, "Abandoning Trade Secrets," Stanford Law Review 73, no. 1 (January 2021): 10-11, https://review.law.stanford.edu/wp-content/uploads/sites/3/2021/01/Hrdy-Lemley-73-Stan.-L.-Rev.-1.pdf.

Case AT.39740, Google Search (Shopping), 2017 E.C.
Catherine Stinson, "Algorithms Are Not Neutral: Bias in Collaborative Filtering," arXiv:2105.01031 (May 2021), https://arxiv.org/abs/2105.01031.
Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (New York: Crown Publishers, 2016).
Charter of Fundamental Rights of the European Union, 2012, O.J. 2012/C 326/02, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN#d1e364-393-1.
Commission Notice on the Definition of Relevant Market for the Purposes of Community Competition Law (EU), 1997 O.J. (97/C 372 /03), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997Y1209(01)&from=EN.
Commission Staff Working Document, "Evaluation of the Commission Notice on the Definition of Relevant Market for the Purposes of the Community Competition Law of 9 December 1997," (July 12, 2021), at 67, https://ec.europa.eu/competition-policy/system/files/2021-07/evaluation_market-definition-notice_en.pdf.
Consolidated Versions of the Treaty on the Functioning of the European Union, October 26, 2012, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT&from=EN.
Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, 2004, O.J. (L 157), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32004L0048R(01)&from=EN.
Dan Jerker B. Svantesson, Solving the Internet Jurisdiction Puzzle (Oxford: Oxford University Press, 2017), https://doi.org/10.1093/oso/9780198795674.001.0001.
Davide Arcidiacono, "The Trade Secrets Directive in the International Legal Framework," European Papers 1, no. 3 (November 7, 2016): 1073-1085, https://www.europeanpapers.eu/en/europeanforum/trade-secrets-directive-international-legal-framework.
Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs (Codified Version) (Text with EEA Relevance), 2009 O.J. (L 111), http://data.europa.eu/eli/dir/2009/24/oj/eng.
Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31996L0009.
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 (Text with EEA Relevance), 2016 O.J. (L 157), http://data.europa.eu/eli/dir/2016/943/oj/eng.
Edward Iacobucci and Francesco Ducci, "The Google Search Case in Europe: Tying and the Single Monopoly Profit Theorem in Two-Sided Markets," European Journal of Law and Economics 47, no 1 (February 2019), https://doi.org/10.1007/s10657-018-9602-y.
Eli Pariser, The Filter Bubble: What the Internet Is Hiding from You (London: Penguin Books, 2011).
Emre Bayamlıoğlu, "The Right to Contest Automated Decisions under the General Data Protection Regulation: Beyond the So-called 'Right to Explanation'," Regulation & Governance (March 14, 2021), https://doi.org/10.1111/rego.12391.
European Commission. 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): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689
Florian Saurwein, Natascha Just, and Michael Latzer, "Governance of Algorithms: Options and Limitations," Info 17, nº 6 (September 2015), https://doi.org/10.1108/info-05-2015-0025.

Francesco Banterle, "The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database Sui Generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis," in Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?, org. Mor Bakhoum et al., MPI Studies on Intellectual Property and Competition Law, vol. 28 (Berlin, Heidelberg: Springer Berlin Heidelberg, 2018), https://doi.org/10.1007/978-3-662-57646-5.

Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Cambridge: Harvard University Press, 2015).

Frédéric Marty, "La protection des algorithmes par le secret des affaires: Entre risques de faux négatifs et risques de faux positifs," Revue internationale de droit économique t.XXXIII, no 2 (2019), https://doi.org/10.3917/ride.332.0211.

Gary Smith, "Be Wary of Black-Box Trading Algorithms," The Journal of Investing 28, no 5 (July 31, 2019): 7–15, https://doi.org/10.3905/joi.2019.1.090.

Hannah Bloch-Wehba, "Access to Algorithms," Fordham Law Review 88, no. 4 (March 2020): 1308, https://ir.lawnet.fordham.edu/flr/vol88/iss4/2/.

Heleen L. Janssen, "An Approach for a Fundamental Rights Impact Assessment to Automated Decision-Making," International Data Privacy Law 10, no 1 (February 1, 2020), https://doi.org/10.1093/idpl/ipz028.

Inge Graef, "Blurring Boundaries of Consumer Welfare: How to Create Synergies Between Competition, Consumer and Data Protection Law in Digital Markets," in Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?, org. Mor Bakhoum et al., MPI Studies on Intellectual Property and Competition Law, vol. 28 (Berlin, Heidelberg: Springer Berlin Heidelberg, 2018), https://doi.org/10.1007/978-3-662-57646-5.

Jamie Bartlett, The People Vs Tech: How the Internet Is Killing Democracy (and How We Save It) (London: Penguin Random House, 2018).

Jay Matthew Strader, "Google, Monopolization, Refusing to Deal and the Duty to Promote Economic Activity," IIC - International Review of Intellectual Property and Competition Law 50, no. 5 (June, 2019): 559-594, https://doi.org/10.1007/s40319-019-00818-9.

Jemima Kiss, "Google Admits Collecting Wi-Fi Data through Street View Cars," The Guardian, May 15, 2010, http://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data.

Joanna Mazur, "Right to Access Information as a Collective-Based Approach to the GDPR's Right to Explanation in European Law," Erasmus Law Review 11, no. 3 (December 2018), https://ssrn.com/abstract=3356770.

Jonas Heitto, "The Trade Secret Directive Proposal and the Narrow Path to Improving Trade Secret Protection in Europe," Computer Law Review International 16, no. 5 (2015), https://www.degruyter.com/document/doi/https://doi.org/10.9785/cri-2015-0504/html.

Joshua G. Hazan, "Stop Being Evil: A Proposal for Unbiased Google Search," Michigan Law Review 111, no 5 (March 2013), https://repository.law.umich.edu/mlr/vol111/iss5/5.

Kirsten Martin, "Ethical Implications and Accountability of Algorithms," Journal of Business Ethics 160, no 4 (December 2019), https://doi.org/10.1007/s10551-018-3921-3.

Lucas Anjos and Pablo Leurquin, "Condenações da Google pela Aplicação do Direito da Concorrência da União Europeia," Revista de Defesa da Concorrência, Vol. 9, nº 1 (June 2021): 104-124, https://revista.cade.gov.br/index.php/revistadedefesadaconcorrencia/article/view/903/532.

Maja Brkan and Grégory Bonnet, "Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: Of Black Boxes, White Boxes and Fata Morganas," European Journal of Risk Regulation 11, no 1 (March 2020), https://doi.org/10.1017/err.2020.10.

Manoel Horta Ribeiro et al., "Auditing Radicalization Pathways on YouTube," arXiv, August 22, 2019, http://arxiv.org/abs/1908.08313.

Mireille Hildebrandt, "Code Driven Law: Freezing the Future and Scaling the Past," in Is Law Computable? Critical Perspectives on Law and Artificial Intelligence, ed. Christopher Markou and Simon Deakin (United Kingdom: Hart Publishers, 2020), 67-84.

Oostveen and Irion, "Golden Age of Personal Data," 16; Moritz Büchi et al., "The Chilling Effects of Algorithmic Profiling: Mapping the Issues," Computer Law & Security Review 36 (April 2020), https://doi.org/10.1016/j.clsr.2019.105367.

Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=.

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) (Text with EEA Relevance), 2016 O.J. (L 119), http://data.europa.eu/eli/reg/2016/679/oj/eng.

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) (Text with EEA relevance), 2022 OJ L 277, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065.

Regulation (EU) 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 (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), 2022, OJ L 265, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925.

Rembert Niebel, Lorenzo de Martinis, and Birgit Clark, "The EU Trade Secrets Directive: All Change for Trade Secret Protection in Europe?" Journal of Intellectual Property Law & Practice 13, no. 6 (June 2018), https://doi.org/10.1093/jiplp/jpx227.

Riccardo Guidotti et al., "A Survey of Methods for Explaining Black Box Models," ACM Computing Surveys 51, no 5 (January 23, 2019), https://doi.org/10.1145/3236009.

"Search Engine Market Share Europe," StatCounter Global Stats, accessed December 1, 2020, https://gs.statcounter.com/search-engine-market-share/all/europe.

Serge Abiteboul and Julia Stoyanovich, "Transparency, Fairness, Data Protection, Neutrality: Data Management Challenges in the Face of New Regulation," Journal of Data and Information Quality, ACM (2019): 3, https://hal.inria.fr/hal-02066516.

Shreya Desai, "Shhh - It's a Secret: A Comparison of the United States Defend Trade Secrets Act and European Union Trade Secrets Directive," Georgia Journal of International and Comparative Law 46, no. 2, (2018): 490, https://digitalcommons.law.uga.edu/gjicl/vol46/iss2/7/.

Siva Vaidhyanathan, The Googlization of Everything (And Why We Should Worry) (Los Angeles: University of California Press, 2011).

Sylvia Lu, "Algorithmic Opacity, Private Accountability, and Corporate Social Disclosure in the Age of Artificial Intelligence," Vanderbilt Journal of Entertainment & Technology Law 23, no. 1 (Fall 2020), https://scholarship.law.vanderbilt.edu/jetlaw/vol23/iss1/3.

Taylor R. Moore, Trade Secrets and Algorithms as Barriers to Social Justice, Center for Democracy & Technology, August 3, 2017, 6, https://cdt.org/wp-content/uploads/2017/08/2017-07-31-Trade-Secret-Algorithms-as-Barriers-to-Social-Justice.pdf.

Zuboff, Shoshana, The Age of Surveillance Capitalism. New York: Profile Books Ltd, 2019.

Lucas Costa dos Anjos is a postdoctoral researcher at the École de Droit of Sciences Po—Paris. His research interests include algorithmic transparency and explainability, trade secrets, tech regulation and the new challenges stemming from artificial intelligence. His research on the subject is currently financed by a Postdoctoral Fellowship from Project Liberty (former McCourt Institute). In addition to being a researcher at the Brazilian Data Protection Authority (ANPD), Lucas is also a Professor at the Law School of Universidade Federal de Juiz de Fora. He holds a Doctor degree in Law and in Sciences Juridiques from Universidade Federal de Minas Gerais and Université libre de Bruxelles, respectively, and a Master degree in Law from Universidade Federal de Minas Gerais. He is also the founder and was a scientific advisor of the Institute for Research on Internet and Society (IRIS).